



A meeting of Trust Board to be held at 10am on  
Thursday 4 March 2021 via Zoom (due to Covid-19)

**AGENDA**

- |    |  |   |
|----|--|---|
| 1  | Welcome, Apologies & Declarations of Conflict of Interest  | <a href="#">Click on links to navigate:</a> |
| 2  | Minutes of the previous meeting of the Trust Board held on 21 January 2021<br><b>For Approval</b>  | TB04/03/2021/01                             |
| 3  | Matters Arising  | TB04/03/2021/02                             |
| 4  | Chair's Update<br><b>For Noting</b>  |   |
| 5  | Chief Executive's Update<br><b>For Noting</b>  |   |
| 6  | Self Service Business Intelligence (BI) Reporting Model<br><b>For Noting</b>                       | TB04/03/2021/03                             |
| 7  | People, Finance & Organisational Development Committee – Terms of Reference<br><b>For Approval</b> | TB04/03/2021/04                             |
| 8  | Covid-19 – update<br><b>For Noting</b>   | TB04/03/2021/05                             |
| 9  | Corporate Plan 2020-21 Progress Report<br><b>For Noting</b>  | TB04/03/2021/06                             |
| 10 | Finance Report (Month 10)<br><b>For Noting</b>   | TB04/03/2021/07                             |
| 11 | Information Governance Policies and Procedures and Management Framework<br><b>For Noting</b>       | TB04/03/2021/08                             |



12 Committee Business:

TB04/03/2021/09

- Audit Committee minutes - 29 October 2020
- Report from the Safety, Quality, Patient Experience and Performance Committee – 19 November 2020

**For Noting**

13 Date & venue of next meeting:

**Thursday 6 May 2021 at 10am. Arrangements to be confirmed.**

14 Any Other Business



Northern Ireland Ambulance Service  
Health and Social Care Trust



# ***TRUST BOARD***

A meeting of Trust Board to be held at 10am on  
Thursday 4 March 2021 via Zoom (*due to Covid-19*)

**TB/04/03/2021/01**



**Minutes of NIAS Trust Board held on Thursday 21 January 2021 at  
10.00am via Zoom (due to Covid-19)**

<b>Present:</b>	Mrs N Lappin	Chair
	Mr W Abraham	Non Executive Director
	Mr D Ashford	Non Executive Director
	Mr J Dennison	Non Executive Director
	Mr T Haslett	Non Executive Director
	Mr M Bloomfield	Chief Executive
	Ms R Byrne	Director of Operations
	Ms M Lemon	Interim Director of HR
	Mr P Nicholson	Interim Director of Finance
	Dr N Ruddell	Medical Director
<b>In Attendance:</b>	Ms L Charlton	Director of Quality, Safety & Improvement
	Mr B McNeill	Programme Director - Clinical Response Model (CRM)
	Ms R O'Hara	Programme Director – Strategic Workforce Planning
	Ms A Quirk	Board Apprentice
	Mrs C Mooney	Board Secretary
<b>Apologies:</b>	Mr A Cardwell	Non Executive Director
	Ms M Paterson	Director of Performance, Planning & Corporate Services

**1 Welcome, Introduction & Apologies**

The Chair welcomed those present to the meeting and noted apologies from Mr Cardwell and Ms Paterson.

The Chair asked members to declare any conflicts of interest at the outset or as the meeting progressed.

2 **Previous Minutes (TB21/01/2021/01)**

The minutes of the previous Trust Board meeting held on 26 November 2020 were **APPROVED** on a proposal from Mr Dennison and seconded by Mr Ashford.

3 **Matters Arising (TB21/01/2021/02)**

The Chair noted that, due to current circumstances, a number of Committees had been postponed and would be rescheduled in the coming weeks. It was noted that the Remuneration Committee would now take place on 4 February 2021 to allow her update members on Senior Executive pay.

4 **Chair's Update**

The Chair commenced her update by asking that her appreciation and thanks to all NIAS staff for their efforts be recorded. She said it was very clear from the updates she had received and media reports of the current pressures facing the service and yet staff continued to strive to ensure that ambulance services were delivered to the public.

The Chair said that one of the most important recent developments was the vaccination programme and added that the Trust was working hard to ensure there was a good uptake of the vaccine amongst staff. The Chair said she wished to record her thanks to other Trusts for their assistance in offering the vaccine to NIAS staff. She indicated that the vaccine was important to Trust staff as well as individuals frontline staff would meet when carrying out their day-to-day duties.

The Chair advised that she had made contact with the DoH Public Appointments Unit and said that she had had some high-level discussions as to how vacant Non-Executive Director positions in general might be filled. The Chair also made reference to the DoH requirement for Non-Executive Director appraisals to be completed and said that this work was ongoing.

The Chair said that the Board/Committee schedule for 2021/22 was currently being finalised and would be shared with members in the near future.

The Chair mentioned that she had asked Mrs Mooney to explore the potential for a digital platform for Board/Committee papers moving forward.

Concluding her report, the Chair advised that the December meeting between the Minister and Trust Chairs had been cancelled but that a further meeting had been scheduled for 3 February. She believed that this would provide an opportunity for Chairs to indicate to the Minister their support at a time of unprecedented challenge.

There were no questions from members and the Chair's report was **NOTED**.

## **5 Chief Executive's Update**

Mr Bloomfield said that it had been an extremely challenging period since the last Trust Board meeting in November. He pointed out that projections indicated that the peak of the third surge had been forecast to take place during this week and efforts had been focussed on this. Mr Bloomfield advised that, while the number of community transmissions had plateaued over the last week, there would be a delay in seeing this in hospital admission and ICU numbers.

Continuing, Mr Bloomfield indicated that the pressures across health and social care had been well documented and added that the focus of today's Board meeting was to provide members with an update on the challenges and actions which the Trust had and continued to take to focus on service delivery. He expressed his appreciation to members for their understanding and support with regard to the need to postpone a number of Committee meetings over the coming weeks.

Mr Bloomfield said the Trust was operating in business continuity mode and that everyone's efforts should be focussed on supporting operational service delivery and patient care. He acknowledged that the experience of some patients around having to wait for extended periods of time in the back of ambulances or waiting for ambulance responses in the community would not be in line with the

high quality service the Trust aimed to provide. The Chief Executive said there was no doubt that this increased the risk to patients and believed the Senior Management Team was confident that the Trust was providing the best service it could with the resources available in the current circumstances.

Mr Bloomfield said that he wished to pay tribute to the significant efforts of Trust staff since the start of the pandemic to ensure the Trust provided the best care to patients despite being exhausted. He pointed out that this applied not only to frontline operational staff but to those staff in the Control Room, support staff and Directors and their teams.

Continuing, the Chief Executive reported that, on 10 December, he, Ms Byrne and Dr Ruddell appeared before the Health Committee to brief members on the Trust response to the pandemic. He said that, on 15 December, pressures on the health and social care system were particularly evident with media images of ambulances queued outside Emergency Departments. Mr Bloomfield believed that this had focussed attention on the seriousness of the situation and led to considerable media attention including on the support received from the National Ambulance Service. He extended his appreciation to Dr Ruddell for undertaking a number of media interviews at this time.

Mr Bloomfield reported that on 18 December he had been pleased to meet with a group of EMTs who had concluded their training as well as a group of qualified paramedics who joined NIAS from other ambulance services. He said that the contribution of these staff would be very welcome in the current pandemic.

Concluding his remarks, Mr Bloomfield reported that the Chair and other Directors had taken the opportunity to visit stations in the run-up to Christmas to thank staff for their work. He acknowledged that the brief visits had been conducted adhering to the current guidelines around social distancing.

The Chair thanked Mr Bloomfield for his report which was **NOTED** by members.



## 6 **NIAS Covid-19 Response Assurance Report (TB21/01/2021/03)**

The Chair drew members' attention to the NIAS Covid-19 Response Assurance Report and said that she very much welcomed and appreciated the level of detail provided to the Trust Board at this time. She believed that the report provided members with the necessary assurances around the work being progressed to underpin NIAS' response to the challenges presented by Covid-19. However, she said that, more importantly, the report provided her as a Non-Executive Director, with an insight into the significant amount of unseen work currently underway within the Trust.

The Chair referred to the tremendous work being taken forward, despite the challenges presented by Covid-19, to ensure the organisation moved forward as planned in its 'Strategy to Transform' and she explained that, as the Assurance Report supported the presentation at agenda item 7, she suggested that discussion should take place during the presentation.

Mr Bloomfield thanked Ms Paterson for co-ordinating the report with input and assistance from Ms Sharpe and Ms Williamson. He said that Directors had been of the view that a paper setting out the overall Trust response would be more beneficial to members than a series of individual papers.

Continuing, Mr Bloomfield explained that the paper set out how the Trust managed the pandemic from the outset and how learning had been identified and applied through subsequent surges.

Members **NOTED** the Covid-19 Response Assurance Report.

The Chair invited the Chief Executive and Directors to proceed with the presentation.

## 7 **Covid-19 Update (TB21/01/2021/04)**

Introducing the presentation which supported the Covid-19 Response Assurance Report, Mr Bloomfield explained that it was intended to update members on the challenges faced by the Trust. He advised that the Trust was currently at REAP Level 3 which determined the service was under extreme pressure. Mr Bloomfield pointed out that this was an improvement on the REAP Level over the last number of weeks which had been at the Level 4 – the

highest level of escalation. He noted that the improvement in REAP Level had been because of improved cover due to the actions taken by the Trust. Mr Bloomfield also welcomed the fact that there had been a slight reduction in the number of staff unable to work due to Covid-19 reasons.

The Chair invited questions from members following the presentation which covered areas such as current organisational pressures; learning from previous Covid-19 waves; key business continuity decisions taken in January 2021; NIAS organisational response; supporting staff health and welfare; governance and assurance and HSCNI Covid-19 response.

Mr Haslett acknowledged that, despite the challenges faced by the Trust, performance had been much better than he had expected. He said that, speaking as a Non-Executive Director, he would like to thank all frontline and support staff for their commitment. He said that he had been particularly impressed by the welfare arrangements put in place.

Mr Ashford echoed Mr Haslett's comments and said that it was reassuring to see the extent of the work ongoing and the degree of success in difficult circumstances. He welcomed the fact that the command and control structure had changed as a result of learning from the first wave and that the current structure was fit for purpose. He sought confirmation that learning continued to be captured.

In response, Ms Byrne explained that the action taken during the first wave of Covid-19 and the subsequent learning changed the Trust's thought processes on how to approach further Covid-19 waves. She said that Silver Command now had the authority and autonomy to make decisions.

Continuing, Ms Byrne explained that, in the first phase, many issues had been escalated to NIAS Gold but having undertaken training, it was now expected that Silver Command would manage such issues.

She pointed out that the Trust would look back at the current phase and determine how it responded to current pressures. Ms Byrne advised that, given the challenges faced by the Trust in the last number of weeks in relation to transferring patients across the

region, extended Silver Command arrangements were put into place with hours of operation between 7am – 11pm.

Mr Ashford referred to the comparison between infection rates in England compared to NI and asked whether it was likely NI would experience a more intense period in the coming weeks.

Mr Bloomfield acknowledged that the projections and modelling being used by HSCNI had indicated the peak as being this week. He stressed that this was modelling and, as such, would be largely influenced by behaviours. He pointed out that the number of hospital admissions were slightly lower than the modelling had projected.

Agreeing with the points made by Mr Bloomfield, Dr Ruddell advised that he held weekly discussions with the Medical Directors of other services whose activity levels were significantly higher. He was of the view that NI's approach to putting early restrictions in place had yielded positive results. He acknowledged that the rest of the UK was seeing a sharp rise which was most likely associated with the easing of restrictions over the Christmas and New Year periods.

Dr Ruddell explained that the greatest pressure in NI had now moved to the hospital setting, and in particular those patients requiring ICU care and high level respiratory support over the coming weeks. He welcomed the vaccination programme in terms of NIAS staff and the wider public being able to receive the vaccine and said that NI was progressing well in terms of numbers being vaccinated.

The Chair said that she had been impressed by the Trust performance in relation to call answering and believed that this was an area which could be easily overlooked in the context of the other pressures facing the Trust. The Chair said that members would be aware of the work underway to ensure calls were answered in line with the five-second target and she commended all involved in these efforts. She noted that the maximum delay in answering a call had been 21 seconds and believed that this would go some way to alleviating public concern that patients would not be conveyed to hospital because of a perception of a focus on Covid-19.

Alluding to the actions taken to support Operations, Mr Bloomfield referred to the decision taken by the Senior Management Team

(SMT) in October to reduce the call handler course from twelve to five weeks. He explained that this decision had not been taken lightly and SMT at the time had stressed the importance of taking the views of the staff involved as well. Mr Bloomfield said that Dr Ruddell had advised on which elements of the truncated course should remain to ensure that those staff answering 999 calls had the necessary skillsets to do so safely. He advised that this had resulted in 20 additional call handlers being in post before Christmas which had proved essential given the outbreak in the Control Room from Boxing Day resulting in up to 30 members of staff having to self-isolate.

Dr Ruddell also pointed out that in addition to the recent action points, there had been many occasions over the past year on which the Trust had released staff from training and postponed training to allow staff provide operational support.

Ms Byrne referred to the assistance given by the PSNI and the NIFRS. She said that, following familiarisation training and receiving their vaccinations, the PSNI officers had commenced shifts in mid-January and, to date, had responded to 25 calls ranging from myocardial infarctions to a road traffic collisions. Ms Byrne reported that the NIFRS staff had recently completed their familiarisation training and had been vaccinated with a view to undertaking shifts in the near future. She acknowledged that, while assistance might not be required immediately, the necessary actions and arrangements had been put in place to support operational staff.

Dr Ruddell welcomed the fact that a significant number of nurses had applied for posts within CSD during the most recent recruitment.

Mr McNeill advised that, in November 2020, a number of PCS crews had volunteered to provide support to emergency response, working shift patterns as opposed to Monday-Friday. He said that, as recently as this week, further discussions had been held with Trade Union colleagues to determine whether it would be possible to increase that further in anticipation of further demand.

Mr Haslett said that, in reading the report, he had been struck by how beneficial the work previously carried out in relation to IPC had been to the Trust and he commended all involved. He paid

particular tribute to the cleaning operatives who were instrumental in ensuring a quick turnaround of vehicles to get back on the road.

Ms Charlton agreed with the comments made by Mr Haslett and mentioned the contribution made by Ms Finn in particular. She acknowledged that there was further work to be done around IPC but agreed that the foundations were now in place to build upon.

Ms Quirk referred to the arrangements which had been put in place for staff welfare and support and asked whether consideration had been given to continuing these beyond Covid-19.

Ms Lemon acknowledged that the area of health and wellbeing was important for staff and she said that up until now there had been limited resources to support this. She acknowledged that, while it was hoped to be able to continue with a number of practical arrangements on a long-term basis, the need for the development of peer support was clear when one took into account the increase in peer support activity during the pandemic. She added that peer supporters now described Covid-19 as a mental health pressure. Ms Lemon described the arrangements in place with Inspire and the potential need for psychological support for staff.

Mr Abraham referred to recent studies carried out in France which focussed on the links between Vitamin D deficiency and the likelihood of contracting Covid-19. He queried whether the Trust was doing any work around immuno-support and commented that it would be beneficial to support staff as much as possible

Ms Lemon said that, while she was not aware of anything being progressed within the service, it was her understanding that work around this was being led by the Chief Medical Officer and the Clinical Advisory Group. She indicated that any issues around the vaccine, occupational health support which related to individuals categorised as Clinically Extremely Vulnerable were being progressed on a regional basis. However she agreed to raise this issue in regional discussions.

Ms Charlton reported on the vaccination programme and advised that, up to 11 January 2021, 739 staff had booked their vaccinations. She explained that an online booking system had subsequently been introduced and it was not yet possible to

ascertain the numbers of NIAS staff who had used this to book their vaccination appointments.

Ms Charlton advised that 280 NIAS staff had tested positive and she acknowledged that there had been a large increase in staff testing positive in December and to date. She added that this was unique to NIAS and replicated patterns across other ambulance services.

Mr Haslett asked whether the DoH had given consideration to the timeframe for the production of the Trust's annual accounts.

Responding, Mr Nicholson indicated that the Trusts had sought clarification from the DoH around the production of Annual Reports and Accounts. He acknowledged that it would be helpful if the DoH adopted a similar pragmatic approach as they had in 2019-20 financial year.

Concluding discussion, the Chair thanked Directors for their input to the detail of the Assurance Report and said she had found it helpful having the presentation in advance of the meeting.

## **8 Update on EU Exit (TB21/01/2021/05)**

The Chair reminded members that the Trust Board had received a verbal update from Mr Billy Newton, Emergency Planning Officer, at its November meeting. She drew members' attention to the paper before them and invited Dr Ruddell to highlight any salient points.

Dr Ruddell advised that the implementation of EU exit on 31 December 2020 had had no tangible impact on NIAS operations. However he indicated that the situation with regard to supply chains and cross-border working of registered healthcare professionals would remain under review in partnership with DoH.

Members **NOTED** the update on EU Exit.

## **9 Finance Report (TB21/01/2021/06)**

At the Chair's invitation, Mr Nicholson presented the Trust Board Finance Report as at the end of November 2020.



Mr Nicholson reported that the Trust was forecasting a breakeven position at the end of 2020-21, subject to a number of assumptions which had been made in the Trust Financial Plan, around Agenda for Change, investment, Covid-19 costs and efficiency savings. He explained that, with the exception of Covid-19 costs, these issues had largely been resolved and the Trust continued to work with HSCB and other stakeholders to highlight emerging cost pressures and service changes with a view to achieving objectives and seeking to deliver financial balance.

Referring to capital expenditure, Mr Nicholson pointed out that the finance report to the November meeting had identified risks to a number of schemes and the Trust's ability to ensure appropriate business case approval, procurement and delivery by 31 March 2021. Mr Nicholson advised that, following a review of capital schemes, the Trust had surrendered £2.2 million of capital to the DoH. He added that £1.5 million of this related to fleet replacement which had been surrendered following advice from the DoH that it would not be able to consider the Fleet Replacement Business Case within a timescale necessary to allow procurements and delivery before 31 March 2021.

However, Mr Nicholson said the Trust had now been advised that the business case would likely be approved and he added Finance staff were now examining how vehicle chassis could be procured and resourced in the current year.

Concluding his report, Mr Nicholson drew members' attention to the detail covering Trust performance against prompt payment of invoices and advised that the Trust had achieved performance of 96.1% to date against a target of 95%.

The Chair thanked Mr Nicholson for his report and invited questions from members.

Mr Haslett acknowledged that, while the Trust had projected its spend in relation to Covid-19 to the end of the year, he did not get any sense from the report of the extent of the Trust's financial exposure. He said that, while he accepted the DoH would cover Covid-19 costs, the Trust was still expected to achieve savings of £2.6 million. Mr Haslett referred to capital

spend and was of the view that this was a significant amount of resources to commit within the last three months of the financial year.

In response, Mr Nicholson reported that the cost to the Trust in terms of the financial impact of Covid-19 would be a full-year effect of approximately £13 million. He acknowledged the fluidity and magnitude of these costs and pointed out that the Trust had received £2 million to date. Mr Nicholson said that the Trust continued to work with colleagues from the DoH, other Trust and the HSCB to unlock the mechanisms to release funding.

Continuing, Mr Nicholson explained that the Trust was also exploring other programmes to access further resources around Covid-19. He emphasised that the Trust had not been driven by the financial aspect of Covid-19 ensuring that the appropriate arrangements were put in place in the first instance.

Mr Nicholson agreed with Mr Haslett's point around the allocation of capital resources late in the financial year. He explained that the Trust had developed the business case in relation to fleet replacement and it was upon advice from the DoH/DF that they would not be able to review the business case within appropriate timeframes which had led the Trust to surrendering £1.5 million to the DoH. Mr Nicholson pointed out that the business case covered a five-year period and said the Trust would use the opportunity to revisit its expenditure profile. He indicated that the Trust would look at bringing forward the fleet replacement to ensure the twelve month profile between vehicles.

Mr Haslett suggested that it would be helpful to provide details of expenditure around consumables and PPE on a monthly basis to allow members gauge whether expenditure was on target and identify any trends.

Mr Nicholson said that work was ongoing to develop these areas for consideration by the Trust's People, Finance & Organisational Development Committee. He acknowledged that the presentation of the financial information presented to the Trust Board was in the format required by the DoH and the



HSCB and referred to staff and non-staff costs. He added that other expenditure largely fell within non-staff costs.

The Chair undertook to discuss with Mr Dennison the presentation of financial information to the People Committee and how this might feed into the Trust Board.

Mr Nicholson referred to earlier discussion around the maintenance and sustainability of a number of programmes implemented throughout the year. He acknowledged that many would continue and believed that the implications of the current year would be felt for many years to come. Mr Nicholson said that Dr Ruddell had alluded to the impact on training and indicated that he would refer to the impact of staff being unable to take annual leave during the year. He advised that work was ongoing at a regional level to assess the implications of that and how that might be managed moving forward.

Mr Nicholson reminded the meeting that the Trust operated within an annual planning cycle and that on 1 April 2021, the Trust would be required to achieve savings of £2.6 million as well as following the process to secure income for the new financial year.

The Finance Report was **NOTED** by the Board.

10 **Date of next meeting**

The next Trust Board meeting will take place on Thursday 4 March 2021. Arrangements to be confirmed.

The Chair indicated that she would be keen for the Board to meet on a face-to-face basis but only when it was safe to do so.

11 **Any Other Business**

There were no items of Any Other Business.

**THIS BEING ALL THE BUSINESS, THE CHAIR CLOSED THE PUBLIC MEETING AT 11.45AM.**

**SIGNED:** \_\_\_\_\_

**DATE:** \_\_\_\_\_

DRAFT

**TB/04/03/2021/02**





**TRUST BOARD – 21 JANUARY 2021**

		<b>INDIVIDUAL ACTIONING</b>	<b>UPDATE</b>
	<b>PUBLIC</b>		
1	Chair to discuss with Chair of People Committee how best to present financial information to Committee	NL	Ongoing
2	Raise linkages of Vitamin D deficiency to likelihood of contracting Covid-19 at a regional level and ascertain if there are any plans in place to explore this further	ML	Guidance has been issued by the Department of Health which had no direct implications for NIAS. Prescribing of Vitamin D remains the remit of an individual's own doctor who is best placed to identify those at risk.



**TB/04/03/2021/03**







**TRUST BOARD**

**PRESENTATION OF PAPER**

<b>Date of Trust Board:</b>	4 March 2021
<b>Title of paper:</b>	Self Service Business Intelligence (BI) Reporting Model
<b>Brief summary:</b>	<p>Members will be briefed on the key benefits of moving to a Self Service Business Intelligence Service Delivery Model.</p> <p>Ms Tracy Avery, Head of Information, will attend the meeting and provide members with a demonstration on the model.</p>
<b>Recommendation:</b>	<b>For Approval</b> <input type="checkbox"/> <b>For Noting</b> <input checked="" type="checkbox"/>
<b>Previous forum:</b>	SMT – 23 February 2021
<b>Prepared and presented by:</b>	Ms Tracy Avery, Head of Information Ms Maxine Paterson, Director of Planning, Performance & Corporate Services
<b>Date:</b>	25 February 2021



**TB/04/03/2021/04**





## TRUST BOARD

### PRESENTATION OF PAPER

<b>Date of Trust Board:</b>	4 March 2021
<b>Title of paper:</b>	People, Finance & Organisational Development Committee – Terms of Reference
<b>Brief summary:</b>	<p>NIAS Standing Order 4.1.1 states that '<i>The Trust shall determine the membership and Terms of Reference of Committees ...</i>'</p> <p>Trust Board approval is sought to the People, Finance &amp; Organisational Development Committee's Terms of Reference.</p>
<b>Recommendation:</b>	<p><b>For Approval</b> <input checked="" type="checkbox"/> <b>For Noting</b> <input type="checkbox"/></p>
<b>Previous forum:</b>	People, Finance & Organisational Development Committee – 2 December 2020
<b>Prepared and presented by:</b>	<p>Ms M Lemon, Interim Director of Human Resources Mr P Nicholson, Interim Director of Finance Mr J Dennison, Chair, People, Finance &amp; Organisational Development Committee</p>
<b>Date:</b>	25 February 2021





December 2020 Version 1

## **PEOPLE, FINANCE & ORGANISATIONAL DEVELOPMENT COMMITTEE - TERMS OF REFERENCE**

### **1 CONSTITUTION**

- 1.1 The Board hereby resolves to establish a Committee of the Board to be known as the People, Finance & Organisational Development Committee (The Committee).
- 1.2 The Committee is a non-executive Committee of the Board and has no executive powers, other than those specifically delegated in these Terms of Reference.
- 1.3 All procedural matters in respect of conduct of meetings of the Committee shall be in accordance with the Trust's Standing Orders.

### **2 MEMBERSHIP OF THE COMMITTEE**

- 2.1 Trust Non-Executive Directors that are to be included as members of this Committee will be nominated by the Trust Board Chair.
- 2.2 A Non-Executive Member of the Committee will be appointed Chair of the Committee by the Trust Board Chair.
- 2.3 In the absence of the Committee Chair, another Non-Executive Member may be temporarily appointed to that role by agreement of the Non-Executive Directors.
- 2.4 A quorum shall be two Non-Executive members including the Committee Chair.

### **3 ATTENDANCE AT MEETINGS**

- 3.1 The Director of Human Resources and the Director of Finance shall normally attend meetings.



- 3.2 The Chief Executive, other Directors, Assistant Directors and senior managers with responsibility for workforce and finance related functions will be invited to attend as appropriate.
- 3.3 The Board Secretary shall attend to the minutes of the meeting and provide appropriate support to the Committee Chair and Committee members.

## **4 FREQUENCY OF MEETINGS**

- 4.1 Meetings shall be held not less than three times a year, and where necessary can be conducted remotely using such as teleconference/video conferencing.

## **5 AUTHORITY**

- 5.1 The Committee will be responsible for assuring the NIAS Board that effective and regularly reviewed arrangements are in place to support Human Resources, Finance and Organisational Development functions within the Trust.
- 5.2 The Board will always retain responsibility for such control and will act after taking account of the recommendations and assurances of the Committee. The Committee, therefore, does not have the executive authority of the Board, but does have sufficient membership, authority and resources to perform its role independently and effectively.
- 5.3 The Committee is authorised by the Board to investigate any activity within its terms of reference. It is authorised to seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Committee.
- 5.4 The Committee is authorised by the Board to obtain external legal, clinical or other independent professional advice and to secure the attendance of individuals with relevant experience and expertise if it considers this necessary.





## 6 DUTIES

6.1 The duties of the Committee can be categorised as follows:

- Provide assurance to Trust Board in relation to all strategic issues relating to Human Resources, workforce and organisational development to deliver the Trust's Strategy, Plans and standards as determined by Trust Board.

These include those related to:

- Health and Wellbeing
- Learning and Development
- Employment Law
- Workforce Planning
- Recruitment and Retention
- Equality and Diversity
- Whistleblowing
- Pay and Conditions

This list is not exhaustive and focus will evolve as the work of the Committee develops.

- Provide assurance on the quality and effectiveness of targeted plans to support the organisation in delivering a positive patient centred culture, embedding the values and behaviours that the Trust aspires to demonstrate, including collective and compassionate leadership.
- Ensure consideration of an evidence based approach to workforce and organisational development work streams to include quantitative and qualitative information.
- To independently contribute to the Board's overall process for ensuring that the Trust Board delivers its statutory responsibility to break even. This includes:
  - To review in detail the financial strategy, so as to be able to confirm to the Trust Board the basis of acceptance.



- To review the financial monitoring information in sufficient detail to advise the Trust Board, with confidence, concerning the financial performance of the Trust.
- To keep Directors up-to-date regarding the financial outlook for the Trust, and to review the key financial assumptions used in estimating the projected position.
- To review achievement of cost improvements and income generation activities in line with the Trust Delivery Plan.
- To receive regular updates on actions taken by the Director of Finance to ensure the provision of effective and sound financial management and information.
- To ensure the Director of Finance provides assurance that adequate training is delivered on an on-going basis to budget holders to enable them to manage their responsibilities.
- To assist and recommend training for SMT and Board, as appropriate.
- To review and approve Capital Business Cases over £0.5m (£0.250m ICT).

## **7 REPORTING**

- 7.1 The minutes of Committee meetings shall be formally recorded. After each meeting, the Chair of the Committee shall make a report to the next Trust Board meeting; and at any point, draw to the attention of the Board any issues that require disclosure to the full Board, or require executive action.

The Chair shall liaise with the Chairs of other Committees on any issues or matter which may be relevant to their areas of responsibility.



## **8 OTHER MATTERS**

- 8.1 The agenda will be sent to members at least five working days before the meeting and supporting papers, wherever possible, shall accompany the agenda, but will be dispatched no later than three working days before the meeting, save in an emergency.

DRAFT



**TB/04/03/2021/05**





**TRUST BOARD**

**PRESENTATION OF PAPER**

<b>Date of Trust Board:</b>	4 March 2021
<b>Title of paper:</b>	Covid-19 Update
<b>Brief summary:</b>	<p>Members will receive a presentation which will provide an update on the current challenges facing the Trust in the context of Covid-19.</p> <p>The presentation will be shared with members prior to the Trust Board meeting.</p>
<b>Recommendation:</b>	<b>For Approval</b> <input type="checkbox"/> <b>For Noting</b> <input checked="" type="checkbox"/>
<b>Previous forum:</b>	n/a
<b>Prepared and presented by:</b>	Ms L Charlton, Director of Quality, Safety & Improvement Ms R Byrne, Director of Operations Ms M Paterson, Director of Planning, Performance & Corporate Services
<b>Date:</b>	25 February 2021





**TB/04/03/2021/06**





## TRUST BOARD

### PRESENTATION OF PAPER

<b>Date of Trust Board:</b>	4 March 2021
<b>Title of paper:</b>	<b>Corporate Plan 2020/21 Progress Report</b>
<b>Brief summary:</b>	<p>This Progress Report represents the collective position on progress delivery against our Corporate Plan.</p> <p>It represents a forecast on anticipated outcomes against our agreed corporate objectives by end of March 2021.</p>
<b>Recommendation:</b>	<b>For Approval</b> <input type="checkbox"/> <b>For Noting</b> <input checked="" type="checkbox"/>
<b>Previous forum:</b>	SMT
<b>Prepared and presented by:</b> <b>Date:</b>	Sarah Williamson, Transformation Manager Maxine Paterson, Director of Planning, Performance & Corporate Services  4 March 2021





# NIAS Corporate Plan 2020/21

Summary Report on Progress, Period Ending March 2021

## Introduction

The purpose of this report is to provide a summary of progress to date to NIAS Trust Board on how well the organisation is delivering the key actions identified within the annual Corporate Plan 2020/21. These actions are linked to the strategy: *Caring Today, Planning for Tomorrow: Our Strategy to Transform 2020-2026*.

## Rating

The BRAG (Blue, Red, Amber, Green) rating is a summary of progress to date and an indication of the assessment that actions identified in the Corporate Plan have been or will be delivered by the completion date. Where the rating is Red or Amber, the objective owner should make clear the remedial action being taken to ensure achievement by year-end and reasons for extension of timeline or any cancellation of action.

Traffic Light BRAG Rating Description Key	
<b>RED</b>	Action forecast to be delivered significantly (i.e. in excess of one quarter) outside completion date or beyond year-end.
<b>AMBER</b>	Action forecast to be (but no more than one quarter) of completion date.
<b>GREEN</b>	Action forecast to be delivered by the completion date.
<b>BLUE</b>	Action complete.

[Type here]

## Summary of Traffic Light Rating System (Period Ending 31<sup>st</sup> March, 2021)

The table below shows a summary of the Rating system assigned to the Actions within the corporate plan for the period ending 30 March 2021.

Traffic Light	Period Ending June 2020	Period Ending Sept 2020	Period Ending March 2021
Significant Delay		8%	23%
Risk Delay		44%	21%
On Track		44%	29%
Complete		4%	27%

At the end of the 2<sup>nd</sup> quarter of 2020/21, 48% of the actions within the Corporate Plan were reported as Blue/Green.

Projected to the end of March 2021, the anticipated Blue/Green ratings to achieve the projected in-year targets (i.e. actions anticipated to be complete by the end of the year) is 57%.

## Frequency of Reporting

The report will be produced on a quarterly basis for consideration by the Board and monitored more frequently by SMT and through internal accountability processes.

## Actions for Delivery by March 2021

Objectives	Key Actions	Lead Director	End of Month Due	BRAG Status	Comment
1.0 Delivering Care					
1.1 We will develop a supporting business case to secure funding in order to improve our service to patients through increased workforce and supporting infrastructure	Business cases to support full implementation of CRM to be submitted to DOH	Programme Director of CRM	January	On Track	Version 1 of SOC was submitted to the Department of Health in March 2020. Collaborative work undertaken with DOH, April to September.  Performance trajectory modelling requested. Version 2 was submitted in October 2020. DOH continue to review the Strategic Outline Case. Letter of support for CRM SOC submitted to DOH 18th January 2021.
1.2 We will develop an Improvement Plan to deliver the best possible response times to patients within existing resources.	Delivery of CAT1 implementation plan actions relating to dispatch, call stack management, and staff roles.	Director of Operations	August	N/A	See below for update against 3 separate elements for action:
	a) Improve Dispatch practices with Control Officers		August	Complete	Complete: Every day there is Cat 1 exception reporting in place with EAC managers. DCM working with Control Officers in relation to Dispatch Practices. Due the COVID-19 pandemic and social distancing progress has been slower than expected.

[Type here]



	b) Re-focus DCMs on incoming call stacks, Cat 1 performance and realign their workload		August	<b>Delay Risk</b>	Prioritised workload focusing on patient safety and performance. Due to the COVID-19 pandemic these meetings and forums have been supported by AACE remotely; Overhead Polling Screens been reinstalled in EAC to ensure oversight of Waiting Screen at changeover times. Completed by EAC manager.
	c) Re-configuration of RRV Dispatch desk		August	<b>On Track</b>	Work regarding this has been resumed.
	d) Recruitment of CSD Supervisors		December	<b>Significant Delay</b>	Further recruitment of CSD Officers is ongoing and training will be completed by 20 <sup>th</sup> November. Recruitment campaign to include Nursing is underway at present. CSD Supervisors has not started; No approved funding stream and alternative solutions are being explored.
1.3. We will commence a Patient Care Service Improvement Programme to improve the quality of our service for this important group of service users	Obtain approval to commence PCS Review Project	Director of Operations	June	<b>Complete</b>	SMT approval gained to commence review.  PCS Improvement Programme established with Assistant Director leadership. Project Manager appointed July 2020. SMT have given approval on the approach and remit of Review; interviews with Directors, DOH underway.
	Conclude PCS review and make proposals for improvement		December	<b>Significant Delay</b>	PCS Review Project Manager recalled to training post to enable contingency plan implementation during second wave of COVID-19 pandemic. First Objective extension anticipated to Q1 21/22

1.4 We will continue to embed our Appropriate Care Pathways developing safe alternatives to ED in order to reduce demand on frontline services increasing the levels of Hear and Treat and See and Treat practice	Implement a range of protocols for nursing homes to increase use of alternative care pathways	Medical Director	March	On Track	COVID-19 has had a major impact on the Care Home Setting. NIAS continues to engage at various levels and with stakeholders to optimise patient pathways including presentations on Nursing Home ECHOs etc.  The regional No More Silos project is advancing significant proposals to ensure Nursing Home access to medical support and appropriate decision-making. NIAS Clinical Directorate are inputting to these plans and workstream meetings as required.
	Demonstrable increase in Hear and Treat (1.5%) and See and Treat (1.5%) against 19-20 baseline		March	On Track	COVID-19 has had a major impact within NIAS with the introduction of Card 36. There is a significant increase in 'See and Treat' figures due to patients declining to attend hospital however this may be against NIAS clinical advice.  H&T increased only by 0.3%, against the background of reduced staffing levels and introduction of Card 36 with increased call volume to CSD from EAC due to reduced operational resources. Additional CSD staff took up post in November 2020 and figures will be monitored until year-end.
2.0 Our Workforce					
2.1 We will develop a comprehensive workforce plan for the whole organisation designed to support our strategy and to ensure our quality of service meets the performance trajectory requirements in terms of time and quality	Completion of workforce plan with Operational and CRM workforce requirements prioritised	Programme Director of Strategic Workforce	January	On Track	Work plan agreed with SMT. Prioritisation of frontline and CRM Workforce Plan for 2020-21, (circa 80% of workforce). Workforce Planning Team established and Terms of Reference agreed at SMT, October 2020. Workshops held with key stakeholders and reflected initial plan, (workbook based on 6 Step Model), presented to SMT October 2020. Assumptions agreed with SMT. Strategic HR Business Partner, Workforce Planning & Change appointed 19th October 2020. HRBP will collectively work with HRPTS, Finance and

[Type here]

					OPS D and AD to ensure that a Qualitative baseline is established. This will effectively contribute to the larger need for joint up reflective capacity planning. Skills for Health will QA workforce plan and provide related training for stakeholders.
2.2 We will develop a Recruitment and Selection Strategy, which will include the appropriate approach to support the delivery of a skilled and effective workforce.	Develop Strategy and Action Plan	Director of HR	December	Significant Delay	NIAS will seek to adopt and implement the regional HSC Recruitment and Selection Strategy
2.3 We will deliver a Clinical Education Plan with educational opportunities across a range of levels, qualifications, topics and specialties for the clinical workforce that aligns with the HCPC requirements for BSc-level paramedic education	Review the Training School structures to support the development of an education academy for NIAS	Medical Director	September	Significant Delay	<p>This work has been adversely impacted by the COVID-19 pandemic and a number of both related and unrelated staffing difficulties within the clinical education department</p> <p>This has led to a pause on this work, with a shift in emphasis, in an endeavour to optimise current staffing establishment to deliver existing priorities. It is anticipated this work will be picked up again in Q4.</p>
	Train up to 48 additional Paramedics. 96 AAPs and 48 ACAs with appropriate investment		March	On Track	The clinical education plan was implemented from Q1 but faced significant impact on delivery due to COVID-19 pandemic. Although the scheduled Paramedic programme was suspended for 5 months and 4 AAP courses were each similarly delayed for 2 months, programmes resumed with mitigating measures in place. Currently, 42 students on the Paramedic programme are due to graduate in February, 38 AAPs completed in July and another 44 AAPs are due to complete in January/February. 20 ACAs completed in July, a further 21 are in training (due to

[Type here]

					complete in December) and another course is scheduled for 24 In February/March.
2.4 We will continue to work with HSCB and Primary Care to develop a model for training Specialist Paramedics to work on a rotational basis in Primary Care	Receive feedback and signoff on business case		June	<b>Significant Delay</b>	This work has been impacted by the COVID-19 pandemic. Liaison with the HSCB Integrated and Primary Care team continues in order to confirm funding and this has been included in Rebuild funding requests with hope to commence Q1/2 21/22.
2.5 We will undertake a review of our Operations Structure to provide more effective support for staff, including on a 24/7 basis	Assess current approach to delivering operational structure review and deliver final recommendations	Director of Operations	September	<b>Significant Delay</b>	Phase 1 (Supervisors and management grades up to band 8) completed and report to be delivered by end of Mar 2021. Phase 2 (band 8 and above) to be completed by end of Q1 21/22.  Interim arrangements to be developed to deliver 16 hour extended on duty management out of hours cover for winter period. To be implemented by end of Sep 2020 through to Mar 2021.
2.6 We will develop a comprehensive Health and Wellbeing Strategy with a range of objectives and measurable outcomes to support the wellbeing of staff.	Develop Strategy and Action Plan	Director of HR	October	<b>Significant Delay</b>	This has been delayed however, significant learning has been achieved during Covid to support the development of this.
2.7 We will establish a new framework to ensure a best practice approach to the management of sickness absence	Develop Attendance Management Framework		September	<b>Significant Delay</b>	Resource supporting the review of OH service and Attendance Management in place.

[Type here]

2.8 We will develop a comprehensive strategy for the management of aggression towards NIAS staff	Conduct risk assessment and needs analysis for physical security measures	Director of Operations	September	Complete	Risk Assessment and needs analysis complete. Action plan in place
	Assess structure and resource requirements		December	On Track	Strategy drafted and shared with the Management of Aggression Working Group for initial comment. Workshop took place in October 2020. Violence Prevention and Reduction Strategy tabled at SMT February 2020.
	Conduct a staff and public awareness campaign		December	Delay risk	Strategy drafted and shared with the Management of Aggression Working Group for initial comment. Workshop took place in October 2020. Violence Prevention and Reduction Strategy tabled at SMT February 2020.
	Review Corporate Management of Aggression Policy & Procedures		March	Delay Risk	Work led by Area Manager and Risk Manager; significant completing priorities at this time. NIAS also await regional HSC policy update.
3.0 Organisational Health					
3.1 We will implement a COVID-19 Recovery and Learning Process to ensure effective transition to delivery of care and working arrangements, which respond to Government,	Develop plan for reinstatement of activities	Director of Planning, Performance and Corporate Services	June	Complete	A plan for re-instatement of activities was developed and is being implemented using on a risk based approach
	Collate learning obtained to feed corporate review of services and		July	Complete	Feedback to collate learning concluded August 2020 and this has been shared widely and with all staff

[Type here]

Public Health and other relevant guidance	improvement opportunities				
	Evaluation of learning advising key recommendations to inform improvement plan	Director of Safety Quality & Improvement	October	Complete	A range of leads from the organisation wide Recovery Group presented the Recovery Framework to Trust Board for their approval. A COVID-19 Learning Framework was approved and a COVID-19 Learning Report and Recommendations for Second Surge was presented to and approved by Trust Board
3.2 We will review the existing Directorate structures and responsibilities to ensure the most effective governance and management arrangements to support the delivery of services	We will establish an Organisational Development function	Chief Executive	June	Complete	New Organisational Restructuring Programme established under Programme Director for Strategic Workforce Planning
	Implement restructuring	Programme Director of Strategic Workforce	January	On Track	<p>Review of roles and responsibilities for each Directorate and related current teams undertaken and agreed at SMT, June 2020.</p> <p>Engagement Plan agreed with SMT and rolled out from June 2020. Restructuring Plan agreed by SMT and in progress. New Posts - SMT approved several Priority posts, these are progressing through related recruitments.</p> <p>SMT establishing a Scrutiny panel to progress priority recruitments. Corporate &amp; Clinical Governance Restructuring agreed and in progress.</p>

3.3 We will establish a Programme Management Framework in order to enhance our capacity to oversee implementation of our 6 year Strategy	Develop strategy for framework for corporate oversight	Director of Performance , Planning & Corporate Services	Sept	<b>Complete</b>	Strategy Implementation Methodology approved by Trust Board in August and plans underway regarding establishment of Strategy Implementing and Monitoring processes (with some contingency due to COVID-19 pressures)
3.4 We will initiate a new Organisational Culture Programme to take focused action to develop a culture of collective and compassionate leadership	Deliver Programme outline Plan	Director of HR	July	<b>Complete</b>	SMT presentation delivered. HSCLC support in place. Culture Audit launched and responses being gathered from staff at present.
3.5 We will review our Human Resources model with a view to establishing a revised model to meet organisational and workforce needs	AACE Review undertaken and report produced	Director HR	July	<b>Complete</b>	AACE review has been delivered and findings shared with SMT. Following this a service model review has commenced to establish model which will meet workforce needs in line with strategic objectives.
3.6 We will evidence compliance with internal audit recommendations	Complete follow up review in line with schedule	Director of Finance	September	<b>On Track</b>	A follow up of outstanding Internal Audit recommendations was completed as part of the 2019-20 Final Accounts.  This was updated for review by SMT in a Workshop in August 2020 and the position at 30 September 2020 formally reviewed by Internal Audit in September/October 2020

	Formally review audit compliance		March	On Track	<p>Managers receive final Internal Audit reports for implementation.</p> <p>Managers receive Follow-up Outstanding Audit Recommendations spreadsheet twice a year for updates for Mid-Year and Year-End internal audit review.</p> <p>SMT Audit Workshops are held leading up to Mid-Year and Year-End Internal Audit reviews Internal Audit review outstanding audit recommendations twice a year at Mid-Year and Year-End.</p> <p>External Audit review Internal Audit reports and outstanding audit recommendations as part of annual accounts audit process.</p>
<b>4.0 Quality Improvement</b>					
4.1 We will develop a new Quality and Safety strategy that focuses on continual improvement, measuring and evidencing the quality of our services for our patients.	Engage with staff and service users to inform the development of strategy for Quality, Safety and Improvement	Director of Safety, Quality & Improvement	October	On Track	Quality and Safety Strategy is in development in Q4; SMT and senior staff to be issued draft proposals for Quality Targets for 2021/22, which have been developed, by Quality and Safety and Clinical Directorates.
	Deliver Strategy for Trust Board for approval		November	On Track	This is anticipated for presentation to Trust Board in March 2021.



	Achieve quality improvement targets at level 1 and 2 as outlined in Attributes Framework		March	<b>Significant Delay</b>	<p>A further Level 2 QI training programme was launched in partnership with SET however due to lack of QI Lead post, operational pressures and COVID-19 pressures the QI targets for level 1 and 2 are not feasible for NIAS to meet in year and an improvement trajectory plan will be required in 21/22.</p> <p>A Quality Lead JD is being finalised for job evaluation. Recruiting a postholder will provide additional capacity for provision of in-house training or commissioning of additional courses.</p>
4.2 We will implement a Programme of transformation and improvement for our Emergency Ambulance Control Room	Implementation of Demand Management Plan	Director of Operations	September	<b>Significant Delay</b>	<p>A project group supported by AACE has been identified and core members agreed.</p> <p>SEMT endorsed the approved approach on 7 July 2020. Progress with the DMP has been delayed due to the COVID-19 pandemic and will recommence Q1 21/22.</p>
	Introduction of new modules to enhance HCP bookings and Inter Hospital Transfer (IFT)		September	<b>Significant Delay</b>	<p>A project group supported by AACE has been identified and core members agreed.</p> <p>SEMT endorsed the approved approach on 7 July 2020. Progress with the DMP has been delayed due to the COVID-19 pandemic and will recommence Q1 21/22.</p>
	Deliver 90% shift coverage to meet demand patterns and facilitate staff well-being		December	<b>Significant Delay</b>	<p>Working Time Solutions are working to support NIAS with this. Project meetings have been arranged. Project completion has been targeted for June 2021.</p>

	Commence Replacement of Telephony System		December	Delay risk	Telephony business case complete however delay from Department of Finance and on that basis have sought approval to re-profile funding to 2021/22.
	Replacement of Integrated Command and Control System, CAD and Radio system		March	Complete	Radio roll out commenced.
4.3 We will demonstrate an improvement in our measurement against Ambulance Quality Indicators to better evidence the safety and quality of our patient care	Review current AQI processes and engaging with front-line staff	Medical Director	November	Complete	A desktop review of the current process for collecting AQIs has been carried out by the new Assistant Clinical Director.
	Test new processes in preparation for ePCR rollout		November	Significant Delay	Initial testing with NIAS staff has begun but this has been limited due to pressures associated with COVID-19.
	Test revised accountability processes for AQIs with local engagement		January	Significant Delay	Due to COVID-19 and historic inefficiency if the historic system, the current AQI measurement has been stopped. Director of Safety & Quality has taken a lead on the framework for oversight of National AQI measures. These are being developing into the REACH project, which at present is on hold due to COVID-19.
	Deliver assurance framework incorporating national best practice for monitoring and reporting key clinical metrics	Director of Safety, Quality & Improvement	March	Delay Risk	An early draft of Performance Management Framework has been agreed by SMT. This will include an Integrated Quality and Performance Report, which will report on these metrics. This will be agreed by Director of SQI and Planning & Performance Directorate. The full report is likely to be in place end of Q1 21/22.

4.4 We will implement an Improvement plan to develop in our processes in Safeguarding, in partnership, with social care services across HSC	Produce Safeguarding Policies and Procedures	Director of Safety, Quality & Improvement	June	Significant Delay	Safeguarding policy and procedure are in draft with anticipated completion early 21/22.
	Appoint Safeguarding Lead		October	On Track	Safeguarding Lead job advertised November 2020. Due to COVID-19 pressures, interviews have not yet taken place.
	Implementation of system to monitor, audit, investigate, report and provide assurance reporting on adherence to safeguarding referral process		December	Complete	Safeguarding Improvement Plan in place with agreed measures to track and monitor quality of safeguarding referrals. Furthermore, a Weekly Safeguarding Review Meeting is held to provide assurance on all referrals made. Safeguarding Pathway in place. Incidents reported on DATIX and followed up by seconded Paramedic and EMT
4.5 Develop an organisational performance management framework to measure improvement and provide corporate governance and assurance	Perform landscape review and audit of information	Director of Performance, Planning & Corporate Services	September	Complete	Full review of existing information landscape complete. Several actions are being taken forward to restructure department and fill existing vacancies to manage demand and optimise governance and data processing.
	Determine information requirements for performance reporting		October	On Track	A new Head of Information took up post in November 2020 and will be instrumental to implementation of new approaches to performance reporting. This is now predicted for completion by Q4 20/21

[Type here]

	Develop overarching strategy and approach to performance management		October	Delay Risk	Draft Performance Framework and Performance Scorecard has been agreed by SMT in November 2020. Plans for a co-production sessions with senior managers and clinicians and service users were put on hold due to COVID-19 pressures. Further engagement process to commence in February/March 2021.
	Deliver performance dashboard for corporate performance		December	On Track	A new Head of Information took up post in November 2020 and will be instrumental to implementation of new approaches to performance reporting. This is now predicted for completion by Q4 20/21.
<b>5.0 Digital Enablers</b>					
5.1 We will continue the implementation of the REACH programme building connectivity across HSC in the mobile environment	Roll out new DTR radios c1000 personal issue devices to front line staff	Medical Director	October	Delay Risk	90% of vehicle radios completed Nov 2020 Handhelds to follow.
	Complete all phases of ePCR roll-out		March	Delay Risk	Go Live date paused due to Ops pressures and inability to access staff for training Recommence Jan /Feb 2021, Go Live.
5.2 We will establish arrangements to improve business intelligence through data warehousing, business intelligence tools and best practice	Agreement to proceed DHCNI /BSO	Director of Performance Planning & Corporate Services	July	Complete	Informally agreed to proceed.
	Requirements scoped and agreed; Business Case submitted to Digital Health Team		Dec	Significant Delay	HSCB commissioned of BSO to undertake initial scoping work. BSO have advised their capacity to manage this currently is constrained- therefor this is delay risk.
	Proof of Concept to Support Business Intelligence Tool completed		September	On Track	Will be incorporated in BC for Data warehouse.

[Type here]

5.3 We will consolidate and refresh our technology infrastructure to maintain service and improve resilience	CAD Hardware replacement including Disaster recovery in the regional data centres		October	Delay Risk	CAD Hardware replaced at NIAS and DR Hardware currently in place at Site 5, NIAS. Footprint established in BSO Data Centre and rack under construction.
	Telephony business case approved by DOH, procurement completed		March	Significant Delay	Second set of DOH BC comments addressed and due to be submitted w/c 9/11. Likely delay from Department of Finance and on that basis have sought approval to re-profile funding to 2021/22.
	Complete active directory configuration to access federated services		March	Delay Risk	Verbal approval on COVID-19 recovery bid for this year funding.
	Deliver benefits realisation of Site 5		March	Delay Risk	Full benefits realisation has been Impacted by COVID-19 however, as a contingency site, it has been very useful.
6.0 Our Infrastructure					
6.1 We will develop a suite of supporting infrastructure strategies for Estates and Fleet in year one to address pressing issues.	Delivery of Fleet replacement business case 2020- 2025	Director of CRM	March	Complete	Fleet Business case for rolling five-year replacement programme developed and on target for submission to the DOH October 2020. Five-year fleet replacement Business case total with a value £ 22,657k has been approved by DOH 25 <sup>th</sup> Jan 2021.
	Draft a Fleet Strategy 2020 – 2025		January	On Track	A Draft Fleet Strategy 2020-25 completed. Presented to Trust Board November 2020. Five-year fleet replacement Business case total value £ 22,657k approved by DOH 25 <sup>th</sup> Jan 2021.
	Estates Strategy to be finalised following engagement process		March	On Track	Consultation document for operational Estates configuration (Hub and Spoke Model) to be developed. Estate condition and functional suitability surveys delayed due to COVID-19. Modelling to confirm Hub and spoke configuration

[Type here]

					commenced September 2020. Surveys scheduled to commence February 2021.
6.2 We will open a new training and administration facility for Emergency Ambulance Control.	Delivery of delivery of training and administration function from new facility	Director of Operations	December	Delay Risk	The new Training and Administration facility was opened early in order to provide a contingency site for EAC. At present due to COVID-19, this is being used as a contingency Control Room, which means training spaces for Control have had to be outsourced.
6.3 We will enhance Cyber Security to ensure we improve preparedness, resilience and response capability.	Develop Information Security Governance Framework	Director of Planning, Performance & Corporate Services	October	Significant Delay	Aligned to DHCNI Governance as part of NIAS Service Delivery review. Implementation plan to be developed.
	Review ICT Delivery Model		December	Complete	This was agreed by SMT in October 2020 and was presented to Trust Board in November 2020.
	Develop framework for Policies, Standards and Procedures		March	Delay Risk	Align to DHCNI Governance as part of NIAS Service Delivery review. Implementation plan to be developed.
6.4 We will engage with the DOH-led approach to exit from EU	Implement DoH recommendations	Medical Director	March	On Track	NIAS continue to attend DoH hosted exit meetings and workshops that have been in place since Feb 2018.
<b>7.0 Communication and Engagement</b>					
7.1 We will develop a new Communications Strategy	By Jul: Benchmarking exercise of ambulance and HSC Trust Communication Strategies with particular focus on use of digital and online channels	Director of Planning, Performance & Corporate Services	July	Complete	Benchmarking of communication functions within Ambulance Services concluded.

	By Aug: Staff and stakeholder engagement process to inform communications strategy.		August	<b>Significant Delay</b>	COVID-19 demands on the small Communications resource in NIAS has limited the ability to engage a range of staff and stakeholders to date. This is now planned for February 2021 but may slip further
	Draft Communications Strategy for Trust Board Approval		December	<b>Delay Risk</b>	This is planned for Trust Board presentation in March 2021 but this is dependent on Covid-19 pressures.
7.2 We will review existing processes around the Knowledge and Skills Framework and implement a new approach to staff appraisal and personal development reviews	Establish a project team and review NIAS Appraisal process	Programme Director of Strategic Workforce	September	<b>Complete</b>	SMT agreed on 7 <sup>th</sup> July 2020 that a project team was not required.
	Benchmark Ambulance Sector Appraisal and Clinical Appraisal systems		December	<b>Complete</b>	Benchmarking Complete. Engagement Plan agreed by SMT October 2020 and due to commence November 2020.
	Develop and agree NIAS Appraisal system and roll out in line with agreed timeframe		March	<b>On Track</b>	Pre consultation/engagement Oct/Nov2020 held with TU Branch Secretary in advance of staff engagement. Engagement finalised. Benchmarking finalised. Next steps were to be agreed with SMT during January and Consultation thereafter. This was deferred due to Business Continuity arrangements and Consultation to commence in March 2021.
7.3 We will develop the range of ways Service users can give us feedback and be involved in service development	Introduce Trust wide Online User Feedback tool Care Opinion	Director of Safety, Quality & Improvement	July	<b>Complete</b>	Launched 3 <sup>rd</sup> August 2020.

[Type here]

	Introduce reporting on PCE through relevant committees and Trust Board as appropriate		December	<b>Delay Risk</b>	PCE reporting has been agreed as part of the new Trust Board committee structure and inclusion in relevant Organisational performance reporting. A new post to be advertised in Q4 2020/21 will support the capacity to implement this.
--	---	--	----------	-------------------	---



**TB/04/03/2021/07**



# **NORTHERN IRELAND AMBULANCE SERVICE**

## **TRUST BOARD FINANCE REPORT**

---

Director of Finance  
January 2021 (Month 10)

## FINANCIAL PERFORMANCE

### Introduction

The purpose of this report is to provide Trust Board with an update on the financial position of the Trust. This includes an update on the requirements not to overspend against Revenue Resource Limits (RRL) and Capital Resource Limits (CRL), and also the requirement to pay non HSC trade creditors in accordance with the Better Payments Practice Code and Government Accounting Rules.

The report includes a number of key risks and assumptions to the achievement of these requirements.

### Financial Breakeven

The Trust is currently reporting a forecast breakeven position for the month ending 31 January 2021 (Month 10), subject to key risks and assumptions.

### Financial position at the end of January 2021 (Month 10)

Financial Breakeven Assessment (£k)	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar
Staff Costs			14,828	19,907	23,759	28,801	36,064	40,931	46,113	51,131		
Other Expenditure			10,590	13,489	17,464	20,183	25,471	29,517	33,392	37,962		
Expenditure Total			25,418	33,396	41,223	48,984	61,535	70,448	79,505	89,093		
Income			200	259	318	336	383	443	500	548		
Net Expenditure			25,218	33,137	40,905	48,648	61,152	70,005	79,005	88,545		
Net Resource Outturn			25,218	33,137	40,905	48,648	61,152	70,005	79,005	88,545		
Revenue Resource Limit (RRL)			24,968	32,804	40,489	48,148	61,152	70,005	79,005	88,545		
Surplus/(Deficit) against RRL			(250)	(333)	(416)	(500)	0	0	0	0	0	0

### Forecast financial position at the end of March 2021

The Trust is also currently forecasting a breakeven position at the end of 2020-21, subject to a number of assumptions particularly in respect of Agenda for Change, investment, Covid-19 costs and efficiency savings. With the exception of Covid-19 costs, these issues have largely been resolved. The forecast costs in relation to Covid-19 during the year are of the order of £13m across a range of areas to support the Trust's response to the pandemic. These include additional staff costs to maintain and enhance cover and increased Independent and Voluntary Ambulance Service provision. Additionally, there have been increased costs in relation to cleaning, personal protective equipment and staff welfare. The Trust awaits the formal allocation of funds for a number of areas of expenditure and has received positive indications from HSCB and DoH that these will be provided. The Trust continues to work with HSCB and DoH to finalise the resource requirements in relation to Covid-19 and other financial pressures and deficits for the current year and beyond.

## NIAS Trust Board Budget Report at January 2021

(£ 000s)	FYB	YTD		
		Budget	Actual	Variance
<b>Chief Executive's Office</b>				
Payroll	562	452	449	3
Non-Payroll	430	419	412	7
<b>Chief Executive's Office Total</b>	<b>993</b>	<b>871</b>	<b>861</b>	<b>11</b>
<b>Director of Finance</b>				
Payroll	1,266	1,098	1,069	28
Non-Payroll	586	530	524	6
<b>Director of Finance Total</b>	<b>1,851</b>	<b>1,627</b>	<b>1,593</b>	<b>34</b>
<b>Director of HR</b>				
Payroll	2,178	1,815	1,796	19
Non-Payroll	1,020	897	878	19
<b>Director of HR Total</b>	<b>3,198</b>	<b>2,712</b>	<b>2,675</b>	<b>38</b>
<b>Dir of Ops (incl Divisions &amp; RCC)</b>				
Payroll	64,637	54,411	53,284	1,127
Non-Payroll	18,575	17,050	18,312	(1,262)
<b>Dir of Ops (incl Divisions &amp; RCC) Total</b>	<b>83,212</b>	<b>71,461</b>	<b>71,596</b>	<b>(135)</b>
<b>Medical Director</b>				
Payroll	9,656	8,685	8,681	4
Non-Payroll	1,933	1,862	1,847	14
<b>Medical Director Total</b>	<b>11,590</b>	<b>10,547</b>	<b>10,528</b>	<b>19</b>
<b>Director of Safety, Quality &amp; Improvement</b>				
Payroll	220	161	157	4
Non-Payroll	103	101	101	0
<b>Director of Safety, Qual &amp; Imp Total</b>	<b>323</b>	<b>262</b>	<b>258</b>	<b>4</b>
<b>Director Of Plan, Perf &amp; Corp</b>				
Payroll	1,250	1,021	1,011	10
Non-Payroll	685	591	571	20
<b>Director Of Plan, Perf &amp; Corp Total</b>	<b>1,936</b>	<b>1,612</b>	<b>1,582</b>	<b>30</b>
<b>NIAS Total Payroll</b>	<b>79,769</b>	<b>67,643</b>	<b>66,448</b>	<b>1,194</b>
<b>NIAS Total Non-Payroll</b>	<b>23,333</b>	<b>21,450</b>	<b>22,644</b>	<b>(1,194)</b>
<b>NIAS Total</b>	<b>103,102</b>	<b>89,093</b>	<b>89,093</b>	<b>0</b>

*Figures last updated: 24/02/2021 13:32*

Underlying this overall financial forecast is a complex budgetary position. There are a range of vacancies creating underspends against the pay budget. The level of underspend is reduced by overtime costs to provide operational cover. There are also levels of absence due to sickness and Covid-19 that can create corresponding financial pressures. Expenditure on Voluntary and Private Ambulance Services (VAS/PAS) to offset these vacancies and maintain cover and performance is creating a corresponding pressure on the non-pay budget. NIAS is also coordinating some VAS/PAS activity on behalf of other HSC Trusts. The cost of this is being recharged to the respective HSC Trust.

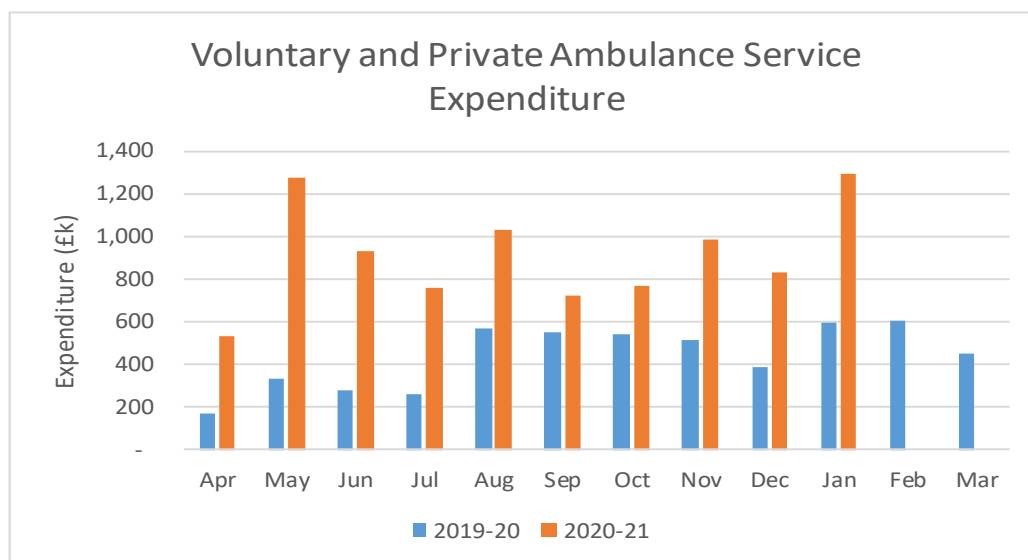
The Trust is required to identify savings proposals to address a forecast £2.6m savings requirement in 2020-21. Plans totalling only £1.6m from a range of non-recurrent measures were identified at the start of the year. A further £0.5m support has been provided by HSCB and a further £0.5m of non-recurrent NIAS measures identified later in the year linked to the capacity to release staff from operational duties.

There are a number of income assumptions included in this financial position. The Trust continues to work with HSCB and other stakeholders to highlight emerging cost pressures and service changes with a view to achieving objectives and maintaining financial balance.

## Voluntary & Private Ambulance Services (VAS/PAS)

The Trust has benefited from significant additional funds in 2020-21 as part of the response to Covid-19. A large proportion of these funds has been applied to additional support from VAS/PAS to maintain and enhance ambulance provision during this difficult period. The Trust is thankful for the support that VAS/PAS has given NIAS and HSC during this time.

Expenditure on VAS/PAS in 2019-20 was £5.2m. Expenditure for the first ten months of 2020-21 is £9.1m. Expenditure by month is shown below.



## Forward Look

Looking forward to 2021-22, there are uncertainties as to the longer-term impact of Covid-19 and the funding available to respond to it. In addition to issues around Covid-19, the publication of the Northern Ireland 2020-21 Draft Budget on 18 January 2021 has identified significant financial challenges across the public sector in Northern Ireland. This will inevitably have an impact on HSC and NIAS in the future.

The Trust will continue to work closely with other HSC organisations and with HSCB and DoH colleagues to refine and develop a financial plan for the HSC as a whole and for NIAS in order to best address or mitigate against the various risks and challenges presented by the Draft Budget.

The Trust continues to work with HSCB and DoH to finalise the resource requirements in relation to Covid-19 and other financial pressures and deficits for the current year and beyond.

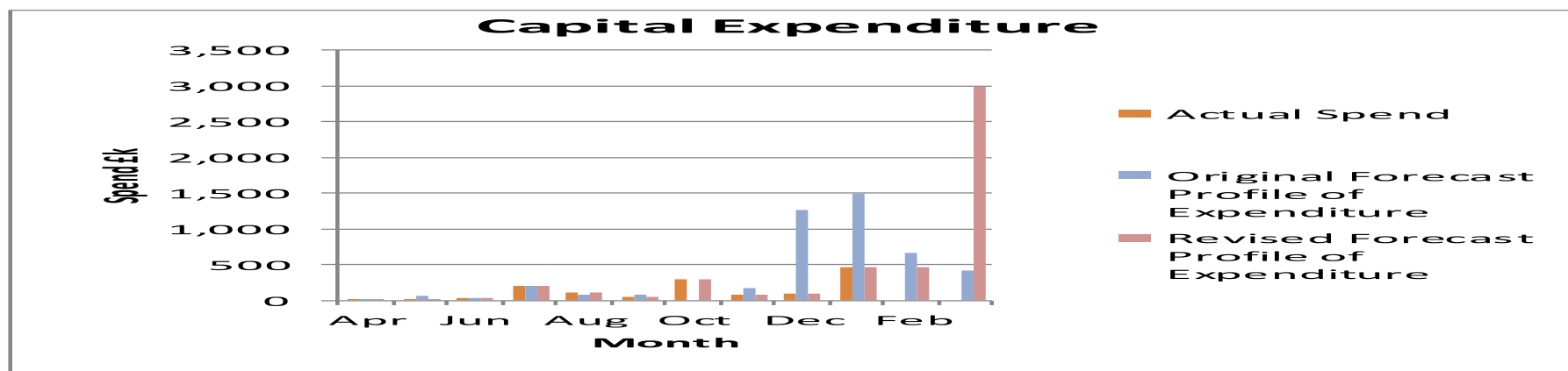
## Capital Spend

The Trust has received a Capital Resource Limit (CRL) allocation of £4.803m (previously £3.330m). Additional allocations are in respect of ICT Schemes and also a reinstatement of some funds following the approval of the Fleet Replacement Business Case. Capital resources of £1.5m were returned in December 2020 following advice from the DoH that the Fleet Replacement Business Case would not be approved within the timescale necessary to allow procurement and delivery before 31 March 2021. The Fleet Replacement Business Case 2020-2025 was subsequently approved in January 2021.

There have been a number of issues that have impacted on the delivery of the full programme of expenditure since the beginning of the year. A number of these risks, specifically in relation to the deliverability of schemes, remain. These risks within schemes are constantly under review as part of the efforts to ensure delivery.

The profile of expenditure towards the end of the financial year is due to a number of factors, including business case approval, the availability of funds, procurement timescales, supplier capacity, internal capacity, project risks and lead times. Significantly, expenditure on fleet is profiled to the end of the financial year to maintain a smooth fleet age profile. The Trust continually reviews capital schemes to minimise any risks towards the end of the financial year.

Cumulative Capital Spend (£k)	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Fleet & Estate	14	6	38	197	113	39	(82)	2	2	132			460
ICT Schemes	0	0	0	0	0	7	382	62	94	221			766
Backlog Maintenance	0	0	0	0	0	0	0	10	0	110			120
Actual Spend	14	6	38	197	113	46	300	74	96	463	0	0	1,346
Original Forecast Profile of Expenditure	14	72	38	197	73	73	0	170	1,265	1,500	670	414	4,487
Revised Forecast Profile of Expenditure	14	6	38	197	113	46	300	74	97	463	466	2,990	4,803



## Prompt Payment of Invoices

The Trust is required to pay non HSC trade creditors in accordance with the Better Payments Practice Code and Government Accounting Rules. The target is to pay 95% of invoices within 30 calendar days of receipt of a valid invoice, or the goods and services, whichever is the latter. A further regional target to pay 70% (increased from 60%) of invoices within 10 working days (14 calendar days) has also been set.

Performance by number of invoices paid for each of these measures is shown below. A range of plans are in place to improve and maintain performance in this area. As aged invoices are cleared and paid, performance between months can vary.

Number	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	YTD Cum	Target
<b>Total bills paid</b>	2,396	2,580	3,354	2,648	2,521	2,457	2,923	2,828	2,971	2,958			<b>27,636</b>	
<b>Total bills paid within 30 calendar days of receipt of undisputed invoice</b>	2,320	2,480	3,212	2,601	2,446	2,398	2,795	2,717	2,817	2,781			<b>26,567</b>	
<b>% bills paid on time 30 days</b>	96.8%	96.1%	95.8%	98.2%	97.0%	97.6%	95.6%	96.1%	94.8%	94.0%			96.1%	>95%
<b>Total bills paid within 10 working days (14 calendar days)</b>	2,093	2,165	2,635	2,277	2,257	2,190	2,468	2,334	2,525	2,100			<b>23,044</b>	
<b>% bills paid on time 10 days</b>	87.4%	83.9%	78.6%	86.0%	89.5%	89.1%	84.4%	82.5%	85.0%	71.0%			83.4%	>70%



**TB/04/03/2021/08**





## TRUST BOARD

### PRESENTATION OF PAPER

<b>Date of Trust Board:</b>	4 March 2021
<b>Title of paper:</b>	Information Governance Policies and Procedures and Management Framework
<b>Brief summary:</b>	<p>The following refreshed Policies and Procedures are being presented for noting to ensure NIAS remains compliant with UK Data Protection and Information Governance Legislation:</p> <ol style="list-style-type: none"><li>1) Confidentiality Code of Conduct</li><li>2) Data Protection Impact Assessment Policy</li><li>3) Data Protection Policy</li><li>4) Data Protection Rights Procedure</li><li>5) Data Quality Policy</li><li>6) Freedom of Information</li><li>7) Information Asset Policy</li><li>8) Information Disclosure and Transfer Policy</li><li>9) Information Governance Policy</li><li>10) Information Lifecycle Management Policy</li><li>11) Information Risk Management Policy</li><li>12) Information Sharing Policy</li><li>13) Retention and Disposal of Information Schedule</li><li>14) Safe Haven Policy</li></ol> <p>Whilst these policies are being noted at Trust Board, we will present an implementation and dissemination plan to ensure all employees are aware of their roles and responsibilities and report back on progress at subsequent Audit Committee.</p>



	Furthermore, we have included a new Governance and Assurance Framework designed to enhance Information Governance compliance and provide assurance to SMT, the Audit Committee and Trust Board.
<b>Recommendation:</b>	<b>For Approval</b> <input type="checkbox"/> <b>For Noting</b> <input checked="" type="checkbox"/>
<b>Previous forum:</b>	SMT – 23 February 2021
<b>Prepared and presented by:</b>  <b>Date:</b>	Ms Tracy Avery, Head of Information Ms Maxine Paterson, Director of Planning, Performance & Corporate Services  25 February 2021

## Background

To ensure compliance with Data Protection and Information Governance (IG) legislation and regulations. All employees should have a clear understanding of their role and accountability for ensuring compliance. To support staff, expectations and best practice processes when handling, processing and managing information should be clearly communicated and accessible to all staff.

To ensure compliance and best practice, HSC organisations provide staff with access to a wide range of Information Governance Policies. This provides the foundation for training and monitoring of IG practices, with key findings being collated and reported to the Chief Executive, Senior Information Risk Owner and the Data Protection Officer for assurance and risk mitigation. However, currently in NIAS, these policies and procedures are limited with restricted access to staff, making compliance and assurance difficult to monitor and report, along with the identification and mitigation of risks/potential breaches.

## Proposal

To support staff across NIAS and ensuring our compliance, Policies and Procedures have been drafted (appendix one) in a consistent corporate template and will be submitted to Trust Board for noting and implementation across NIAS. These will be uploaded to SharePoint and shared with Directors for dissemination and incorporated to a plan to improve information governance across NIAS.

Additionally, a governance framework has been developed for noting to ensure effective monitoring, compliance and assurance in relation to Information Governance, IT Security and Clinical Data usage (appendix two).

## Appendix One

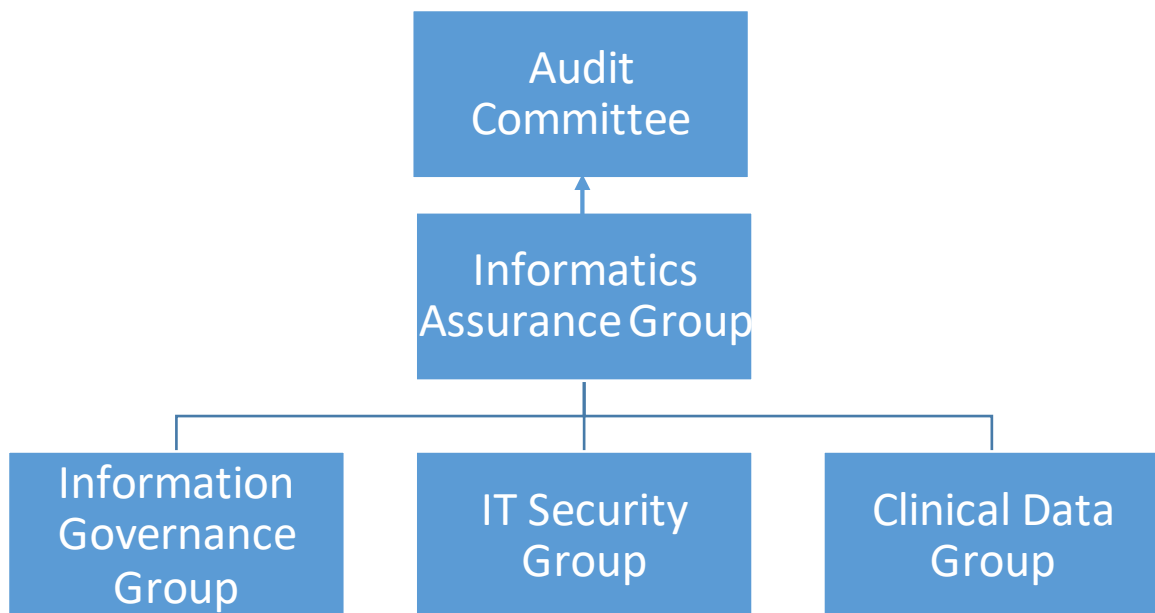
List of Policies and Procedures, including each policy or procedure:


- 1) Confidentiality Code of Conduct
- 2) Data Protection Impact Assessment Policy
- 3) Data Protection Policy
- 4) Data Protection Rights Procedure
- 5) Data Quality Policy
- 6) Freedom of Information
- 7) Information Asset Policy
- 8) Information Disclosure and Transfer Policy
- 9) Information Governance Policy
- 10) Information Lifecycle Management Policy
- 11) Information Risk Management Policy
- 12) Information Sharing Policy
- 13) Retention and Disposal of Information Schedule
- 14) Safe Haven Policy





## Appendix Two


Management Framework Overview and terms of reference.



  
IAG Terms of  
Reference.docx

  
IGG Terms of  
Reference.docx

  
ITSG Terms of  
Reference.docx

  
CDG Terms of  
Reference.docx





## CONFIDENTIALITY CODE OF CONDUCT

### Links

The following documents are closely associated with this policy:

- Data Protection legislation
- Data Protection Policy
- Data Protection Rights Procedure
- The Information Governance Review (Caldicott2) (2013)
- Common Law Duty of Confidentiality
- Human Rights Act 1998
- Retention and Disposal of Information Schedule
- Safe Haven Policy
- Freedom of Information Act 2000
- Freedom of Information Policy and Procedure
- Archiving Procedure
- Research, Management and Governance Policy
- Untoward Incident Reporting Policy
- Information Sharing Policy
- Disciplinary Policy
- Police Interviews & Witness Statements Standard Operating Procedure
- Information Request Procedure
- HSC Code of Practice on Confidentiality
- HSC Care Record Guarantee
- A guide to confidentiality in health and social care (HSCIC 2013)
- HSC Constitution (2013)
- PRF Storage Standing Operating Procedure
- Social Media Policy
- Research Management and Governance Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy and procedure for NIAS

## Contents

<b>Date</b>	1
1. Introduction	5
2. Objectives	6
3. Scope	7
4. Definitions	7
4.1 Confidential information	7
4.2 Personal confidential data (PCD)	7
4.3 Special Category Data	8
4.4 Processed	8
4.5 Rights of the Data Subject	8
4.6 Data Protection legislation	8
5 Responsibilities	8
5.1 Chief Executive Officer	8
5.2 Senior Information Risk Owner (SIRO)	8
5.3 Caldicott Guardian	9
5.4 Head of Information Governance	9
5.5 Data Protection Officer	9
5.6 Corporate Services Compliance Manager	9
5.7 Information Asset Owners (IAOs)	9
5.8 All staff	9
6 Legal considerations	9
6.1 Data Protection legislation	10
6.2 Freedom of Information Act 2000 (FOI)	11
6.3 Human Rights Act 1998	12
6.4 Common Law Duty of Confidentiality	12
6.5 Caldicott Principles (2013) – The Information Governance Review	12
7 Protecting information	13
8 Storage of Patient Report Forms (PRFs)	14
9 Disposal of confidential information, including archiving	14
10 Information sources	14
11 Requests for information	14
11.1 Requests for personal information from staff and patients	15
11.2 Requests from the police	15
11.3 Requests from coroners	15
11.4 Requests for non-personal information	15
11.5 Requests from solicitors	16
11.6 Requests for information on other individuals	16
11.7 Telephone enquiries	16
11.8 Requests from overseas	17
12 Patient choice	17
13 Patient consent and National Data Opt-Out	18
14 Abuse of privilege	18
15 Social networking sites	18
16 Adverse incident reporting	19
17 Working in an open plan environment	19
18 Working from home	20
19 Specific departmental considerations	21
19.1 Operational staff	21
19.2 EOC (both A&E and PTS)	21
19.3 Human Resources	22
19.4 Clinical Audit and Research staff	22
19.5 Patient Experience staff	22

19.6	IM&T staff .....	22
19.7	Safeguarding staff.....	22
19.8	Performance Management Information team (PMIT) .....	23
19.9	Coroners Team.....	23
19.10	Accessing PCD or PII from any information system .....	23
19.11	Amending PCD or PII on any information system .....	23
20	Confidentiality audits.....	23
21	Non-compliance.....	24
22	Education and training .....	24
23	Consultation .....	24
24	References.....	24
<b>25</b>	<b>Monitoring.....</b>	<b>24</b>
	<b>Plan for Dissemination of Procedural Document.....</b>	<b>26</b>
	<i>Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result. ....</i>	<i>27</i>
	Reporting Incidents (post GDPR) .....	28
	Confidentiality breach .....	29
	Availability breach .....	30
	Integrity breach .....	30
	When is an incident reportable under the GDPR? .....	30

## 1. Introduction

1.1. This document has been compiled in line with the national HSC Code of Practice on Confidentiality.

The HSC is committed to the delivery of a first-class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- Understand the reasons for processing personal information;
- Give their consent for the disclosure and use of their personal information;
- Gain trust in the way the HSC handles information and;
- Understand their rights to access information held about them.

Source: Confidentiality: HSC Code of Practice

The HSC Care Guarantee (2011) and the (former) Health and Social Care Information Centre (HSCIC) document 'A guide to confidentiality in health and social care: Treating confidential information with respect' provide further guidance. The latter document identified five confidentiality rules:

### Rule 1

Confidential information about service users or patients should be treated confidentially and respectfully.

### Rule 2

Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.

### Rule 3

Information that is shared for the benefit of the community should be anonymised.

### Rule 4

An individual's right to object to the sharing of confidential information about them should be respected .

### Rule 5

Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

- 1.2. The nature of the work undertaken by NIAS employees and volunteers brings them into possession of a great deal of confidential, and often highly sensitive information, both patient and non-patient related. Therefore, it is essential that the public at large believe that we as a whole maintain confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose. NIAS also has statutory obligations to maintain records, systems and procedures ensuring data records are stored and disposed of accordingly.
- 1.3. This document describes the responsibilities of all staff and lays down guidelines in order to ensure confidentiality is maintained.
- 1.4. All staff working for NIAS has a legal duty of confidentiality to the subjects of information they come into contact with. This duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence (e.g. patient to healthcare professional).
- 1.5. Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, there is a legal basis to do so, when it is in the public interest or there is legal justification to do so.

## **2. Objectives**

## 2.1 The key objectives of this document are:

- To ensure that information is processed in accordance with relevant legislation and guidance.
- To provide comprehensive guidance on the correct way to handle information.
- To reiterate the duty of confidence each member of staff has to the subjects of information processed by NIAS.

### 3. Scope

This document applies to all employees of NIAS including permanent, temporary, voluntary and contract staff, who come into contact with personal and non-personal information.

### 4. Definitions

#### 4.1 Confidential information

4.1.1 The Oxford English dictionary definition of confidential is 'intended to be kept secret' (2017).

Confidential information is any information held, personal and non-personal, that when provided was done so in the expectation it would not be disclosed without relevant authority. It can be anything that relates to patients, staff, their family and friends and also to NIAS information that is protected from release under the Freedom of Information Act 2000 (FOI).

This class of information may be stored in any manner e.g. on paper, electronically, video, photograph, and could be stored on any device, including portable such as laptops, mobile/smart phones, tablets and digital cameras. This list is not exhaustive. Confidential information may also be passed by word of mouth.

#### 4.2 Personal confidential data (PCD)

4.2.1 Personal confidential data (PCD) is anything that can identify an individual e.g. name, address, date of birth, HSC number, National Insurance number and photographs. For living individuals, this type of information is protected by law under Data Protection legislation.

### **4.3 Special Category Data**

- 4.3.1 Certain types of information are particularly sensitive under Data Protection legislation, including personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic or biometric data, data concerning health or data concerning a person's sex life or sexual orientation. Again, these data can only be processed if certain conditions under Data Protection legislation are met. Reference should be made to the Data Protection Policy for further information.

### **4.4 Processed**

- 4.4.1 Any action that can be performed on the information e.g. collection, retention, destruction etc.

### **4.5 Rights of the Data Subject**

- 4.5.1 Under Data Protection legislation, individuals are afforded several rights relating to the processing of their personal information. These include access to, rectification of and erasure of their personal information. A full list and how to manage them is included within the Data Protection Rights Procedure.

### **4.6 Data Protection legislation**

- 4.6.1 Legislation including, but not limited to the UK Data Protection Act 2018 and General Data Protection Regulation 2016

## **5 Responsibilities**

### **5.1 Chief Executive Officer**

- 5.1.1 The Chief Executive Officer is the NIAS accounting officer and has overall accountability and responsibility for Information Governance (IG).

### **5.2 Senior Information Risk Owner (SIRO)**



5.2.1 The SIRO oversees information risk management and takes ownership of the risk assessment process for information risk.

### **5.3 Caldicott Guardian**

5.3.1 The Caldicott Guardian acts as the 'guardian' of PCD and oversees the use and sharing of this type of information

### **5.4 Head of Information Governance**

5.4.1 The Head of IG manages the day to day IG agenda, provides assurance to the Board on compliance with the DSPT and provides advice and assistance on IG related matters to NIAS e.g. disclosure

### **5.5 Data Protection Officer**

5.5.1 The Data Protection Officer (DPO) ensures NIAS can demonstrate its compliance with Data Protection legislation

### **5.6 Corporate Services Compliance Manager**

5.6.1 The IG and Compliance Manager manages requests for information and provides assurance to the Head of IG on the records management function.

### **5.7 Information Asset Owners (IAOs)**

5.7.1 Assigned owner of an information asset who reports to the SIRO

### **5.8 All staff**

5.8.1 All staff have a responsibility to comply with legislation and guidance relating to IG and to report any risks or areas of concern.

## **6 Legal considerations**

The disclosure of confidential information needs to be both lawful and ethical.

There is a range of legislation and guidance that limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range that require information to be used or disclosed.

## **6.1 Data Protection legislation**

6.1.1 Data Protection legislation legislates for the processing of the *personal* information of *living* individuals. The term 'processing' includes any action performed on the data including obtaining, holding, recording, using, disclosing and disposal. The legislation applies to staff as well as patient records and covers both paper and electronic records.

6.1.2 NIAS meets its obligations under Data Protection legislation as it works in line with the six principles:

Data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes...
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

An additional principle is also in force that requires an organisation *'shall be responsible for, and to be able to demonstrate, compliance with the principles.'*

6.1.3 The Data Protection legislation allows for third party access to personal information in certain specified circumstances. Further information can be found on the Information Commissioner's website – [www.ico.org.uk](http://www.ico.org.uk)

6.1.4 Sanctions available to the Information Commissioner's Office (ICO)

The ICO can impose sanctions on an organisation for a breach of confidentiality, data loss incident or for not complying with Data Protection legislation. These include:

- A fine of up to €10,000,000 (or 2% of annual turnover)
- A fine of up to €20,000,000 (or 4% of annual turnover)
- Information notices
- Assessment notices
- Enforcement notices
- Powers of entry and inspection

6.1.5 Reference should also be made to the Data Protection Policy and the Data Protection Rights Procedure.

## **6.2 Freedom of Information Act 2000 (FOI)**

6.2.1 The FOI came into full effect on the 1<sup>st</sup> January 2005 and legislates for the general right of access to *non-personal* information held by public authorities. The idea behind the FOI was to encourage greater openness by these authorities. One of the stipulations of this act is the requirement for each authority to develop a publicly accessible publication scheme that would detail all information routinely available. The NIAS version is available via the NIAS website – [www.NIAS.HSC.uk](http://www.NIAS.HSC.uk)

6.2.2 FOI contains a number of exemptions – valid reasons – why a request for information can be refused. Further information can be found on the ICO's website – [www.ico.org.uk](http://www.ico.org.uk)

6.2.3 Reference should also be made to the Freedom of Information Policy and Procedure.

### **6.3 Human Rights Act 1998**

Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This identifies a duty to protect the privacy of individuals and preserve the confidentiality of their health records. Compliance with Data Protection legislation ensures NIAS is meeting its obligations under Human Rights legislation.

### **6.4 Common Law Duty of Confidentiality**

This is not an act of law, therefore, does not have a legal basis. However, the principles contained within have been built from case law. The key principle is that information confided should not be disclosed further without the confider's permission for reasons other than those already agreed.

### **6.5 Caldicott Principles (2013) – The Information Governance Review**

6.5.1 The Caldicott principles are a set of guidelines developed specifically for handling patient identifiable data (PII). NIAS has an identified Caldicott Guardian who will oversee work to establish the highest practical standards for handling PII.

6.5.2 The seven principles are:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential data
- Access to personal confidential data should be on a strict need-to-know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

### 6.5.3 Duty to share

The IG Review identified that the duty to share information can be as important as the duty to protect patient confidentiality. Staff should have the confidence to share information if it is considered to be in the best interest of the service user while still complying with the Caldicott framework.

## 7 Protecting information

7.1 All staff have a duty to protect the information they process on a day-to-day basis, whether this is personal or non-personal. The following should be adopted as good practice by all NIAS employees:

- Do not leave confidential information on view. Paper files should be locked away in drawers/cabinets. Staff should 'lock' computers when away from their work area
- Never share your passwords or PIN numbers with anyone else
- Confidential phone calls should not be conducted in an open office. If working from home, headphones should be used and confidential conversations not conducted within earshot of unauthorized individuals.
- Adopt a 'clear desk policy' where possible
- Do not disclose confidential information over the telephone unless you are **100%** certain of the identity of the caller. If in doubt, check the caller's identity and establish whether they are in fact entitled to receive the information. Call back if necessary. Do not accept a mobile or direct dial phone number. If in doubt, do not release the information and check with the Head of IG.
- Faxing confidential information should only be carried out if the receiving fax is in a secure location or additional measures have been taken to ensure its security. Reference should be made to the NIAS Safe Haven policy for full guidelines.
- PCD or PII should not be sent via external email as its security cannot be assured. However, HSC mail (email address ending in HSC.net) is deemed secure if the

message is being sent to another HSC.net account or other secure email address. Reference should be made to the Safe Haven policy for a full list of addresses and further guidance.

- All mobile devices and removable media must be protected to at least 256 AES bit encryption.
- Home workers should abide by the home working agreement.

## **8 Storage of Patient Report Forms (PRFs)**

The security of PRFs must be maintained from the moment of creation. PRFs must be stored securely on both vehicles, within the locked drugs cabinet or glovebox, and on stations, within the standard container within a locked room. Reference should be made to the Clinical Records Keeping Policy and PRF Storage Standing Operating Procedure.

## **9 Disposal of confidential information, including archiving**

The duty of confidentiality continues right through to the ultimate disposal of information. NIAS has developed a Retention and Disposal of Information Schedule and reference should be made to this document prior to the destruction of any information. Additionally, we have developed an Archive Procedure which should be referred to when archiving confidential information. References to both of these are included in the Information Lifecycle Management Policy.

## **10 Information sources**

There is a wide variety in the types of information received and stored by NIAS and this information flows in from a number of sources. There are two broad categories of information held by NIAS:

- Patient, relative and public data gathered as a result of a transport request – A&E or PTS service provision
- Staff data – permanent, temporary, voluntary and contracted

## **11 Requests for information**

Requests for information may come from a variety of sources and it is dependent on the source and type of information requested, as to how the request should be handled. Reference should be made to the Information Request Procedure.

### **11.1 Requests for personal information from staff and patients**

Requests by individuals to access their own records, both staff and patient, are known as the 'Right of Access by a Data Subject' and are a given right under Data Protection legislation. Requests do not have to be made in writing, however, NIAS must be satisfied of the identity of the person making the request. Requests must be completed within one month. Reference should be made to the Data Protection Rights Procedure when handling these requests. These are managed by the IG and Compliance Manager.

### **11.2 Requests from the police**

Requests are often received from the police for copies of PRFs, incident logs and recordings of calls. Under Data Protection legislation, they are permitted access to these records, without the consent of the data subject, due to a crime and taxation exemption within the Data Protection Act 2018. However, these requests must be made in writing using an official police form. *Under no circumstances should information be handed out at the scene of an incident.* Police requests are managed by the IG and Compliance Team between 8.00 and 16.00 Monday to Friday and by the Emergency Operations Centre (EOC) at all other times.

### **11.3 Requests from coroners**

Requests are often received from coroners for copies of PRFs, incident logs and recordings of calls. The Trust has a legal obligation to provide this information. Furthermore, the information provided cannot be redacted to remove identifiable information relating to individuals other than the patient.

### **11.4 Requests for non-personal information**

Requests for non-personal information are governed by the requirements of FOI. Reference should be made to the Freedom

of Information Policy and Procedure prior to releasing information. These requests are managed by the IG and Compliance Manager.

### **11.5 Requests from solicitors**

A letter of authorisation must accompany requests from solicitors, for information pertaining to their client, from the individual who is the subject of the information. These requests are managed by the IG and Compliance Team.

### **11.6 Requests for information on other individuals**

Requests for information on other individuals, whether they be patients or staff should only be released on a 'need to know' basis. The requester must be able to justify why the request is being made and that they are entitled to make the request and receive the information. There are circumstances when information can be released to third parties. Further guidance can be found in the Data Protection Policy. If in doubt, do not disclose the information without seeking advice from the Head of IG or IG and Compliance Manager beforehand.

### **11.7 Telephone enquiries**

If a request for information is made over the telephone, the response will be dependent on who is making the request, and what the request is for.

- Individuals making a request for their own personal information, under Data Protection legislation may do so over the telephone, however, NIAS must be satisfied as to the identity of the requester.
- An individual making a request under FOI must be asked to put their request in writing (email is acceptable)
- An individual making a request under the Environmental Information Regulations 2004 may do so via the telephone or in writing.
- Check the individual is entitled to have access to the information. If in doubt, ask for the request to be put in writing and seek advice from the Head of IG.
- Never release any confidential information over the telephone unless you are entirely sure of the identity of the



caller and their entitlement to receive the information. If in doubt, call them back. Do not accept a mobile or direct dial telephone number. Further guidance can be found in the NIAS Safe Haven Policy.

## **11.8 Requests from overseas**

11.8.1 There may be occasions when confidential information is requested from overseas or must be transferred overseas when accompanying a foreign national who may have received treatment from NIAS. Although these will be rare occurrences, procedures must be followed to protect the information. The General Data Protection Regulation ensures that European Union (EU) member states have the same level of protection in place as the UK. Personal information must not be transferred outside of these states unless that country or territory can demonstrate an adequate level of protection for the data.

11.8.2 Data Protection legislation makes allowances for the transfer of medical information to accompany a patient.

11.8.3 Ideally, when transferring personal information outside of the UK, consent should be obtained from the data subject. However, if this is not possible, the following conditions must be satisfied prior to its release:

- The reason for the information request is valid
- The method of transferring the information is secure
- Details on how the information will be kept secure by the recipient are supplied
- There is a documented retention period for the information

11.8.4 Only when these conditions are satisfied should the information be released.

## **12 Patient choice**

Under Data Protection legislation, an individual can object to the processing of their personal data. In the context of NIAS, this may

mean refusing to supply details to complete a PRF. The attending crew should respect the wishes of the patient. However, they should explain why the information is required and that it will be held securely. Reference should be made to the Data Protection Rights Procedure.

### **13 Patient consent and National Data Opt-Out**

Where consent is to be relied upon to share or process personal information, this must be explicit and the individual well informed. The consent must also be recorded. If the information required can be anonymised this is the option that should be adopted. Reference should be made to the 'Research, Management and Governance Policy'.

Individuals have the right to opt out of the use of their information for research purposes. They do this using the national data opt-out service managed by HSC Digital. Records relating to those who have chosen to opt-out must not be used for research purposes.

Data Protection legislation allows for the processing of personal information, not for direct health care, without consent under certain circumstances. Reference should be made to the Data Protection Policy or advice sought from the Head of IG or IG and Compliance Manager.

### **14 Abuse of privilege**

It is strictly forbidden for employees to access any information relating to their own family, friends or acquaintances without consent. Looking at patient or staff records out of curiosity is totally unacceptable. Disciplinary proceedings will be instigated should abuse of privilege be discovered.

### **15 Social networking sites**

Access to social networking sites (for example Facebook) is not routinely allowed from NIAS computers. Requests for access will be assessed on a case by case basis. Staff using these sites from personal computers should be aware that they still have a duty of confidentiality to NIAS and its service users. Discussions, taking place on these sites containing negative or critical comments,

about NIAS, its staff and service users, will not be tolerated and action will be taken against any member of staff found in breach of this.

Under no circumstances should patient details be posted to these sites. Reference should be made to the Social Media Policy.

## **16 Adverse incident reporting**

Possible breaches or risks of breaches of patient confidentiality or other confidential information will constitute an adverse incident and will be reported through the NIAS incident reporting procedure. Reference should be made to the Incident Reporting Policy. The IG risk register will be used to log any identified risks to the confidentiality of information. Serious breaches in confidentiality must be reported to the Commissioners. The NIAS Annual Report is also required to indicate the number of confidentiality incidents reported throughout the year. The Head of IG and the Information Security Manager will use their judgment to determine if an IG incident or cyber security incident (respectively) would equate to level 2 severity and report accordingly. All IG and cyber security serious incidents judged to be at level 2 or above must also be logged on the DSPT using the incident reporting tool. All serious incidents must be reported to the ICO within 72 hours of becoming aware. The definitions of IG and Cyber Security Serious Untoward Incidents can be found in Appendices 2 and 3.

## **17 Working in an open plan environment**

Working in an open plan environment poses possible risks to the security and confidentiality of information. The following guidance should be adhered to when working in this type of setting:

- When printing confidential or personal information to a shared printer, please ensure that the printing is collected immediately.
- Confidential telephone conversations should be conducted within a closed office environment. Within the EOC and PTS control, holding confidential conversations in an open plan environment is unavoidable.
- Confidential/personal information should not be left on desks or in public view.

- A 'clear desk' policy should be adopted (where applicable/possible), at a minimum, confidential/personal information should be locked away when not in use.
- Users should lock the PC screen when moving away from their desk – even for short periods of time. Please note: EOC are exempt from this for both patient safety reasons and the fact that the environment is secure, however, they should use the 'lock CAD screen' functionality.

## **18 Working from home**

As the number of staff working from home increases, there are specific considerations to take into account:

- Content on monitors / laptop screens must not be visible to other members of the household. They must be faced away from windows to prevent overlooking by individuals outside of the house. (Privacy screens are available if the location of the work space does not support this).
- Headphones must be used when attending an online meeting where conversations may be overheard by others within the household. The employee must also be aware of who is in earshot when discussing confidential / personal matters during an online meeting.
- All home listening devices must be turned off (e.g. Alexa) when confidential conversations are taking place.
- Confidential / personal information must not be printed on personal printers. Where NIAS has provided a printer for home use, all confidential printouts must be kept secure and disposed of via the confidential waste process i.e. cross shredder when no longer required. Printing should be kept to a minimum.
- Computers must be locked when not in use, even for short periods of time e.g. coffee, comfort breaks
- Confidential / personal paperwork must be locked away when not in use and not accessible by other household members.
- Passwords must not be written down, shared or made available to anyone else.

- Should a data breach occur, this must be reported via the IR1 process as soon as possible (no later than 48 hours after it has been identified).

## **19 Specific departmental considerations**

There are specific considerations for certain areas of NIAS:

### **19.1 Operational staff**

- 19.1.1 Operational staff are the employees who will have the most direct contact with patients and their relatives. Information confided during treatment and/or transportation, whether this is by word of mouth or held in writing, must be kept confidential in accordance with this Code of Conduct.
- 19.1.2 On occasions, staff may be required to provide statements to the police with reference to incidents they may have attended. This is acceptable if the police have completed the necessary paperwork (see Police Requests). Reference should be made to the Police Interviews and Witness Statements Standard Operating Procedure.
- 19.1.3 Operational staff may be required to obtain evidence of clinical experience to complete their portfolios, in the form of PRFs. However, it is strictly forbidden for staff to photocopy a 'live' document as control needs to be maintained over copies being released. Staff wishing to refer to a particular incident within their portfolio must re-write the information on to a blank PRF omitting any patient identifiable information. Alternatively, a redacted copy can be obtained from the Clinical Audit department following a written request. An anonymised version of a completed electronic patient report form (ePRF) can be printed off from the web viewer by a member of staff holding relevant Smartcard access rights.

### **19.2 EOC (both A&E and PTS)**

EOC staff have contact with patients and their relatives on a day-to-day basis and must respect the confidentiality of these individuals at all times. In addition, due to the nature of the functions carried out in the EOC, it is also necessary to store

information pertaining to operational staff on the Computer Aided Dispatch (CAD) system. This information must be afforded the utmost confidentiality.

### **19.3 Human Resources**

Personnel records afford the same level of protection as patient information, as laid down in this Code of Conduct. All Human Resources staff should respect the privacy of other staff members at all times.

### **19.4 Clinical Audit and Research staff**

Clinical Audit staff have access to all the PRFs completed by operational staff throughout NIAS. As these forms contain a substantial amount of sensitive personal and patient information, these must be treated in accordance with the requirements of this Code of Conduct.

### **19.5 Patient Experience staff**

Information handled by the members of the Patient Experience team may contain particularly sensitive information relating to both staff and patients. The confidentiality of this must be maintained at all times. Any disciplinary proceedings brought because of a complaint or investigation will also be kept strictly confidential.

### **19.6 IM&T staff**

IM&T staff have access to patient and staff information either through Data Protection access requests or through the maintenance of information systems. All staff must be aware of the security measures in place when transmitting the information to third parties and confidentiality must be maintained at all times.

### **19.7 Safeguarding staff**

Information handled by the Safeguarding team may contain particularly sensitive and highly confidential information relating to service users. The confidentiality of this must be maintained at all times.

## **19.8 Performance Management Information team (PMIT)**

PMIT staff have access to patient and staff information through analysis work. All staff must be aware of the security measures in place when transmitting the information to third parties and confidentiality must be maintained at all times.

## **19.9 Coroners Team**

The Trust has a legal obligation to provide information to coroners when requested. This information cannot be redacted, therefore, information relating to individuals other than the patient may be disclosed and included in the coroners disclosure bundle.

## **19.10 Accessing PCD or PII from any information system**

Although there are system specific considerations, there are also generic ones that will relate to all information systems and all staff:

- Staff have a duty of confidentiality to the data subject and must not disclose PCD or PII without the relevant authority, legal basis or consent to do so.
- PCD and PII must only be accessed on a 'need to know' basis (see section 6.6.2).
- Where possible, a reason for accessing the information must be noted to support audit processes
- IAOs must ensure that correct access rights are applied to the systems they 'own' to ensure access is only allowed to those staff that have relevant authority to access the information

## **19.11 Amending PCD or PII on any information system**

Staff must not abuse the privilege of system access by inappropriately amending / editing a record with non-approved information. Proper processes must be followed and any amendments to information annotated, where possible, with the reason for the edit. Reference should be made to the Data Protection Rights Procedure.

## **20 Confidentiality audits**



Confidentiality audits will be conducted by the IG and Compliance Team at regular intervals. Reports will be presented to the IG Group highlighting any areas for concern and recommendations made.

All systems should have the ability to produce audit reports detailing who has accessed personal information.

## **21 Non-compliance**

All staff agree to uphold confidentiality on signing of their contract of employment with NIAS. This agreement continues after employment has ceased. Non-compliance with this statement and this Code of Conduct will result in disciplinary action being taken in accordance with the Disciplinary Procedure.

## **22 Education and training**

All NIAS staff must complete mandatory training in IG on an annual basis. The national e-learning programme, developed by HSC Digital, is used to provide this training. New starters are required to complete this within six weeks of the start of their employment.

## **23 Consultation**

This Code of Conduct will be presented to the IG Group for consultation. The group has delegated authority to approve this document.

## **24 References**

The Information Governance Reviews (2013) available from: <https://www.gov.uk/government/publications/the-information-governance-review>

Guide to the Notification of Data Security and Protection Incidents (2018) available from: <https://www.dsptoolkit.HSC.uk/Help/29>

## **25 Monitoring**

The Head of IG will monitor the implementation of this code of conduct, including the minimum requirements for the DSP Toolkit, and take an assurance report to the IG Group. This report will be sent on an annual basis. However, if the ongoing monitoring of



this document shows that there are significant implications for its implementation, then it will be sent to the group sooner.

National guidance issued by the ICO, HSC Digital and the Department of Health will be monitored and included within this document, and those to which it refers, should it be deemed relevant.

Further assurance as to compliance with this Code of Conduct will be achieved by undertaking 'spot checks' and surveys with staff.

## Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Confidentiality Code of Conduct</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead:</b>	<b>Tracy Avery, Head of IG and DPO, Tracy.Avery@nias.hscni.net</b>
<b>Previous document already being used?</b>	<b>Yes</b>	<b>Print name, title and contact details</b>	
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	All staff as they are all subject to confidentiality responsibilities.		
<b>Proposed methods of dissemination:</b> <b>Including who will disseminate and when</b> Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/</i></li> </ul>		<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> <li>• Inclusion within local induction</li> </ul>	

<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Confidentiality Code of Conduct provides staff with the detail and guidance required on how to ensure the confidentiality requirements and responsibilities for the Trust are upheld.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## Reporting Incidents (post GDPR)

A breach is defined as;

Article 4(12) “Personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Breach reporting is now mandatory for all organisations. The GDPR definitions, notification and communication requirements will include breaches that organisations might not have notified under the previous data protection regime. The traditional view that a data breach is only reportable when data falls into the wrong hands is now replaced by a concept of a ‘risk to the rights and freedoms of individuals’ under Article 33 of GDPR. Any security breach that creates a risk to the rights and freedoms of the individual is a personal data breach and could be notifiable to the ICO if it reaches a certain threshold. Any personal data breach that could create a significant risk to the rights and freedoms of an individual must be notified to the Information Commissioner via the HSC Digital reporting tool. All personal data breaches will involve a breach of security at some point in the processing and the additional use of this tool for NIS incident reporting will save the health and social care sector time and effort in reporting.

Personal data is defined as;

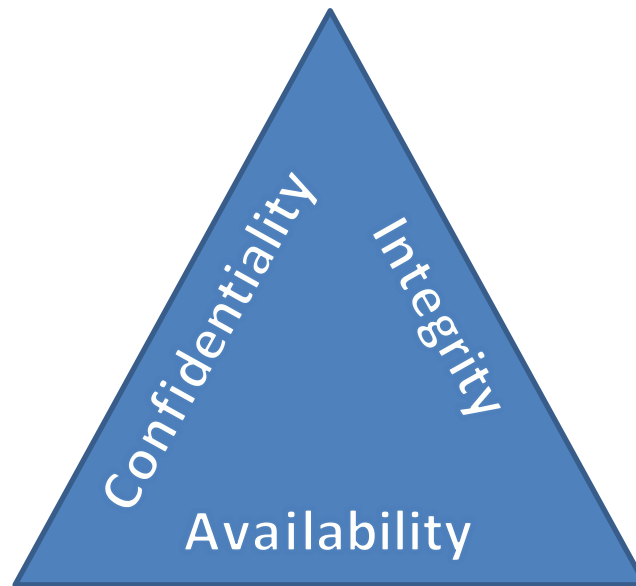
‘any information relating to an identified or identifiable living individual’

And an “identifiable living individual” means a living individual can be identified, directly or indirectly, by reference to \_ (a) an identifier such as a name, an identification number, location data or an online identifier, or (b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

This definition now makes it clear that all paper records that relate to a living individual are included in the definition and any aspect of digital processing such as IP addresses and cookies. Geographical data and biometric data are also clarified as being personal data when they can also be linked to a living individual.

## What are the types of breaches?

The three types of breaches as defined in the Article 29 Working party on personal data breach notification are Confidentiality, Integrity and Availability (CIA)



The CIA Triangle

**Confidentiality breach** – unauthorised or accidental disclosure of, or access to personal data.

### Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as a confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data, the breach would still represent an availability breach and require notification if there is a potential for a serious impact on the rights and freedoms of the individual.

**Availability breach** – unauthorised or accidental loss of access to, or destruction of, personal data

#### Example

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled. This is to be classed as an availability breach

**Integrity breach** – Unauthorised or accidental alteration of personal data

#### Example

Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a 'do not resuscitate' notice on the wrong patient record may have the significant consequence of death whilst an entry recording the incorrect patient blood pressure may not have the same significant effect.

### **When is an incident reportable under the GDPR?**

#### Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner when determining what the significance and likelihood a data breach will be.

The significance is further graded rating the incident on a scale of 1 – 5 (1 being the lowest and 5 the highest).

The likelihood of the consequences occurring are graded on a scale of 1 – 5 (1 being a non-occurrence and 5 indicating that it has occurred).

Where the personal data breach relates to a vulnerable group in society, the minimum score will be a 2 in either significance or likelihood unless

the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

(Vulnerable – ‘A child known to safeguarding or with mental health conditions. Adult with capacity issues or known to adult safeguarding.)

#### Establish the likelihood that adverse effect has occurred

No	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required

#### Grade the potential severity of the adverse effect on individuals

No	Likelihood	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach.
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job

<b>3</b>	Potentially some adverse effect	An adverse effect may be the release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health
<b>4</b>	Potentially pain and suffering / financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment
<b>5</b>	Death / catastrophic event	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

### **Breach assessment grid**

This operates on a 5 x 5 basis with anything other than the 'grey breaches' being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours

Severity (impact)	Catastrophic	5	5	10	15 20 25 DHSC & ICO		
	Serious	4	4	8			
	Adverse	3	3	6	9 12 15 ICO		
	Minor	2	2	4			
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5



	Not occurred	Not Likely	Likely	Highly Likely	Occurred
	Likelihood that citizens; rights have been affected (harm)				

There are a limited number of circumstances where, even when an organisation is aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances, notification may not be necessary;

- Encryption – where the personal data is protected by means of encryption
- ‘Trusted partner’ – where the personal data is recovered from a trusted partner organization
- Cancel the effect of a breach – where the controller can null the effect of any personal data breach

#### Example of how the ‘trusted’ partner can be used to contain a breach

There may be a confidentiality breach, whereby personal data is disclosed to a third party or other recipient in error. E.g. this may occur where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them and it may be aware of their procedures, history etc. The recipient may be considered as ‘trusted’.

### **Sensitivity factors**

Sensitivity factors have been incorporated into the grading scores. If a breach involves certain categories of special categories / vulnerable groups, it must be assessed as at least:

A likelihood of ‘Not likely or incident involved vulnerable groups (where no adverse effect occurred)’ - Not likely on the grid

And a severity of ‘Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred’ – Minor on the grid.

So even where an incident involves special categories / vulnerable groups, on the breach assessment grid, it would be a minimum of 4 and so would not always be reported to the ICO. It would be reported to the ICO if the Likelihood of harm is assessed as at least 'Likely'.

### **Special categories of personal data**

Under the GDPR, special categories are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- processing of genetic or biometric data
- data concerning health
- data concerning a person's sex life or sexual orientation

In addition, those categories not listed in GDPR:

- vulnerable children
- vulnerable adults
- criminal convictions / prisoner information
- special characteristics listed in Equality Act 2010
- communicable diseases as defined by public health legislation
- sexual health
- mental health

### **Assessing risk to the rights and freedoms of an individual (likelihood)**

The GDPR give interpretation to as to what might constitute a high risk to the rights and freedom so an individual. This may be a breach which has the potential to cause one or more of the following:

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation

- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

### **Questions asked when reporting an incident**

1. Organisation name
2. Organisation code
3. Name of the person submitting the incident
4. Email address of person submitting the incident
5. Sector
6. What has happened?
7. How did you find out?
8. Was the incident caused by a problem with a network or an information system?
9. What is the local ID for this incident?
10. When did the incident start?
11. Is the incident still on going?
12. Have data subjects or users been informed?
13. IOs it likely that citizens outside England can be affected?
14. Have you notified any other (overseas) authorities about this incident?
15. Have you informed the police?
16. Have you informed any other regulatory bodies about this incident?
17. Has there been any media coverage of the incident (that you are aware of)?
18. What other actions have been taken or are planned?
19. How many citizens are affected?
20. Who is affected?
21. What is the likelihood the people's rights have been affected?
22. What is the severity of the adverse effect?
23. Has there been any potential clinical harm as a result of the incident?
24. Has the incident disrupted the delivery of healthcare services?
25. Which of these services are operated by your organisation?

Further information and the full copy of this guidance can be found at:  
<https://www.dsptoolkit.HSC.uk/Help/29>

## DATA PROTECTION IMPACT ASSESSMENT POLICY AND PROCEDURE (Data Protection by Design and Default)

### Links

The following documents are closely associated with this policy:

- Service Transition Agreements
- Information Risk Management Policy
- Information Commissioner's Guide to Privacy Impact Assessments

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy and procedure for NIAS

## Contents

1	Introduction.....	3
2	Objectives.....	4
3	Scope.....	4
4	Definitions.....	5
4.1	Information Asset.....	5
4.2	Data Protection Impact Assessment.....	5
4.3	Privacy Risk.....	5
4.4	Data Protection Legislation.....	5
4.5	National Data Opt-Out.....	5
5.	Responsibilities.....	6
5.1	Chief Executive Officer.....	6
5.2	Senior Information Risk Owner (SIRO) .....	6
5.3	Caldicott Guardian .....	6
5.4	Head of Information Governance.....	6
5.5	Data Protection Officer (DPO) .....	6
5.6	Information Asset Owner (IAO).....	6
5.7	Corporate Services Manager.....	6
5.8	Project Managers.....	7
6.	General Policy .....	7
7.	The DPIA Process .....	8
7.1	Information Gathering.....	9
7.2	Screening Questions.....	9
7.3	Full DPIA .....	9
8.	Consultation.....	10
9.	References .....	10
10.	Monitoring Compliance and Effectiveness.....	10
	Plan for Dissemination of Procedural Document .....	12
	DPIA process.....	14
	Screening Questions.....	15
	Full Data Protection Impact Assessment (DPIA) .....	21
	Record of Approval.....	39

## 1 Introduction

- 1.1 The Information Commissioner's Office (ICO) identified Privacy Impact Assessments (PIA) as a key tool in addressing confidentiality and privacy concerns that may arise with the introduction of or significant change to a process.
- 1.2 Recent changes to Data Protection legislation have specifically included 'data protection by design and default'. This change requires organisations to identify any impact to an individual's privacy with the introduction of a new system or service. The process by which this is to be assessed has been renamed as a Data Protection Privacy Impact Assessment (DPIA)

## **2 Objectives**

The key objectives of this policy are:

- 2.1 To ensure that new systems or significant changes to existing systems or processes take account of potential information governance (IG) implications
- 2.2 To provide assurance to the Senior Information Risk Owner (SIRO) and the NIAS Board that there is a robust system in place for protecting information
- 2.3 To increase public confidence in NIAS data collection processes and the services provided
- 2.4 To minimise privacy risks associated with the incorrect processing and management of information.
- 2.5 To ensure that NIAS meets its statutory obligations regarding the processing and management of information.

## **3 Scope**

- 3.1 This policy applies to all potential new or significantly changing processes, systems or assets within NIAS.
- 3.2 This policy applies to all NIAS employees including permanent, temporary, voluntary and contract staff, who

come into contact with personal and non-personal information.

## **4 Definitions**

### **4.1 Information Asset**

4.1.1 Are assets that are owned or contracted by NIAS that are considered to have value. They are likely to include computer systems, information, software and staff.

### **4.2 Data Protection Impact Assessment**

4.2.1 A structured assessment of the potential impact on privacy for new or significantly changed processes or systems

### **4.3 Privacy Risk**

4.3.1 Falls within 2 categories:

- Risks to the individual because of contravention of their rights in relation to privacy, or loss, damage or misuse of their personal information
- Risks to the organisation because of failure to comply with the law, a failure to meet public expectations on the protection of personal information or a perceived harm to privacy.

### **4.4 Data Protection Legislation**

4.4.1 Legislation including, but not limited to, the UK General Data Protection Regulation (UK GDPR) and UK Data Protection law.

### **4.5 National Data Opt-Out**

4.5.1 The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes



## **5. Responsibilities**

### **5.1 Chief Executive Officer**

- 5.1.1 The Chief Executive Officer is the Accounting Officer of NIAS and has overall accountability and responsibility for IG.

### **5.2 Senior Information Risk Owner (SIRO)**

- 5.2.1 The Senior Information Risk Owner (SIRO) will take ownership of the risk assessment process for information risk. This role is within the remit of the Director of Strategy and Transformation.

### **5.3 Caldicott Guardian**

- 5.3.1 The Caldicott Guardian will act as the 'guardian' of patient identifiable information and will oversee the use and sharing of patient information. This role is within the remit of the Medical Director.

### **5.4 Head of Information Governance**

- 5.4.1 The Head of Information Governance will manage the day to day IG agenda and provide assurance to the Board.

### **5.5 Data Protection Officer (DPO)**

- 5.5.1 The Data Protection Officer will ensure NIAS can demonstrate its compliance with Data Protection legislation. This role is included in the remit of the Head of IG.

### **5.6 Information Asset Owner (IAO)**

- 5.6.1 Information Asset Owners (IAO) are directly accountable to the SIRO and will provide assurance that new systems and processes have met the necessary level of DPIA.

### **5.7 Corporate Services Manager**

- 5.7.1 Corporate Services Manager will ensure that requests for new systems and processes have been assessed for privacy impact.

## **5.8 Project Managers**

- 5.8.1 Project Managers will ensure that the DPIA forms part of the business case and formal project documentation through the Project Toolkit.

## **6. General Policy**

- 6.1 Data Protection legislation has identified that where processing, in particular that using new technologies, is likely to result in a high risk to an individual, an assessment of the risk must be undertaken.
- 6.2 DPIAs are required when the processing is of such a wide scope or will use personal information in such a way that there would be a genuine risk to the privacy of an individual. It will not always be necessary to conduct a full-scale DPIA. An initial assessment of any privacy risks should be undertaken at the start of a project to identify the level of assessment required. The DPIA should also identify if any processing will be subject to the National Data Opt-Out.
- 6.3 The DPO should be involved in the DPIA process to provide advice and assistance only.
- 6.4 Answering the questions set out in Appendix 3 will identify if a full-scale DPIA is required. Typically, if any questions are answered 'yes' a full DPIA will be required. The DPO will advise if this is the case when reviewing the screening questions.
- 6.5 Full scale DPIAs involve more in-depth assessment of privacy risks and liabilities. Privacy concerns should be voiced, and solutions put forward to accept, mitigate or avoid them. They will usually be recommended where:
- new and intrusive technology is being used

- where personal and sensitive information which was originally collected for a limited purpose is going to be reused in a new and unexpected way

6.6 The questions used within the full-scale DPIA can be found in Appendix 4.

## 7. The DPIA Process

The Information Commissioner has produced guidance on DPIAs. This identifies that the DPIA process should be flexible in that it should begin early in the life of a project or can run alongside the project development process. The following steps were identified:



It is important to consult with internal and external stakeholders as required throughout the process.

## **7.1 Information Gathering**

- 7.1.2 Sufficient information must be gathered to allow for the screening questions to be answered as fully as possible. The project outline or brief should be used as a basis for this information gathering exercise.
- 7.1.3 It may be useful to search for information about projects of a similar nature that may have already undergone a DPIA. These could include consultations with HSC Digital or the ICO.
- 7.1.4 On completion of the information gathering, the screening questions for the DPIA can be answered.

## **7.2 Screening Questions**

- 7.2.1 The purpose of the screening process is to ensure that NIAS has considered any risks involved with the introduction of, or change to, a system or process.
- 7.2.2 Any identified risks should be assessed to identify whether they are proportionate to the benefits of the new system or change.
- 7.2.3 Completion of the screening questions will identify if a full-scale assessment is required.

## **7.3 Full DPIA**

- 7.3.1 DPIAs should be completed by the Project Manager, other key senior project team member or the Information Asset Owner (IAO) at the initial stage of a project or as an integrated part of the project to ensure that privacy concerns are identified.
- 7.3.2 A list of stakeholders should be included in the DPIA and the role they have to play in the project. Details of consultation with stakeholders should be included.
- 7.3.3 Additional expertise may be required to provide advice and assistance on the completion of the DPIA depending on the type of project, for example:

- the Data Protection Officer
- expertise in relevant technologies
- expertise in information security processes
- expertise in records and information management

Please note: the above roles should not complete the DPIA

#### 7.3.4 An effective DPIA should show:

- the identification of impacts on privacy
- identification of privacy risks that can be avoided
- identification of privacy risks that can be mitigated
- identification of privacy risks that can be accepted

#### 7.3.5 The actions resulting from a DPIA should be reviewed throughout the project to assess their effectiveness.

Appendix 2 shows the internal process to follow when completing a DPIA

## 8. Consultation

This policy will be presented to the Information Governance Group for consultation. The Group has delegated authority to approve this document.

## 9. References

- 9.1 Information Commissioner's Office Guide to Data Protection Impact Assessments - <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>
- 9.2 National Data Opt-Out – HSC Digital  
<https://digital.nhs.uk/services/national-data-opt-out>

## 10. Monitoring Compliance and Effectiveness

- 10.1 The Head of IG will monitor the implementation of this policy, and take an assurance report to the IG Group. This report

will be sent on an annual basis. However, if the ongoing monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the Group sooner.

## Plan for Dissemination of Procedural Document

Appendix 1

<b>Title of document:</b>	<b>Data Protection Impact Assessment Policy and Procedure</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead:</b>	<b>Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@Nias.hscni.net</b>
<b>Previous document already being used?</b>	<b>No</b>	<b>Print name, title and contact details</b>	
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	All staff have a responsibility to ensure that any new processes, systems or changes are implemented with regard to impact on personal information and confidentiality in accordance with legislation and national guidance therefore, all need to be aware of this policy.		
<b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b>  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/</i></li> </ul>		<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>	

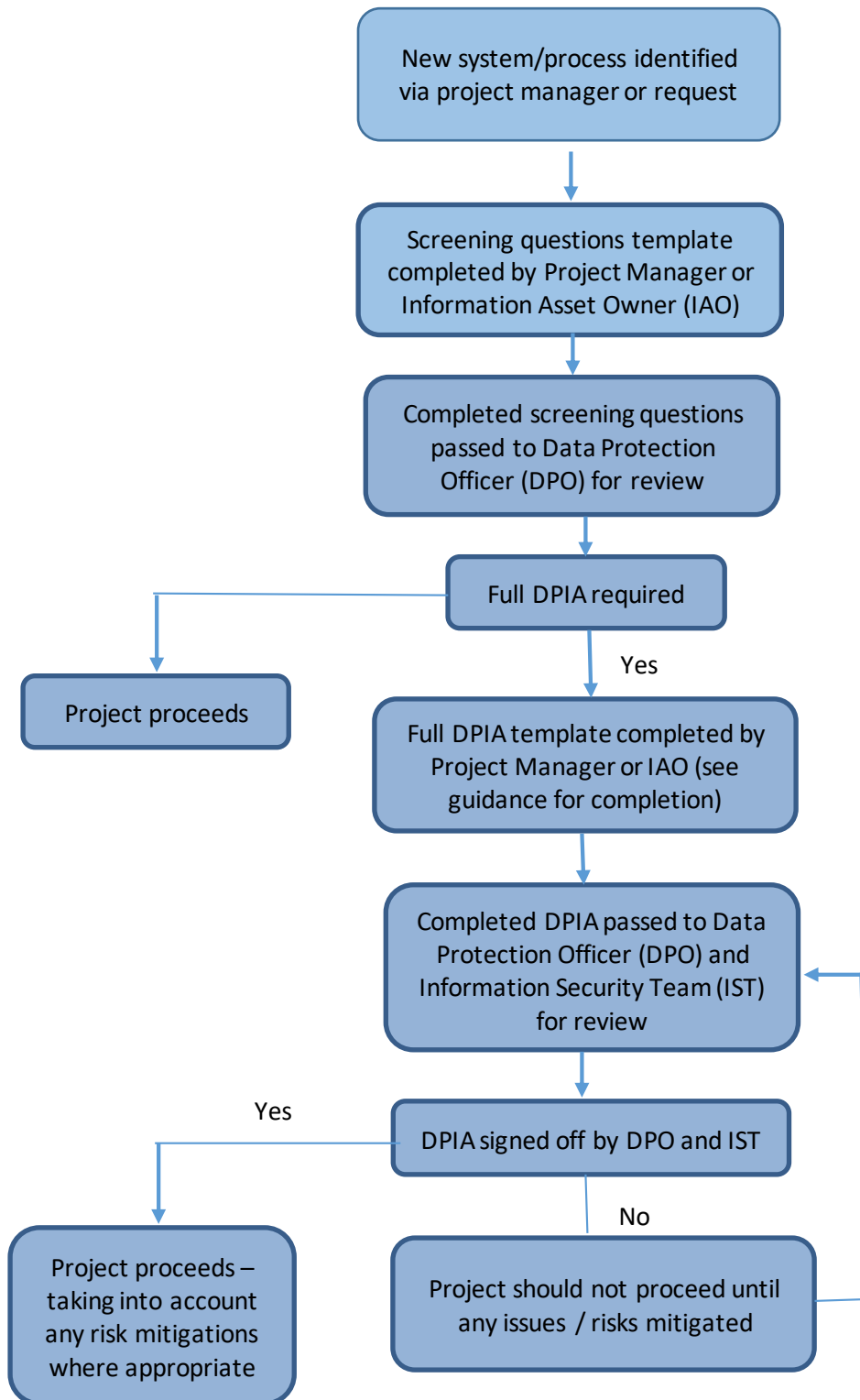
<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Data Protection Impact Assessment Policy and Procedure provides staff with the detail and guidance required on how to complete a DPIA at the beginning of a project to ensure that privacy and confidentiality issues are identified and addressed in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*



## Appendix 2

### DPIA process



## Screening Questions

The initial stage in the Data Protection Impact Assessment (DPIA) process is the completion of the screening questions as these will identify if a full DPIA is required. Not all new systems or processes will require a full assessment. Please provide as much information as possible in order that an informed review can be undertaken. The completed screening questions will be reviewed by the Data Protection Officer (DPO). However, the DPO is unable to complete the template as they will be responsible for final sign off. They can provide advice on any aspect of this process though.

The use of acronyms should be avoided as the reader may not be familiar with them.

**Text in red is for guidance only and should be replaced by your comments/answers**

<b>Completed by – name / job title:</b>	Name and job title of person completing this template
<b>Purpose of asset / system:</b>	Description of the purpose of the new/amended system/process. Include sufficient detail to be able to provide an overview to someone who may have no prior knowledge or experience of this.
<b>Asset / system name:</b>	Name of the system / process e.g. CAD
<b>Supplier of system / asset:</b>	Name of the supplier of the system / process e.g. MIS
<b>Executive sponsor – name / job title:</b>	Name of the Executive or business lead for this project
<b>Project Manager – name / job title:</b>	Name and job title of the individual who will be managing the implementation
<b>Information Asset Owner (IAO) – name / job title:</b>	Name and job title of the member of staff who will become the IAO for the system when it comes into operation (for guidance on IAO

	please refer to the Information Asset Policy available in the policy library
<b>Information Asset Administrator(s) – name / job title:</b>	Name and job title of the member of staff who will become the IAA for the system when it comes into operation (for guidance on IAAs please refer to the Information Asset Policy available in the policy library)
<b>Date:</b>	Date this template was completed
<b>Proposed implementation date:</b>	Date when the system / process is due to be implemented

No	Question	Response	Comment
1	Has a DPIA been carried out on a very similar processing activity?	Yes / No	If this relates to a system that may have been introduced elsewhere, particularly if it is a national initiative, then a DPIA may have already been completed by another Trust or organisation that can be used as a reference.
2	Will the system involve the processing of personal confidential data, including sensitive/special categories?	Yes / No	Personal information is anything that can identify an individual. Sensitive / special category data includes medical, gender, sexual orientation, trade union membership, race, ethnicity and religion.
3	If 'yes' to Q2: Has this data already been made publicly available by	Yes / No	A simple test would be to do a google search to see if the information is

	<b>the data subject e.g. have they put it on social media?</b>		already on the public domain.
<b>4</b>	<b>Will data be processed on a large scale?</b> <i>Likely to be large scale if it involves NIAS staff, any group of patients or one region of the East Midlands</i>	<b>Yes / No</b>	If unsure on the scale, include the number of individuals who will be included in any processing in this box
<b>5</b>	<b>Does the data concern vulnerable data subjects?</b> <i>Vulnerable data subjects include; employees, patients, children, any group of the population requiring special protection.</i>	<b>Yes / No</b>	If yes, include in this box what type of vulnerability e.g. children
<b>6</b>	<b>Will the system involve the collection of new information about individuals?</b>	<b>Yes / No</b>	Will the process / system involve collecting more information from individuals than we already have. E.g. we already hold name but will need to also collect address
<b>7</b>	<b>Will the system compel individuals to provide information about themselves?</b>	<b>Yes / No</b>	Will individuals have no choice about providing information about themselves.
<b>8</b>	<b>Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?</b>	<b>Yes / No</b>	Will the process / system mean that we will be sending information to someone new e.g. PRFs will routinely be sent to GPs, but not to dentists so this would be a change in disclosure
<b>9</b>	<b>Are you using information about individuals for a purpose it is currently not used for, or in a way it is not currently used?</b>	<b>Yes / No</b>	This would be if, for example, CAD data was used for reasons other than healthcare

10	<b>Will the system involve using new technology which may be perceived as being privacy intrusive (e.g. use of biometrics or facial recognition)?</b>	Yes / No	This is self-explanatory – it would include any type of facial recognition etc. that an individual does not have any real control over
11	<b>Will the system result in automated decision making or action being taken against individuals that may have a significant impact on them?</b>	Yes / No	Will the system / process have any human intervention at all for any form of decision making e.g. credit references are often automated using algorithms based on answers
12	<b>Is the information about individuals of a kind likely to raise privacy concerns?</b> <i>Consider health records, criminal records or other information that could be considered particularly private</i>	Yes / No	If unsure, enter what type of information is being processed as one person's idea of privacy may differ from another's
13	<b>Will processing of information include evaluating or scoring, including profiling and predicting, in order to create or use personal profiles?"</b>	Yes / No	This would include surveys, questionnaires etc. where a score is assigned to a particular answer and used to make a decision or create a profile
14	<b>Will processing include systematic monitoring such as processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" e.g. CCTV?</b>	Yes / No	This could include such things as body cams or any other sort of camera functionality.
15	<b>Will datasets be matched, linked or combined, for example originating from</b>	Yes / No	Will the information being processed then be linked with another set of data from another system or

	<b>two or more data processing activities or systems?</b>		process e.g. inputting ePRF data into a hospital Patient Admin System
16	<b>Will the system require individuals to be contacted in ways that they may find intrusive?</b>	Yes / No	Will individuals be 'cold called' or contacted without prior consent
17	<b>Will data be transferred across borders outside the European Union?</b>	Yes / No	Self-explanatory. Notably though if data is going to the USA.
18	<b>Does the processing in itself prevent data subjects from exercising a right or using a service or a contract?</b> <i>Examples include processing in a public area that people cannot avoid or refusing data subjects access to a service or entry into a contract.</i>	Yes / No	Examples include processing in a public area that people cannot avoid or refusing data subjects access to a service or entry into a contract.
19	<b>Has this project / process already started as a pilot without a DPIA being undertaken?</b>	Yes / No	If yes, provide further details

This section will be completed by the DPO after an assessment of the responses to the screening questions. There are circumstances when 'yes' answers have been provided but a full DPIA was not required. Therefore, it is important to enter details in the 'comments' column if any of the answers are 'yes'.

For completion by the Data Protection Officer:					
DPIA Required?	Yes / No	Priority of DPIA	High	Medium	Low
Is the processing operation excluded from needing a DPIA by EU/UK law?			Yes / No		
Has the Information Commissioner's Office (ICO)			Yes / No		

excluded the processing operation from needing a DPIA?			
Findings of due diligence (ICO) – any concerns?		Yes / No	
DPIA reference no:	Reference number will be supplied by the DPO		
Reason:			
Completed by:		Date:	

## Full Data Protection Impact Assessment (DPIA)

The Data Protection Officer (DPO) will advise if a full DPIA is required based upon the responses to the 'Screening Questions' template. This should be completed as fully as possible, with sufficient detail to allow for an individual who does not know about the system / process to be able to make an informed assessment. If insufficient detail is included, the DPIA will be returned to the completer for more information. The DPO and Information Security and Technical Operations Manager can advise on how to complete the template, however, they cannot complete the form as they are required to 'sign it off'.

The use of acronyms should be avoided as the readers may not be familiar with them.

**Text in red is for guidance only and should be replaced by your comments/answers**

### 1) **Basic Information about new / change of system**

<b>Completed by – name / job title:</b>	Name and job title of person completing this template
<b>Description of subject of assessment:</b>	Description of the purpose of the new/amended system/process. Include sufficient detail to be able to provide an overview to someone who may have no prior knowledge or experience of this.
<b>Asset / system name:</b>	Name of the system / process e.g. CAD
<b>Executive sponsor – name / job title:</b>	Name of the Executive or business lead for this project
<b>Project Manager – name / job title:</b>	Name and job title of the individual who will be managing the implementation
<b>Information Asset Owner (IAO) – name / job title:</b>	Name and job title of the member of staff who will become the IAO for the system when it comes into operation (for guidance on IAOs please refer to the Information Asset Policy available in the policy library)
<b>Information Asset Administrator(s) (IAA) – name / job title:</b>	Name and job title of the member of staff who will become the IAA for the system when it comes into operation (for guidance on IAAs please refer to the Information Asset Policy available in the policy library)



<b>Date DPIA form completed:</b>	Date the form was completed
<b>DPIA reference no:</b>	This reference will have been allocated by the DPO and will show on the final section of the 'Screening Questions' template

**Please note: the IAO will need to sign this DPIA off in order to demonstrate that they are aware of the system / process they will have responsibility for.**

**This document should be read in conjunction with the DPIA screening questions completed prior to this document in order to assess whether there is an impact on privacy / confidentiality with the introduction of this new / changed system**

## 2) Key questions

**NB: Please use the 'comments' section to provide further information**

Question		Response	Comment
2.1	Will the system involve the processing of personal identifiable data or confidential data?	Yes / No  Details to be provided in section 2.4	Details of what personal information can be stated at 2.4
2.2	Is this a new use or personal information or a changed or unchanged use of personal information that it already collected?	New / changed / unchanged	New / changed – self-explanatory.  Unchanged – if information is already being processed but a new process is being introduced. E.g. a new addition to the functionality of CAD
2.3	State the purpose for the processing of the data (e.g. <i>patient treatment, administration, audit, research etc.</i> )	Please provide as much detail as possible in the comments section	Please provide as much information as possible – rather than just 'healthcare' as there may be differing levels of healthcare e.g. direct or indirect

2.4	Please select personal data items that will be collected:	<input type="checkbox"/> Personal / administration details (e.g. name, address, contact details, age, gender, HSC no., NI no.)	Please tick all that apply and provide in the comments box details of the exact information being processed for 'Personal / administration details', Education and training skills', 'Employment details' and 'Financial details'.
		<input type="checkbox"/> Education and training details (i.e. qualifications, skills database, training records)	See above
		<input type="checkbox"/> Employment details (i.e. career history, recruitment and termination details, attendance records, appraisals)	See above
		<input type="checkbox"/> Financial details (i.e. income, salary, investments)	See above
		<input type="checkbox"/> Racial or ethnic origin	
		<input type="checkbox"/> Political opinions	
		<input type="checkbox"/> Religious & other beliefs	

		<input type="checkbox"/> Trade Union membership	
		<input type="checkbox"/> Physical or mental health condition	
		<input type="checkbox"/> Sexual life / orientation	
		<input type="checkbox"/> Gender reassignment	
		<input type="checkbox"/> Marriage / civil partnership	
		<input type="checkbox"/> Offences (including alleged)	
		<input type="checkbox"/> Criminal proceedings	
		<input type="checkbox"/> Clinical data	
		<input type="checkbox"/> Other unique identifier	Please specify <b>Please include in here details of any information being processed that does not fall within one of the above boxes.</b>
2.5	<p>Identifying if the collection of personal / confidential information is necessary to meet the purpose of the system:</p> <ul style="list-style-type: none"> <li>Will the processing actually achieve the</li> </ul>	Please provide details in the comments section.	<p><b>Consideration must be made to the amount of personal information being processed and whether this is all necessary for the purpose.</b></p> <p><b>It is useful to provide a reason why the amount of information being processed is necessary.</b></p>

	<p>stated purpose?</p> <ul style="list-style-type: none"> <li>• Is the amount of personal / confidential information proportionate to that purpose?</li> <li>• Can the same purpose be achieved without processing the personal / confidential information ?</li> <li>• Can the same result be achieved by processing less data?</li> </ul>		
2.6a	<p>Are other organisations involved in the processing of the data?</p> <p>If 'yes', are they registered with the Information</p>	<p>Yes / No</p> <p>If 'yes' please provide their details</p> <p>Yes / No</p> <p>If 'yes' – please enter their Data Protection</p>	<p>This can include contractors or third parties.</p> <p>The registration number can be found on the ICO website:</p> <p><a href="https://ico.org.uk/ESDWebPages/Search">https://ico.org.uk/ESDWebPages/Search</a></p> <p>If unsure, the DPO will be able to assist.</p>

	Commissioner's Office (ICO)?  <i>(advice available from the Data Protection Officer)</i>	notification number in the comments section	
2.6b	If 'yes' to section 2.6a, does the 'other' organisation hold any security accreditation	Yes / No  If 'yes' please provide details	Details of any accreditation e.g. ISO27001, should be available from the organisation's website
2.6c	If 'yes' to section 2.6a, does the 'other' organisation have a privacy notice on their website	Yes / No  If 'yes' please copy the web link in the comments box	Privacy notices are a legal requirement and should contain information about Information Governance compliance etc. They can often be located at the foot of the home page of their website
2.7a	If other organisations are involved, is there a 3 <sup>rd</sup> party contract or processing agreement in place that contains the required Information Governance	Yes / No  If 'yes' – please provide details in the comments section.  Please provide a copy of the contract or processing agreement	We need to be able to assure ourselves that any other organisations involved have adequate levels of IG compliance, security etc. in place.

	clauses including Data Protection and Freedom of Information?	<p>If 'no' – please provide details as to any other documentation that may be in place e.g. Service level agreement, Memorandum of understanding etc.</p> <p>Please provide a copy of any relevant documentation</p>	
2.7b	Does the work involve employing contractors external to the organisation?	<p>Yes / No</p> <p>If 'yes', please provide a copy of the confidentiality agreement or contract</p>	See 2.7a above
2.8	What is the source of the information / where will the information being processed be gathered from? (e.g. <i>patients, staff, another system</i> )	Please provide details in the comments section	Where will the information being processed in the system have originated from e.g. information in CAD may have come from the patient, a third party, police or another health care professional

2.9	<p>What is the legal basis for processing of personal data? (under the General Data Protection Regulation (GDPR))</p> <p><i>(advice available from Data Protection Officer)</i></p>	<p><input type="checkbox"/> Art 6(1)(a) Consent Where consent is the legal basis, please give details of how the consent will be obtained and recorded</p> <p><input type="checkbox"/> Art 6(1)(b) Contract</p> <p><input type="checkbox"/> Art 6(1)(c) Legal obligation</p> <p><input type="checkbox"/> Art 6(1)(d) Vital interests</p> <p><input type="checkbox"/> Art 6(1)(e) Public task</p> <p><input type="checkbox"/> Art 6(1)(f) Legitimate interests Where legitimate interests is the legal basis please provide details of what these are</p>	<p>One of these must be ticked if personal information is being processed. Consent should be the last option as this has additional complexities attached.</p> <p>If unsure, this column can be used to add in details and the DPO can assess which legal basis applies.</p>
2.10 a	<p>What is the legal basis for processing special category data?</p>	<p><input type="checkbox"/> Art 9(2)(a) Explicit consent Where consent is the legal basis, please give details of</p>	<p>One of these must be ticked if information about any of the following is being processed:</p> <p>Health Racial or ethnic origin Religious or philosophical beliefs</p>



	(advice available from Data Protection Officer)	how the consent will be obtained and recorded	<p>Trade Union membership Biometric / genetic Political opinions Sex life or sexual orientation</p> <p>As 2.10a, consent should be the last option to consider as there are added complexities.</p> <p>If unsure, this column can be used to add in details and the DPO can assess which legal basis applies.</p>
		<input type="checkbox"/> Art 9(2)(b) Employment, social security and social protection law	
		<input type="checkbox"/> Art 9(2)(c) Vital interests	
		<input type="checkbox"/> Art 9(2)(d) Not for profit bodies	
		<input type="checkbox"/> Art 9(2)(e) Made public by the data subject	
		<input type="checkbox"/> Art 9(2)(f) Legal claims	
		<input type="checkbox"/> Art 9(2)(g) Substantial public interest	
		<input type="checkbox"/> Art 9(2)(h) Health or social care	
		<input type="checkbox"/> Art 9(2)(l) Public health	
		<input type="checkbox"/> Art 9(2)(j) Archiving, research and statistics	
2.10 b	If the legal basis is Art9 (2) (i), does this fall within the scope of the National Data Opt-out?	Yes / No / Not relevant.	This would only apply if the legal basis chosen in 2.10b is 'archiving, research and statistics'

2.11	Have individuals / other stakeholders been involved in a consultation process?	<p>Yes / No</p> <p>If 'yes' provide details of the consultation process</p> <p>If 'no' explain why this is</p>	Individuals may need to be consulted on new systems processes that involve their personal information. This is not always the case, in particular in the case of processing health information for direct care or for a legal requirement.
2.12	How will the accuracy and completeness of information in the system be maintained?	Please provide details in the comments section:	What are the quality assurance processes for the information? E.g. are there any pre-set parameters
2.13	Will the new system allow for data to be amended?	<p>Yes / No</p> <p>If 'no' please provide details as to why this isn't possible</p>	Is it possible to retrospectively amend any inaccuracies?
2.14	Who will have access to information in the system?	Please provide details in the comments section.	List who will have access – this should not be names – just job roles, departments etc.
2.15	How will the information in the system be accessed?	Please provide details in the comments section	Provide details on how access is provided e.g. Smartcard, login and password etc. State if the login is generic or individually assigned
2.16	Will the system allow for auditing of	Yes / No	Is it possible to audit who has had access, what has been accessed and is a reason for access noted?

	access to the information?	If 'no' please provide details as to why this isn't possible	
2.17	Is there a process in place to allow for individuals to request access to their personal information?	Yes / No  If 'yes' – please provide details in the comments section	The standard answer for this for internal systems is:  'Yes – the subject access process is managed by the Information Governance Team. Please see the Data Protection Rights Policy for further information'  If information is being processed on our behalf by a third party, details of their subject access process will need to be included
2.18	Is there a process in place where an individual can request that their personal information is rectified or forgotten?	Yes / No  If 'yes' – please provide details in the comments section	The standard answer for this for internal systems is:  'Yes – the subject access process is managed by the Information Governance Team. Please see the Data Protection Rights Policy for further information'  If information is being processed on our behalf by a third party, details of their subject access process will need to be included
2.19	Where will information in the system be stored?	Please provide details in the comments section	Provide information on whether data is hosted in house or externally. If external, further information will be required as to the security of the external provider (see 2.19 below)
2.20	If the information is being stored externally,	Please provide details in the comments section	Information about the external supplier's security arrangements need to be included, including access controls, system security etc. If this involves paper records,

	what security arrangements are in place?		physical building security, protection etc. will also need to be included.
2.21	What is the data retention period for data in the system?	Please provide details in the comments section	Reference should be made to the NIAS Retention and Disposal of Information Schedule (available in the library) or the Records Management Code of Practice for Health and Social Care (2016): <a href="https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016">https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016</a>
2.22	How will data in the system be destroyed at the end of the retention period?	Please provide details in the comments section	Will information be deleted, sent to an archive facility, repatriated etc.
2.23	Does the system involve sending information off site?	Yes / No  If 'yes' – please provide details in the comments section If 'yes' – give details of the method of transport/transfer to be used in the comments section If 'yes' – will any personal	This is quite self-explanatory. Please provide details of transfer methods – including what security is in place when transferring e.g. encryption.  If data is transferred, is any going out of the EEA. If so, provide details of the security in place in that country / area.

		or sensitive data be transferred outside the European Economic Area? Please provide details of what data will be sent, and where in the comments section.	
2.24	How will individuals be informed about the proposed use of their personal information? (e.g. leaflets, privacy notice)	Please provide details in the comments section.	Are individuals being notified as part of this new process / system about the use of their information? If so, how. If not, is it already included in the Trust privacy notice (available on the Trust website – ‘Your Information’ section). If it is not in the notice, please note here that the notice will need to be updated – this will then be picked up by the DPO.
2.25	Will staff be trained in the use of the system prior to implementation?	Yes / No  If ‘no’ please provide justification as to why training will not be provided.	Staff should be trained in the use of a new system / process prior to being allowed access to ensure they are fully aware of any security / Information Governance implications and responsibilities
2.26	Is there a business continuity / disaster recovery plan	Yes / No  If ‘no’ please provide details of the	If ‘no’ – what measures are in place if there is a failure – how is information protected etc.

	in place if the system fails?	measures in place to protect information in the event of a failure	
2.27	Will there be any reports run?	Yes / No  If 'yes' provide details of whether they will contain personal / confidential information, who will be the recipients and how are they sent securely in the comments section.	Provide information on recipients, in particular any external to the Trust. What level of security is on these reports?

### 3) Cloud service considerations

**This section requires completing if a 'Cloud' based solution is involved.**

The answers to the following questions should be included within the contract with the provider.

Question		Response	Comment
3.1	Why is a cloud-based solution being considered over an in-house solution?	Please provide details in the comments section.	This could be taken from a business case for the process / system.
3.2	What type of data will be hosted in the cloud?	Please provide details in the	Please provide details of what information will

		comments section.	be hosted e.g. personal, corporate etc.
3.3	What cloud service provider is being used?	Please provide details in the comments section.	Name of supplier
3.4	Will the cloud service be hosted on the HSCN network?	Please provide details in the comments section.	This is the health and social care secure network
3.5	What measures have been put in place in the event of the service provider ceasing to operate?	Please provide details in the comments section.	Self-explanatory – what will happen to the data etc.
3.6	What security measures are in place for the asset in the cloud service, including protection from cyber security attacks, control of user access to the data, secure transfer of data between the cloud service provider and the Trust?	Please provide details in the comments section.	Self-explanatory – provide as much information as possible
3.7	Has an assessment of the cloud service providers financial position and solvency been performed?	Yes / No  If 'yes' what was the outcome?  If 'no' the reason why this hasn't been undertaken.	Self-explanatory
3.8	What measures have been put in place to repatriate data from the asset in the cloud service back to the Trust, at the end of the service contract?	Please provide details in the comments section, including any additional infrastructure requirements and	Self-explanatory – provide as much information as possible

		associated costs to the Trust.	
3.9	Has the legal ownership of any data that is uploaded to the asset in the cloud service been identified?	Please provide details in the comments section.	This should be included in any contract with the provider

#### 4) Data flow

This section describes the data owners and processors, and the flow of data between them. Please detail the data flow for the proposed system / project in a flow chart below. (An example of a data flow is below).



Data flow.pdf

This does not have to be too complex, however, it will need to clearly show any flows between organisations as well as those internally



## 5) Risk management

An essential element of the DPIA process is the assessment of risks, and identification of actions that will mitigate the risk from occurring or make the situation acceptable if the risk materialised. Record any new risks identified from performing the DPIA here.

Any risks identified by implementing or not implementing this process / system should be logged here, along with scores before and after mitigation. It should also be noted where any risks will be managed / monitored

Risk ID	Description	Consequence on the data subject of the risk occurring (1-5)	Likelihood of the risk occurring (1-5)	S c o r e	Is the risk Accepted or Mitigated – give details	Consequence following mitigation (1-5)	Likelihood following mitigation (1-5)	S c o r e
This will be allocated by the DPO	There is a risk to ..... If .....				.			

If the risk is not accepted, please identify where these risks will be monitored:

The risks identified as part of this DPIA process will be monitored at

.....  
...

## 6) References

List any policies, procedures, guidance or legislation referred to within the DPIA here.

### Record of Approval

Information Asset Owner Approval:	
Name:	
Title:	
Signature:	
Date:	

Information Security and Technical Operations Manager Approval:	
Name:	
Title:	
Signature:	
Date:	

Data Protection Officer Approval:	
Name:	
Title:	
Signature:	
Date:	

### For completion by Data Protection Officer:

Document Status:	
DPIA Status:	Approved / Rejected
Comments:	

<b>Publication and Accountability:</b>			
<b>Included in privacy notice</b>	Yes / No	<b>Date included in privacy notice:</b>	If not included, reason why not:
<b>Included in Record of Processing Activities (ROPA)</b>	Yes / No	<b>Date included in ROPA:</b>	If not included, reason why not:



## DATA PROTECTION POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation
- Data Protection Rights Procedure
- Code of Conduct for Confidentiality
- Employees Guide to Confidentiality and Security
- The Information Governance Review (AKA Caldicott 2) 2013
- Information Lifecycle Management Policy
- Archiving Procedure
- Information Disclosure and Transfer Policy
- Retention and Disposal of Information Schedule
- Safe-haven Policy
- Children's Act 2004
- ICO's Data Sharing Code of Practice – May 2011
- Safeguarding Children Policy
- Safeguarding Adults Policy
- Information Sharing Policy
- Data Protection Impact Assessment Policy and Procedure
- Review of Data Security, Consent and Opt-Outs (2016)
- Working Together to Safeguard Children (2015)
- Information Sharing: Advice for practitioners providing safeguarding

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Data Protection Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy and Procedure for NIAS

## Contents

1. Introduction.....	3
2. Objectives.....	4
3. Scope.....	5
4. Definitions.....	5
4.1 Personal information .....	5
4.2 Special category data.....	5
4.3 Processing.....	5
4.4 Data subject .....	5
4.5 Recipient.....	5
4.6 Third party.....	6
4.7 Data Protection legislation .....	6
4.8 Notification .....	6
5. Responsibilities.....	6
5.1 Data Protection Officer.....	6
5.2 Corporate Services Manager .....	6
5.3 All NIAS staff .....	6
5.4 Duties relating to confidentiality and the protection of personal data:.....	7
6. Data Protection principles .....	7
7. Special category data.....	9
8. Conditions for processing.....	9
9. Fair processing notices .....	11
10. Information sharing.....	11
11. Information sharing – safeguarding children and adults .....	12
12. Rights of individuals.....	14
13. Data Protection Impact Assessments.....	14
14. Sanctions.....	14
15. Incident reporting.....	15
16. Abuse of privilege.....	15
17. Additional assurances.....	16
18. Consultation.....	17
19. Monitoring compliance and effectiveness of the policy.....	17
Plan for Dissemination of Procedural Document .....	22

## 1. Introduction

- 1.1 In order to operate, Northern Ireland Ambulance Service HSC Trust (NIAS) needs to collect and use certain types of

personal information about the people we deal with on a day-to-day basis. These include current, past and prospective employees, patients, suppliers, customers/clients and others with whom we communicate. In addition, we may occasionally be required, by law, to collect and use personal information to comply with Government requirements. This personal information must be handled properly however it is collected, recorded and used and includes information held either on paper or electronically.

- 1.2 The General Data Protection Regulation (GDPR) came into full effect on 25 May 2018. This procedure details how NIAS will comply with its legal obligations under the GDPR, and the supporting UK Data Protection Act 2018, relating to the rights of individuals. Following Brexit the UK adopted this regulation for enforcement and renamed it UK GDPR.
- 1.3 Data Protection legislation legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for information relating to deceased persons.
- 1.4 One aspect of the Data Protection legislation relates to the rights of individuals with regard to their personal information. Details of these rights and how to manage them is included in the Data Protection Rights Procedure.
- 1.5 The correct handling of personal information by NIAS is considered very important. Failure to do so would undermine the confidence felt in us by the general public, its stakeholders and its employees. To this end, NIAS ensures that personal information is treated lawfully, correctly and with respect.

## **2. Objectives**

The key objectives of this policy are:

- 2.1 To ensure that personal information is processed in accordance with the requirements of Data Protection legislation.



- 2.2 To meet the requirements of the Data Security and Protection Toolkit, which is a component of the Care Quality Commission Key Lines of Enquiry.
- 2.3 To provide guidance on the correct way to handle requests for personal Information.

### **3. Scope**

- 3.1 This policy, applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who come into contact with personal information.
- 3.2 All employees allocated responsibility for responding to access requests by data subjects will be aware of the legal obligations NIAS is under.

### **4. Definitions**

#### **4.1 Personal information**

- 4.1.1 Personal information is information that can be used to identify an individual.

#### **4.2 Special category data**

- 4.2.1 Special category data is personal data which is more sensitive so needs more protection (see section 7 for list of categories)

#### **4.3 Processing**

- 4.3.1 Processing is carrying out any function on the data including obtaining, amending, deleting and disclosing.

#### **4.4 Data subject**

- 4.4.1 The data subject is the individual who is the subject of the personal information

#### **4.5 Recipient**

4.5.1 Someone other than the data subject who may receive the personal information

#### **4.6 Third party**

4.6.1 Someone other than the subject of the personal information

#### **4.7 Data Protection legislation**

4.7.1 Legislation, including but not limited to, the GDPR and UK Data Protection Act 2018

#### **4.8 Notification**

4.8.1 Although notification is not a requirement of the Data Protection legislation, the Digital Economy Act 2017 (s108) requires all organisations processing personal information to register and pay a fee, based upon staff numbers and volume of personal data processed, to the Information Commissioner's Office (ICO).

### **5. Responsibilities**

#### **5.1 Data Protection Officer**

5.1.1 Responsibility for compliance with Data Protection legislation falls under the remit of the Data Protection Officer (DPO). This role is undertaken by the Head of Information Governance.

#### **5.2 Corporate Services Manager**

5.1.1 The Corporate Services Manager is responsible for the processing and management of right of access requests and for responding to patient queries regarding the sharing of information.

#### **5.3 All NIAS staff**

5.3.1 All NIAS staff whether clinical or administrative, who come into contact with personal information have a responsibility to ensure this is processed in accordance with Data Protection legislation.

## **5.4 Duties relating to confidentiality and the protection of personal data:**

- 5.4.1 All HSC bodies have a common law duty of confidence to patients and staff alike. Everyone working for NIAS who records, handles, stores or otherwise comes across patient or personal information has a duty to maintain this confidentiality.

## **6. Data Protection principles**

- 6.1 Data Protection legislation is based around six principles relating to the processing of personal data with an additional principle of 'accountability' all of which must be adhered to, to maintain compliance. NIAS fully endorses and adheres to these principles.

- 6.2 The six principles as detailed in the Data Protection legislation are:

1. Personal data shall be:

- (a) Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
- (b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation')
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- (d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which

they are processed, are erased or rectified without delay ('accuracy')

- (e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation')
  - (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')
2. The controller shall be responsible for, and be able to demonstrate, compliance with the principles ('accountability')

### 6.3 Therefore, NIAS will:

- ensure the conditions surrounding the fair and lawful collection and use of personal data are adhered to (see section 7)
- Ensure the purposes for which personal data is processed are transparent and unambiguous.
- collect and process appropriate data, and only to the extent it is necessary to fulfil the operational needs of NIAS or to comply with legal obligations
- ensure the quality and timeliness of the personal data held
- ensure procedures are in place to determine the retention needs of personal data held

- ensure the technical and organisational measures in place to protect data are appropriate and effective
- Ensure the rights of the individuals, who are the subjects of the data held, are respected and can be fully exercised as detailed in Data Protection legislation. (see section 12)

## **7. Special category data**

7.1 The following types of data are classed as ‘special category’ and are

Identified with Data Protection legislation as being more sensitive:

- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

## **8. Conditions for processing**

8.1 In order to process personal data, there must be a valid lawful basis

– Condition for processing. There are six available lawful bases for processing and none is considered better or more important than another. One of these must support the processing for it to be lawful, and this should be recorded. Privacy notices should also reflect these lawful bases.

- a) Consent: the individual has given clear consent to the processing of their personal data for one or more specific purposes
- b) Contract: processing is necessary for a contract you have with the data subject, or because they have asked to take specific steps before entering into a contract

- c) Legal obligations: the processing is necessary to comply with the law
- d) Vital interests: the processing is necessary to protect the vital interests (the life) of the data subject or another individual
- e) Public task: the processing is necessary to perform a task in the public interest or to perform the organisation's authorised task or function
- f) Legitimate interests: the processing is necessary for the organisations legitimate interests (**please note: this can only be used by a public authority if the action does not fall within its public task**) Advice should be sought from the DPO when applying this condition.

If special category data is being processed, one of the above must apply plus one of the following:

- a) Consent: the data subject has given *explicit* consent to the processing of their personal data.
- b) Employment and social security obligations: processing is necessary for the purposes of carrying out obligations in the field of employment and social security and social protection law.
- c) Vital interests: the processing is necessary to protect the vital interests of the data subject, or another individual, where they are incapable of giving consent
- d) Legitimate activities (not for profit): processing is carried out for the legitimate interests of a foundation, association or not-for-profit organisation
- e) Public information: the processing involves data which are manifestly made public by the data subject
- f) Legal claims: processing is necessary for the establishment, exercise or defence of legal claims
- g) Public interest: processing is necessary for reasons of substantial public interest
- h) Medical / social care: processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems
- i) Public health: processing is necessary for reasons of public interest in the area of public health

- j) Research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

## **9. Fair processing notices**

9.1 Individuals should be made aware of how and why their personal information may be shared. Fair processing (or privacy) notices are available on the NIAS website, on NIAS vehicles and in leaflets provided to patients.

9.2 The 'right to be informed' is linked to the provision of fair processing notices. Notices must contain the following information, and be reviewed on a regular basis:

The following information must be provided:

- The name and contact details of NIAS
- The contact details of the Data Protection Officer
- The purposes for processing personal data
- The legal basis for the processing
- Recipients of the personal data
- Details of any overseas transfers
- Retention periods for personal data
- Reference to the rights of individuals
- How to withdraw consent to processing (if this was the legal basis for processing)
- How to lodge a complaint

Further information can be found in the Data Protection Rights procedure.

## **10. Information sharing**

10.1 Data Protection does not prevent the sharing of information, it Legislates for how this can be done lawfully.

10.2 Information sharing agreements are used to manage the sharing Of information with partner organisations.

10.3 Reference should be made to the Information Sharing Policy for Guidance on how to share information appropriately.

10.4 Personal information will be anonymised wherever possible. If anonymisation is not possible, every attempt will be made to contact the data subject to obtain their consent to share if the sharing is for non-direct healthcare purposes or a legal basis is not available.

10.5 The IG and Compliance Team will manage and respond to any patient queries around the use and sharing of their information and will provide further explanations when required.

## **11. Information sharing – safeguarding children and adults**

11.1 Section 11 of the Children Act 2004 places duties on a range of organisations and individuals to ensure their functions and any services that they contract out to others are discharged having regard to the need to safeguard and promote the welfare of children.

Working Together (2015) provides clear guidance in line with section 11 on an organisation and professional responsibilities in relation to data protection and information sharing. They expect that:

- all organisations should have arrangements in place which set out clearly the processes and the principles for sharing information between each other, with other professionals and with the Local Safeguarding Children's Board (LSCB); and
- No professional should assume that someone else will pass on information which they think may be critical to keeping a child safe. If a professional has concerns about a child's welfare and believes they are suffering or likely to suffer harm, then they should share the information with local authority children's social care.

Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents



and carers (2015) supports frontline practitioners working in child or adult services who have to make decisions about sharing personal information on a case by case basis. The advice includes the seven golden rules for sharing information effectively and can be used to supplement local guidance and encourage good practice in information sharing. All staff that suspect that a child is being, or at risk of being, abused should complete a safeguarding referral.

11.2 The Care Act 2014 is succinct in a provider's role regarding safeguarding adults at risk of abuse and an organisations and professional's responsibility in relation to data protection.

Gaining consent for a referral is recognised as best practice to ensure that information is shared safely and in line with the making safeguarding personal principles.

There is an expectation that agencies will set up information sharing agreements governing the sharing of information and in line with the principles set out in the 2013 Caldicott review that:

- information will only be shared on a 'need to know' basis when it is in the interests of the adult
- confidentiality must not be confused with secrecy
- informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement
- It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk.

Where an adult has refused consent to information being disclosed for these purposes, then practitioners must consider whether there is an overriding public interest that would justify information sharing (for example, because there is a possibility that others are at risk of serious harm).

The decision about who needs to know and what needs to be known about the suspected abuse must be made on a case by case basis. All staff who suspect that an adult is

being, or at risk of being, abused should complete a safeguarding referral.

## **12. Rights of individuals**

Data Protection legislation provides several rights to data subjects. These rights are:

- the right of be informed
- the right of access by the data subject
- the right to rectification
- the right of erasure ('right to be forgotten')
- the right to restriction of processing
- the right to data portability
- the right to object
- rights in relation to automated decision making and profiling

Details of these rights and procedural guidance on how these rights are to be processed in practice can be found in the Data Protection Rights Procedure.

## **13. Data Protection Impact Assessments**

13.1 Under Data Protection legislation there is an obligation to implement technical and organisational measures to demonstrate that data protection and security measures have been considered at the outset of a project. This is known as 'data protection by design and default'.

13.2 A Data Protection Impact Assessment (DPIA) is a process designed to help identify any identity and minimise and data protection risks.

13.3 Further information on DPIAs and the process can be found in the Data Protection Impact Assessment Policy and Procedure.

## **14. Sanctions**

14.1 Failure to comply with Data Protection legislation can expose NIAS to a number of sanctions that can be imposed by the ICO. The level of sanction will be dependent on the infringement:

Tier one – maximum financial penalty of €10,000,000 or 2% of annual turnover

Tier two – maximum financial penalty of €20,000,000 or 4% of annual turnover

The table in Appendix 1 shows which infringements fall under which Tier (based upon the articles in the GDPR)

14.2 As well as financial penalties, the ICO has additional powers:

- Information Notice: this requires the organisation to provide the ICO with specific information within a specified period of time
- Audits: The ICO can conduct unannounced audits
- Enforcement Notice: This compels an organisation to take the action specified in the notice to bring about compliance with Data Protection. Failure to comply with an Enforcement Notice can be a criminal offence.

## **15. Incident reporting**

15.1 Data Protection legislation dictates that serious data breaches must be reported within 72 hours of discovery. Failure to do so can attract a tier one fine.

15.2 Data breaches will be reported via the internal incident reporting process with the Data Protection Officer assessing the severity. Incidents identified as serious based upon the Data Security and Protection Toolkit incident reporting tool will be reported via that method.

## **16. Abuse of privilege**

16.1 It is strictly forbidden for employees to access any information relating to their own family, friends or acquaintances without consent. Looking at patient or staff

records out of curiosity is totally unacceptable. Disciplinary proceedings will be instigated should abuse of privilege be discovered.

## **17. Additional assurances**

17.1 NIAS will make further assurances relating to the fair and lawful processing of personal data in order to provide additional safeguards for the protection of this information.

- An appropriately trained Data Protection Officer will be appointed with a direct reporting line to the NIAS Board.
- Everyone handling personal data is appropriately trained to do so in accordance with the requirements of Data Protection legislation. All aspects of IG, including data protection, are covered in the essential learning and induction programmes which form part of the NIAS mandatory training requirements
- Everyone is fully aware of the need for strict confidentiality with regard to the processing of personal data.
- Everyone is aware of the importance of maintaining the accuracy of the personal data held.
- Policies are in place regarding the management of information and the retention and disposal of records held, including any legal obligations.
- Everyone is aware of the NIAS IM&T Security Policy.
- Anyone wishing to make an enquiry about the handling/managing of personal data knows what to do or who to contact for assistance.
- Everyone is aware of the need to limit information held to that which is relevant and of the importance of not including personal opinions about an individual.
- Requests for personal information are handled promptly and in accordance with the timescales detailed in Data Protection legislation.

- Everyone is aware of the procedure for handling subject access requests

## **18. Consultation**

- 18.1 This policy will be presented to the IG Group for consultation. The group has delegated authority to approve this document.

## **19. Monitoring compliance and effectiveness of the policy**

- 19.1 This policy will be reviewed annually by the Head of IG and approved by the IG Group, which reports in to the Finance and Performance Committee, a committee of the NIAS Board.
- 19.2 This policy will meet the requirements of the Data Security and Protection Toolkit, which is a component of the Care Quality Commission Key Lines of Enquiry.
- 19.3 National guidance issued by the Information Commissioner's Office (ICO) will be monitored and included within this policy should it be deemed relevant.
- 19.4 All requests made by individuals relating to their rights will be logged and monitored to ensure that legal obligations are adhered to.
- 19.5 Awareness training in Data Protection is included within the essential education and corporate induction programmes.
- 19.6 The Data Protection notification will be maintained by the Head of IG.
- 19.7 Patient queries around the use and sharing of information will be logged and used as a learning tool to review publications around the use of information.



<b>Tier one - €10,000,000 – or 2% of annual turnover</b>
(article 8) conditions applicable to child's consent in relation to information society services ( <i>relate to providing web services to children</i> )
(article 11) processing which does not require identification ( <i>using identifiable data when it is not necessary</i> )
(article 25) data protection by design and default ( <i>see section 13</i> )
(article 26) joint controllers ( <i>not agreeing on joint responsibilities to comply with legislation</i> )
(article 27) representatives of controllers of processors not established in the Union ( <i>not having sufficient safeguards in place when GDPR does not apply</i> )
(article 28) processor ( <i>processor does not abide by agreement with controller</i> )
(article 29) processing under the authority of the controller or processor ( <i>processing data outside of authorised instruction</i> )
(article 30) records of processing activities ( <i>not having a log of processing activities i.e. an information asset register</i> )
(article 31) cooperation with the supervisory authority ( <i>not co-operating with the ICO</i> )
(article 32) security of processing ( <i>not abiding by security requirements</i> )
(article 33) notification of a personal data breach to the supervisory authority ( <i>not advising the ICO of a breach</i> )
(article 34) communication of a personal data breach to the data subject ( <i>not informing a data subject their information has been the subject of a breach</i> )
(article 35) data protection impact assessment ( <i>see section 13</i> )
(article 36) prior consultation ( <i>not consulting the ICO if processing is considered high risk</i> )
(article 37) designation of a Data Protection Officer ( <i>not appointing a Data Protection Officer</i> )
(article 38) position of the Data Protection Officer ( <i>not supporting the Data Protection Officer in undertaking their duties</i> )
(article 39) tasks of the Data Protection Officer ( <i>Data Protection Officer not having correct tasks assigned</i> )
(article 42) certification ( <i>relates to certification not yet in force</i> )
(article 43) certification bodies ( <i>relates to certification not yet in force</i> )
<b>Tier two - €20,000,000 – or 4% of annual turnover</b>
(article 5) principles relating to processing of personal data ( <i>not abiding by the principles – see section 6</i> )

(article 6) lawfulness of processing ( <i>not abiding by the conditions for processing – see section 8</i> )
(article 7) conditions for consent ( <i>not abiding by responsibilities for obtaining lawful consent</i> )
(article 9) processing of special categories of personal data ( <i>not abiding by the conditions for processing – see section 8</i> )
(article 12) transparent information, communication and modalities for the exercise of the rights of the data subject ( <i>not supporting the provision of information in accordance with the rights of individuals</i> )
(article 13) information to be provided where personal data are collected from the data subject ( <i>not having adequate privacy notices – see section 9</i> )
(article 14) information to be provided where personal data have not been obtained from the data subject ( <i>not having adequate privacy notices – see section 9</i> )
(article 15) right of access by the data subject ( <i>not complying with the rights of individuals – see section 12</i> )
(article 16) right to rectification ( <i>not complying with the rights of individuals – see section 12</i> )
(article 17) right to erasure ('right to be forgotten') ( <i>not complying with the rights of individuals – see section 12</i> )
(article 18) right to restriction of processing ( <i>not complying with the rights of individuals – see section 12</i> )
(article 19) notification obligation regarding rectification or erasure of personal data or restriction of processing ( <i>not complying with the rights of individuals – see section 12</i> )
(article 20) right to data portability ( <i>not complying with the rights of individuals – see section 12</i> )
(article 21) right to object ( <i>not complying with the rights of individuals – see section 12</i> )
(article 22) automated individual decision-making, including profiling ( <i>not complying with the rights of individuals – see section 12</i> )
(article 44) general principle for transfers ( <i>transfers made which are not compliant with legislation</i> )
(article 45) transfers on the basis of an adequacy decision ( <i>transfers made without adequate consideration of risk</i> )
(article 46) transfers subject to appropriate safeguards ( <i>transfers made without sufficient safeguards in place</i> )
(article 47) binding corporate rules ( <i>not abiding by agreed binding corporate rules</i> )



(article 48) transfers or disclosures not authorised by Union law ( <i>court judgements only apply if based on international agreement</i> )
---

(article 49) derogations for specific situations ( <i>additional infringements as identified by UK law</i> )
--

## Appendix 2

### Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Data Protection Policy</b>		
<b>Version Number:</b>	<b>V1.0</b>	<b>Dissemination lead: Print name, title and contact details</b>	<b>Tracy Avery, Head of Information Governance &amp; Data Protection Officer Tracy.Avery@nias.hscni.net</b>
<b>Previous document already being used?</b>	<b>No</b>		
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	All staff need to be aware of the legalities of the Data Protection legislation and how it impacts on them and service users		
<b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b>  Some examples of methods of disseminating information on procedural documents include:  <ul style="list-style-type: none"><li>• <i>Information cascade by managers</i></li><li>• <i>Communication via Management/</i></li></ul>		<ul style="list-style-type: none"><li>• Information cascade by managers</li><li>• Notification via articles in bulletins</li><li>• Posting on the Intranet</li></ul>	

<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Data Protection Policy provides staff with the detail and guidance required on how the legalities of Data Protection impact on themselves and service users.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*



## DATA PROTECTION RIGHTS PROCEDURE

### Links

The following documents are closely associated with this policy:

- Data Protection legislation
- Data Protection Policy
- Information Disclosure and Transfer Policy
- Clinical Record Keeping Policy
- Data Quality Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy and procedure for NIAS

## Contents

1. Introduction.....	3
2. Objectives.....	4
3. Scope.....	4
4. Definitions.....	5
4.1 Personal information .....	5
4.2 Processing.....	5
4.3 Data subject.....	5
4.4 Recipient.....	5
4.5 Third party .....	5
4.6 Data Protection legislation.....	5
5. Responsibilities.....	5
5.1 Data Protection Officer .....	5
5.2 Corporate Services Manager.....	6
5.3 All NIAS staff.....	6
5.4 Duties relating to confidentiality and the protection of personal data.....	6
6. Rights under Data Protection legislation .....	6
7. Procedural guidance on respecting individuals' rights .....	7
7.1 The right to be informed .....	7
7.2 The right of access.....	8
7.3 The right to rectification .....	9
7.4 The right to erasure.....	11
7.5 The right to restriction of processing.....	12
7.6 The right to data portability.....	13
7.7 The right to object .....	14
7.8 Rights in relation to automated decision making and profiling.....	14
8. Consultation.....	14
9. Monitoring compliance and effectiveness of the policy .....	15
Appendix 2 .....	18
Plan for Dissemination of Procedural Document.....	18

## 1. Introduction

- 1.1 In order to operate, Northern Ireland Ambulance Service HSC Trust (NIAS) needs to collect and use certain types of

personal information about the people we deal with on a day-to-day basis. These include current, past and prospective employees, patients, suppliers, customers/clients and others with whom we communicate. In addition, we may occasionally be required, by law, to collect and use personal information to comply with Government requirements. This personal information must be handled properly however it is collected, recorded and used and includes information held either on paper or electronically.

- 1.2 The General Data Protection Regulation (GDPR) came into full effect on 25 May 2018. This procedure details how NIAS will comply with its legal obligations under the GDPR, and supporting UK Data Protection legislation, relating to the rights of individuals.
- 1.3 Data Protection legislation legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for information relating to the deceased.
- 1.4 The correct handling of personal information by NIAS is considered very important. Failure to do so could undermine the confidence felt in us by the general public, its stakeholders and its employees. To this end, NIAS ensures that personal information is treated lawfully, correctly and with respect.

## **2. Objectives**

The key objectives of this procedure are:

- 2.1 To ensure that the rights of individuals, under Data Protection legislation, are respected.
- 2.3 To provide guidance on the procedural aspects of respecting these rights.

## **3. Scope**

- 3.1 This procedure, applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who come into contact with personal information.



- 3.2 All employees' allocated responsibility for responding to requests by data subjects to invoke their rights will be aware of the legal obligation NIAS is under.

## **4. Definitions**

### **4.1 Personal information**

- 4.1.1 Personal information is information that can be used to identify an individual.

### **4.2 Processing**

- 4.2.1 Processing is carrying out any function on the data including obtaining, amending, deleting and disclosing.

### **4.3 Data subject**

- 4.3.1 The data subject is the individual who is the subject of the personal information

### **4.4 Recipient**

- 4.4.1 Someone other than the data subject who may receive the personal information

### **4.5 Third party**

- 4.5.1 Someone other than the subject of the personal information

### **4.6 Data Protection legislation**

- 4.6.1 Legislation, including but not limited to, the GDPR and UK Data Protection law

## **5. Responsibilities**

### **5.1 Data Protection Officer**

- 5.1.1 Responsibility for compliance with Data Protection legislation falls under the remit of the Data Protection Officer. This role is undertaken by the Head of Information Governance (IG).

## **5.2 Corporate Services Manager**

5.2.1 Corporate Services Manager is responsible for the processing and management of requests by individuals to invoke their rights under Data Protection legislation.

## **5.3 All NIAS staff**

5.3.1 All NIAS staff whether clinical or administrative, who come into contact with personal information or receive a request from an individual to invoke their rights, have a responsibility to ensure this is processed in accordance with Data Protection legislation and this procedure.

## **5.4 Duties relating to confidentiality and the protection of personal data**

5.4.1 All HSC bodies have a common law duty of confidence to patients and staff alike. Everyone working for NIAS who records, handles, stores or otherwise comes across patient or personal information has a duty to maintain this confidentiality.

## **6. Rights under Data Protection legislation**

6.1 Data Protection legislation provides the following eight rights to individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

6.2 Therefore, NIAS will:

Ensure the rights of the individuals, who are the subjects of the data held, are respected and can be fully exercised as detailed in Data Protection legislation.

## **7. Procedural guidance on respecting individuals' rights**

The table attached at Appendix 1 provides an overview of how requests can be made, any fees chargeable and time limits to respond. Identification can be requested for rights 2 – 8 if there is any identity about the individual's legality to make the request.

All requests made under the following rights, and actions taken must be recorded in the Data Protection Rights log.

Whatever action is taken in response to a request, the individual must receive an explanation and also be advised of their right to complain to the Information Commissioner's Office (ICO) or that they may seek to enforce their right through a judicial remedy.

### **7.1 The right to be informed**

Individuals have the right to be informed about the collection and use of their personal data. Individuals must be provided with 'privacy information', ideally at the time the information is collected. However, due to the nature of emergency work undertaken by NIAS, it is not feasible to provide information in the form of a leaflet. Therefore, comprehensive information will be provided on the NIAS website with reference to the website made via other suitable means. The information provided must be concise, transparent, intelligible and easily accessible. Child friendly versions of privacy information must be made available.

The following information must be provided:

- The name and contact details of NIAS
- The contact details of the Data Protection Officer
- The purposes for processing personal data
- The legal basis for the processing
- Recipients of the personal data
- Details of any overseas transfers

- Retention periods for personal data
- Reference to the rights of individuals
- How to withdraw consent to processing (if this was the legal basis for processing)
- How to lodge a complaint

Information will be provided via the NIAS website using a layered approach i.e. an overarching notice supported by links to other relevant / appropriate information.

A printable leaflet will be available to individuals making a request for a privacy notice who do not have access to the website.

The IG Compliance Manager will regularly review the privacy notices to ensure the content remains current and appropriate.

## **7.2 The right of access**

Individuals have the right of access to their personal data. This allows individuals to be aware of the lawfulness of the processing.

They will have the right to obtain:

- confirmation that their data is being processed
- access to their personal data
- other supplementary information (links to 7.1 – ‘right to be informed’)

### **7.2.1 Process:**

- When an individual submits a request for their personal data, the individual handling the request must satisfy themselves as to the identity of the requester. If there is any reasonable doubt over the identity of the requester, additional information can be requested.
- If clarification or additional detail is required to assist in identifying the information being requested, the individual must be contacted as soon as possible. The ‘clock’ will

then start from the date of receipt of the clarification / additional detail.

- The request must be responded to within one month of receipt. If the request is complex or numerous, this deadline can be extended for another two months. The requester must be informed of the decision to extend and the reasons why within a month of receipt of the request or any additional information / clarification requested in order to process the request.
- If the request is considered to be manifestly unfounded or excessive, a reasonable charge can be made.
- Where a decision is made to either charge for a manifestly unfounded or excessive request or to refuse it, this must be noted in the log.
- If the request is submitted electronically, the response should also be provided in a commonly used electronic format.

**Please note:** anyone can receive a request for information under this right e.g. a paramedic could receive a verbal request from the person they are treating. The details of the request, along with ID verification if applicable, must be passed to the IG Compliance Manager.

The process relating to 'clarification' and 'extension of deadline to respond' noted in this section applies to other rights where these are allowed.

### **7.3 The right to rectification**

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. Data can be inaccurate if it is 'incorrect or misleading'.

If the data refers to a mistake that has subsequently been rectified, it could be possible to argue that the record of the mistake is, in itself accurate and should be kept. This would be particularly pertinent in the case of a medical record

where an initial diagnosis, made in good faith, later proves to be incorrect.

If the individual's personal data has been disclosed to a third party, they must be informed of the rectification wherever possible. In addition, the individual must be informed about the third parties to whom their personal data has been disclosed.

### 7.3.1 Process:

- When an individual submits a request for rectification the reason for the request must be provided. A correction can only be made if there is clear evidence to support the request. If there is any doubt about the identity of the person making the request, more information can be requested from them.
- Wherever possible, a note should be included within a file clearly stating what correction has been made and for what reason. The supporting evidence should also be retained. A senior manager will be required to sign the correction.
- Amendments made to electronic records should be clearly annotated with who has made the amendment and why.
- A patient report form (PRF) is a medical record, the contents of which cannot be deleted. The original paper PRF cannot be amended as they are scanned into an electronic system and then destroyed by shredding. If rectification is appropriate, a copy of the original PRF must be made showing exactly the same details. Details of the correction must be noted in the free text notes section and then signed by a senior manager. The Caldicott Guardian will be required to sign the bottom of the PRF. The top copy must be passed to Clinical Audit for scanning and the second copy passed to the receiving location (if transported) for inclusion within their record.
- Electronic PRFs cannot be amended once finalised. If a correction is required, details of the amendment can be

appended to the original record. The record will clearly show who has made the amendment and for what reason.

- If the request is considered to be manifestly unfounded or excessive, a reasonable fee can be made for the administrative costs or the request can be refused. Justification for the decision will need to be communicated to the requester. The request will not have to be complied with until the fee has been received.
- If the request is complex or you have received a number of requests from the same individual, the time to respond can be extended by two months.

## **7.4 The right to erasure**

Individuals have the right to have personal data erased (or forgotten). However, this is not an absolute right and will only apply in certain circumstances.

An individual has the right to have their personal data erased if:

- it is no longer necessary for the purpose you originally collected it for
- consent has been relied upon and the consent is withdrawn
- there is no longer a legitimate interest to continue its processing
- the data has been processed unlawfully
- there is a legal obligation to comply

If the personal data has been disclosed to others, each recipient must be contacted to inform them of the erasure unless this is impossible or involves disproportionate effort.

The right to erasure does not apply for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation

- for the performance of a task carried out in the public interest
- for archiving purposes in the public interest or scientific or historical research
- for the establishment, exercise or defence of legal claims
- if the processing is necessary for public health purposes
- if the processing is for health-related purposes

#### 7.4.1 Process:

- Each request for erasure will be considered on a case by case basis with consideration being given to whether the right of erasure applies to the request.

### 7.5 The right to restriction of processing

Individuals have the right to request the restriction or suppression of their personal data where they have a particular reason for doing so. This can be seen as an alternative to the right of erasure. This is not an absolute right and only applies in certain circumstances. When processing is restricted, it is permissible to store the data but not use it.

An individual has the right to request the restriction of processing of their personal data in the following circumstances:

- The accuracy of the data is being contested
- The data has been unlawfully processed
- The data is no longer needed, however, the individual needs to keep it in order to establish, exercise or defend a legal claim
- The individual has objected to the processing and a decision is being made as to whether legitimate interests override those of the individual

It is important to note that if an individual has challenged the accuracy of their data and asked for it to be rectified or if they have objected to the processing, they also have the right to request restriction while the matters are being investigated.



‘Processing’ includes a broad range of operations including collection, structuring, dissemination and erasure of data.

Restricting data can be done by temporarily moving it to another processing system or making it unavailable to users.

#### 7.5.1 Process:

- Each request for the restriction of processing will be considered on a case by case basis with consideration being given to whether the right of restriction is valid.
- If the restriction has been applied to the data while another action is being investigated e.g. accuracy, a decision must be taken as to whether the restriction is lifted on conclusion of the investigation

### 7.6 The right to data portability

This right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows for them to move, copy or transfer their data easily from one IT environment to another in a safe and secure way without hindrance.

This right only applies to personal data an individual has provided to an organisation, where it is based on consent or as part of a contract or where processing is carried out by automated means (no manual intervention).

#### 7.6.1 Process:

- The personal data must be provided in a structured, commonly used and machine-readable format e.g. CSV files.
- The information can be transmitted directly to another organisation if this is technically feasible if this is at the request of the individual.

## 7.7 The right to object

Individuals have the right to object to their personal data being processed for the following reasons:

- The processing is based on the legitimate interests or the performance of a task in the public interest (including profiling)
- Direct marketing
- The processing is for the purpose of scientific/historical research and statistics

It is highly unlikely that NIAS will receive objection request for the latter 2 points above.

### 7.7.1 Process:

- Each request to object will be considered on a case by case basis as the objection must be relative to their own particular situation.
- Arrange for the processing to stop unless it can be demonstrated that the legitimate grounds for processing outweigh the interests of the individual or if the processing is for the establishment, exercise or defence of legal claims

## 7.8 Rights in relation to automated decision making and profiling

The right to object to automated decision making does not relate to NIAS at the present time. The definition of 'automated individual decision-making' is '*making a decision solely by automated means without any human intervention.*'

## 8. Consultation

- 8.1 This procedure will be presented to the IG Group for consultation. The group has delegated authority to approve this document.

## **9. Monitoring compliance and effectiveness of the policy**

- 9.1 This procedure will be reviewed annually by the Head of IG and approved by the IG Group, which reports in to the Finance and Performance Committee, a committee of the NIAS Board.
- 9.2 This procedure will meet the requirements of the Data Security and Protection Toolkit, which is a component of the Care Quality Commission Key Lines of Enquiry.
- 9.3 National guidance issued by the ICO will be monitored and included within this procedure should it be deemed relevant.

<b>Right</b>	<b>Method of request</b>	<b>Time limit</b>	<b>Fee chargeable</b>	<b>Circumstances when time limit can be extended by two months</b>	<b>Circumstances when fee allowable</b>
Right to be informed	Privacy notices should be made available as a matter of course	One month	No	None	None
Right of access	Verbal or writing	One month	No	Complex or numerous	Manifestly unfounded or excessive
Right to rectification	Verbal or writing	One month	No	Complex or numerous	Manifestly unfounded or excessive
Right to erasure	Verbal or writing	One month	No	Complex or numerous	Manifestly unfounded or excessive
Right to restrict processing	Verbal or writing	One month	No	Complex or numerous	Manifestly unfounded or excessive
Right to data portability	Verbal or writing	One month	No	Complex or numerous	None
Right to object	Verbal or writing	One month	No	None	None
Rights in relation to automated decision making and profiling	Not applicable to NIAS	Not applicable to NIAS	Not applicable to NIAS	Not applicable to NIAS	Not applicable to NIAS

Please note: individuals must be advised of an extension to deadline within one month. Additional information / clarification must be requested as soon as possible after receipt of request.

## Plan for Dissemination of Procedural Document

Title of document:	Data Protection Rights Procedure		
Version Number:	1.0	Dissemination lead: Print name, title and contact details	Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@nias.hscni.net
Previous document already being used?	No		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	All staff	
	Awareness for Reference Purposes	All staff	
	Awarenessto inform staff / other stakeholders	All staff	
Who does the document need to be disseminated to?	All staff have a responsibility to ensure that requests for individuals to express their rights under the GDPR are managed appropriately.		
Proposed methods of dissemination:  Including who will disseminate and when  Some examples of methods of disseminating information on procedural documents include:  <ul style="list-style-type: none"><li>Information cascade by managers</li><li>Communication via Management/</li></ul>		<ul style="list-style-type: none"><li>Information cascade by managers</li><li>Notification via articles in bulletins</li><li>Posting on the intranet</li></ul>	

<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Data Protection Rights Procedure provides staff with the detail and guidance required on how to manage and process requests from individuals to exercise their rights under the GDPR.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*







## DATA QUALITY POLICY

### Links

The following documents are closely associated with this policy:

- Clinical Records Keeping Procedure
- Information Lifecycle Management Policy
- Data Protection Policy
- Data Protection Rights Procedure
- Data Protection legislation (see 'definitions' section 4)
- Information Risk Management Policy
- Quality Impact Assessment Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New Policy and Procedure for NIAS

## Contents

1.	Introduction.....	4
2.	Objectives.....	4
3.	Scope.....	4
4.	Definitions.....	5
4.1	Data Protection legislation.....	5
4.2	Data.....	5
4.3	Information.....	5
5	Responsibilities.....	5
5.1	Senior Information Risk Owner (SIRO) .....	5
5.2	Medical Director (Caldicott Guardian) .....	5
5.3	Executive Directors .....	5
5.4	Information Governance Group .....	6
5.5	Informatics Assurance Group .....	6
5.6	Data Quality and Compliance Group.....	6
5.7	Head of Information Governance .....	6
5.8	Data Protection Officer .....	6
5.9	Information Asset Owners (IAO) .....	6
5.10	Information Asset Administrators (IAA) .....	7
5.11	All NIAS staff.....	7
6	General Policy .....	7
7	Information Governance and Quality Assurance .....	8
8	Data Quality and Validation Framework.....	9
9	Consultation.....	9
10	Monitoring Compliance and Effectiveness of the Policy .....	9
	Appendix 1 .....	10
	Plan for Dissemination of Procedural Document.....	10
	Data Quality and Validation Framework.....	12

## **1. Introduction**

- 1.1 Northern Ireland Ambulance Service HSC Trust (NIAS) understands that data quality is crucial to the safe and effective delivery of services. The availability of complete, accurate and timely data is important in supporting care delivery, clinical governance, management of information, clinical audit and achieving service targets.
- 1.2 Data and information collected by NIAS has many uses including, patient care, commissioning, planning and auditing. Therefore, data quality must be of a high standard to ensure NIAS can function effectively. In addition, approved information sharing will be used to support identified purposes, as inaccuracies in the information could impact on other HSC Organisations.
- 1.3 The effective use of performance information depends on data that is robust and accurate. Sufficient high quality information must be available to allow confidence that performance can be monitored, with remedial action taken when necessary.

## **2. Objectives**

- 2.1 The key objectives of the policy are:
  - NIAS will demonstrate its commitment to data quality and ensure that all data is captured accurately and in a timely manner
  - To ensure that all staff are aware of and understand the standards expected by NIAS with regard to data quality and its wider implications
  - To embed the principle that data quality is fundamental in the delivery of patient care and to support effective strategic planning
  - To define responsibilities relating to data management and quality and to clarify the legal requirements

## **3. Scope**

- 3.1 The scope of this policy covers information contained on all information systems within NIAS. Reference should also be made to

the 'Clinical Records Keeping Policy and Procedure' for specific guidance on completing paper patient report forms.

- 3.2 This policy applies to all NIAS employees, including permanent, temporary, voluntary and contract staff who process data and information.

## **4. Definitions**

### **4.1 Data Protection legislation**

Legislation including, but not limited to, the UK General Data Protection Regulation 2021 and Data Protection Act 2018 which legislates for the processing of and access to the personal information of living individuals

### **4.2 Data**

Facts and statistics collected for reference or analysis.

### **4.3 Information**

Data that has been analysed, processed and organised, providing knowledge.

## **5 Responsibilities**

### **5.1 Senior Information Risk Owner (SIRO)**

The Senior Information Risk Owner (SIRO) has overall responsibility for data quality assurance within the Trust. The SIRO is within the remit of the Director of Strategy and Transformation

### **5.2 Medical Director (Caldicott Guardian)**

The Medical Director is responsible for clinical data quality assurance within the Trust.

### **5.3 Executive Directors**

The Executive Directors are responsible for ensuring that all areas they oversee have data quality as an overarching principle embedded within them.

#### **5.4 Information Governance Group**

The IG group is responsible for providing assurance regarding data quality through the receipt of records of business from the Data Quality and Compliance Group.

#### **5.5 Informatics Assurance Group**

The Informatics Assurance Group is responsible for monitoring the activities of the IG Group.

#### **5.6 Data Quality and Compliance Group**

The Data Quality and Compliance group receives updates on data quality issues and changes to systems or processes that may impact on data quality in accordance with the group's terms of reference.

#### **5.7 Head of Information Governance**

The Head of IG will monitor the information asset audits and provide reports to the IG group.

#### **5.8 Data Protection Officer**

The Data Protection Officer will ensure NIAS can demonstrate its compliance with Data Protection legislation

#### **5.9 Information Asset Owners (IAO)**

The Information Asset Owners (IAO) will have responsibility for ensuring data quality is managed within the information system they have responsibility for. They are also responsible for reporting the levels of data quality compliance against agreed measures and ensuring all new staff using 'their' system are trained prior to being given access.

## **5.10 Information Asset Administrators (IAA)**

The Information Asset Administrators (IAA) will support the IAOs.

## **5.11 All NIAS staff**

All NIAS staff have a responsibility to ensure that data they record is accurate and timely.

# **6 General Policy**

6.1 The following are widely recognised attributes of good data quality

- Valid
- Complete
- Accurate
- Timely
- Clear/Concise
- Appropriate
- Relevant

6.2 IAOs are responsible for ensuring that documented data quality checks of frameworks are in place for 'their' information system.

6.3 Validation processes will (where appropriate) report on:

- Missing data
- Incomplete fields
- Number of records validated
- Verification process e.g. parameters
- Number of errors

6.4 It is the responsibility of all staff using NIAS information systems to ensure that data is recorded promptly and accurately in accordance with the operating policies and procedures for those systems and the 'principles of good data quality'.

6.5 It is the responsibility of the IAOs, with support from the IAAs, to ensure that all new users of the information system are trained prior to being allowed access.

- 6.6 Staff will take due care and attention to ensure that the data they enter into information systems supports the attributes of good data quality.
- 6.7 Staff using data for secondary purposes will ensure that data accessed is transferred accurately
- 6.8 All patient level data will be entered in real time where possible and where this is not possible as soon as reasonably practicable.
- 6.9 Staff will be held accountable by the relevant IAO for their performance in relation to data quality
- 6.10 Certain items of data will be identified as high priority by NIAS as they feed the NIAS Integrated Board Report (IBR). It is the responsibility of the relevant IAO to ensure the accuracy of this data prior to its publication in the IBR.
- 6.11 IAOs will take part in quality assurance audits as detailed in the validation framework template (Appendix 2)
- 6.12 IAOs will undertake regular validation audits on their asset to ensure the information remains current.

## **7 Information Governance and Quality Assurance**

IG provides a consistent way of processing information. The information quality assurance initiative of IG will establish and maintain good data quality standards through best practice guidelines and clear policies and procedures. Under this initiative:

- 7.1 All staff will be expected to abide by this policy
- 7.2 Regular audits will be undertaken around data quality using the IAO audit questionnaire
- 7.3 IAOs are expected to take ownership of, and seek to improve the data quality within 'their' information system where necessary
- 7.4 Wherever possible, data quality should be assured at the time of collection



7.5 Data standards and minimum data sets will be set and align with national standards where applicable

7.6 NIAS will promote data quality assurance through policies, procedures, user manuals and training

## **8 Data Quality and Validation Framework**

8.1 The processes providing assurances around data quality and validation have been included in the NIAS 'Data Quality and Validation Framework' template which can be found at Appendix 2

## **9 Consultation**

9.1 This policy will be presented to the IG Group for consultation. The group has delegated authority to approve this document.

## **10 Monitoring Compliance and Effectiveness of the Policy**

10.1 IAOs will be required to contribute to information asset audits, by means of face to face interviews or questionnaires. The Head of IG will compile a report for the IG Group. This will provide assurance that data quality checks are being undertaken.

## Appendix 1

### Plan for Dissemination of Procedural Document

Plan for Dissemination of Procedural Document			
Title of document:	Data Quality Policy		
Version Number:	V1.0	Dissemination lead: Print name, title and contact details	Tracy Avery, Head of Information Governance and Data Protection Officer Tracy.Avery@nias.hscni.net
Previous document already being used?	No		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	All staff	
	Awareness for Reference Purposes	All staff	
	Awareness to inform staff / other stakeholders	All staff	
Who does the document need to be disseminated to?	All staff need to be aware of the importance that data must be of the highest quality to support the business		

<p><b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b></p> <p>Some examples of methods of disseminating information on procedural documents include:</p> <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Articles in bulletins</li> <li>• Posting on the Intranet</li> </ul>
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p><b>It is important for staff to be aware of the need to process data of the highest quality to support the business</b></p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## Data Quality and Validation Framework

This framework is designed to assess the quality of data sets and/or information systems and to identify areas for improvement. The answers to the questions are either yes or no; if the answer to one of the questions below is 'no' then actions to improve data quality should be identified and implemented. If the answer to any of the questions is 'don't know' then this information should be found out. Please make any additional comments and / or detail evidence in the space provided.

<b>Name of information system:</b>	
<b>Name and Job title:</b>	
<b>Signed:</b>	
<b>Date:</b>	

<b>Systems and processes</b>	<b>Yes</b>	<b>No</b>
1. Are you clear about why the information is being collected?		
i. Is the information collected to meet statutory requirements?		
ii. If not, is the information used to meet clearly identified needs?		
<i>Evidence / comments:</i>		
2. Is there clear and up to date guidance for employees on how to use the information system, including which data to use for reporting purposes?		

<i>Evidence / comments:</i>		
3. Is the data validated for completeness, robustness and accuracy? <i>i.e. 'sense checking'</i>		
<i>Evidence / comments:</i>		
4. Are regular audits on validation undertaken? If yes, please state how often		
<i>Evidence / comments:</i>		
5. Does the information system have adequate controls to minimise;		
i. human error?		
ii. Prevent erroneous data entry?		
iii. Unauthorised data entry or manipulation?		
<i>Evidence / comments:</i>		
6. Do you have adequate arrangements in place for the security of the data?		
<i>Evidence / comments:</i>		

Data Quality Policy		Page:	13 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

7. If applicable, has action been taken to address the results of any previous internal or external reviews of data quality? e.g. internal audit		
<i>Evidence / comments:</i>		
<b>People and skills</b>	<b>Yes</b>	<b>No</b>
8. Is it clear who is responsible for updating the information system?		
<i>Evidence / comments:</i>		
9. Is it clear who is responsible for authorising;		
i. changes to the information system?		
ii. Communicating changes in the information system?		
<i>Evidence / comments:</i>		
10. Is relevant training provided for you and/or employees using the information system?		
<i>Evidence / comments:</i>		

Data Quality Policy		Page:	14 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

11. Do you and/or appropriate employees understand the importance of processing quality data and the consequences of poor data?		
<i>Evidence / comments:</i>		
12. Is consistency ensured in recording data when several people are involved in this task?		
<i>Evidence / comments:</i>		
<b>Data use and reporting</b>	<b>Yes</b>	<b>No</b>
13. Is the data captured and reported in a timely manner?		
<i>Evidence / comments:</i>		
14. Is the information presented in a clear/concise and relevant format?		
<i>Evidence / comments:</i>		
15. Is the data subject to appropriate levels of verification and information asset owner approval?		

Data Quality Policy		Page:	15 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

*Evidence / comments:*

Actions identified to address issues raised from using the checklist	Date for completion
<p>1. Are you clear about why the information is being collected?</p> <p style="padding-left: 40px;">i. Is the information collected to meet statutory requirements?</p> <p style="padding-left: 40px;">ii. If not, is the information used to meet clearly identified needs?</p> <p><i>Actions:</i></p> <p style="padding-left: 40px;">i.</p> <p style="padding-left: 40px;">ii.</p>	
<p>2. Is there clear and up to date guidance for employees on how to use the information system, including which data to use for reporting purposes?</p> <p><i>Actions:</i></p>	
<p>3. Is the data validated for completeness, robustness and accuracy? <i>i.e. 'sense checking'</i></p> <p><i>Actions:</i></p>	

Data Quality Policy		Page:	16 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	



Actions identified to address issues raised from using the checklist	Date for completion
<p>4. Are regular audits on validation undertaken? If yes, please state how often</p> <p><i>Actions:</i></p>	
<p>5. Does the data system have adequate controls to minimise;</p> <p>i. Human error? ii. Prevent erroneous data entry? iii. Unauthorised data entry or manipulation?</p> <p><i>Actions:</i></p> <p>i.</p> <p>ii.</p> <p>iii.</p>	
<p>6. Do you have adequate arrangements in place for the security of data?</p> <p><i>Actions:</i></p>	
<p>7. If applicable, has action been taken to address the results of any previous internal or external reviews of data quality? e.g. internal audit</p> <p><i>Actions:</i></p>	

Data Quality Policy		Page:	17 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

Actions identified to address issues raised from using the checklist	Date for completion
<p>8. Is it clear who is responsible for updating the information system?</p> <p><i>Actions:</i></p>	
<p>9. Is it clear who is responsible for authorising:</p> <ul style="list-style-type: none"> <li>i. changes to the information system</li> <li>ii. communicating changes in the information system</li> </ul> <p><i>Actions:</i></p> <ul style="list-style-type: none"> <li>i.</li> <li>ii.</li> </ul>	
<p>10. Is relevant training provided for you and/or employees using the information system?</p> <p><i>Actions:</i></p>	
<p>11. Do you and/or appropriate employees understand the importance of processing quality data and the consequences of poor data?</p>	

Data Quality Policy		Page:	18 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

Actions identified to address issues raised from using the checklist		Date for completion
<i>Actions:</i>		
12. Is consistency ensured in recording data when several people are involved in this task?  <i>Actions:</i>		
13. Is the data captured and reported in a timely manner?  <i>Actions:</i>		
14. Is the information presented in a clear/concise and relevant format?  <i>Actions:</i>		
15. Is the data subject to appropriate levels of verification and information asset owner approval?  <i>Actions:</i>		

Data Quality Policy		Page:	19 of 20
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	



## FREEDOM OF INFORMATION POLICY AND PROCEDURE (INCLUDING ENVIRONMENTAL INFORMATION REGULATIONS)

### Links

- Freedom of Information Act 2000
- Data Protection legislation
- Environmental Information Regulations 2004
- Information Lifecycle Management Policy
- Retention and Disposal of Information Schedule
- Employees Guide to Confidentiality and Security
- Department of Constitutional Affairs Codes of Practice
- Data Protection Policy
- Data Protection Rights Policy and Procedure Information Governance Review 2013 (aka Caldicott2)
- Safe Haven Policy
- Data Protection Impact Assessment Policy and Procedure

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Informatics and Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				Rewritten in Corporate Template

## Contents

1.	Introduction .....	4
2.	Objectives .....	4
3.	Scope.....	5
4.	Definitions .....	5
5.	Responsibilities .....	6
6.	Legal Obligations – Freedom of Information Act 2000.....	6
7.	Legal Obligations – Freedom of Information Act 2000 and Environmental Information Regulations 2004.....	7
8.	Classes of Information .....	8
9.	Charges and Fees .....	8
10.	Identifying which Act to apply .....	10
11.	Conditions for non-disclosure.....	11
12.	Qualified Exemptions/Exceptions (FOIA & EIR) .....	12
13.	Absolute Exemptions (FOIA only).....	12
14.	Refusal of Requests and Right to Appeal .....	14
15.	Advice and Assistance.....	14
16.	Personal Information.....	15
17.	Consultation with Third Parties.....	15
18.	Public Sector Contracts .....	16
19.	Records Management.....	16
20.	Additional Assurances .....	16
21.	Consultation.....	17
22.	Monitoring Compliance and Effectiveness of the Policy .....	17
	Appendices.....	19

Freedom of Information Policy and Procedure		Page:	3 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

## 1. Introduction

- 1.1 The Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR) are part of the Government's commitment to greater openness in the public sector. This commitment is shared by Northern Ireland Service HSC Trust (NIAS).
- 1.2 Both Acts came into full effect on 1<sup>st</sup> January 2005 and legislate for a general right of access (subject to exemptions/exceptions) to recorded information held by public authorities. By establishing these legal rights of members of the public, it will enable them to question the decisions of public authorities more closely and ensure that the services we provide is delivered efficiently and effectively.
- 1.3 All non-personal information may be accessible under the Acts, including both electronic and paper versions. The Acts are retrospective and include information held prior to 1<sup>st</sup> January 2005.
- 1.4 The Acts clearly explain and define the interface between the Acts and Data Protection legislation. This policy does not overturn the common law of confidence or statutory provisions (including the Human Rights Act 1998 and Data Protection that prevent disclosure of personal identifiable information. The right to release personal information is covered by the right of access under Data Protection legislation.
- 1.5 The procedure to follow when handling requests for information can be found in **Appendix 1**.

## 2. Objectives

- 2.1 The key objectives of this policy, and the associated procedure, are:

Freedom of Information Policy and Procedure		Page:	4 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021



- To ensure that non-personal information is processed in accordance with the requirements of the FOIA and EIR
- To provide guidance on the correct way to handle requests for non-personal information

### 3. Scope

- 3.1 This policy and procedure applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who come into contact with non-personal information.
- 3.2 All employees allocated responsibility for responding to Freedom of Information (FOI) and EIR requests will be aware of the legal obligations NIAS is under.

### 4. Definitions

- 4.1 **Applicant:** The individual, group or organisation making the request for information
- 4.2 **Exemption:** A valid reason for non-disclosure of information under the FOIA
- 4.3 **Exception:** A valid reason for non-disclosure of information under the EIR
- 4.4 **Publication Scheme:** A publication detailing all the information routinely available from the organisation.
- 4.5 **Public Interest Test:** Determining whether the interests of the public are better served by withholding or disclosing the information
- 4.6 **Personal Information:** Information from which an individual's identity can be obtained
- 4.7 **Third Party:** Someone other than the applicant

Freedom of Information Policy and Procedure		Page:	5 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

- 4.8 **Data Protection legislation:** Legislation including, but not limited to, the General Data Protection Regulation and UK Data Protection law.

## 5. Responsibilities

- 5.1 The Chief Executive Officer is the NIAS Accounting Officer and has overall accountability and responsibility for IG
- 5.2 Advice may be sought from **Directors** in cases where it is not clear whether information can be disclosed
- 5.3 **Senior Managers** may be required to undertake an internal review following an appeal made by the applicant
- 5.4 The **Head of Information Governance and Data Protection Officer** will provide assurance to the IG Group on compliance with statutory obligations.
- 5.5 The mandatory role **Data Protection Officer (DPO)** will ensure NIAS can demonstrate its compliance with Data Protection legislation
- 5.6 The **Information Governance Coordinator** will manage requests for information and provide assurance to the Head of IG and DPO on compliance with statutory obligations through key performance indicators.
- 5.7 **All staff** will have a responsibility to comply with legislation and guidance relating to the FOIA and support the IG Officer with providing information requested by applicants.

## 6. Legal Obligations – Freedom of Information Act 2000

Full implementation of the FOIA means that all public authorities are required to meet a number of legal obligations. The one specific to FOIA is:

*Maintain a Publication Scheme*

Freedom of Information Policy and Procedure		Page:	6 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

- 6.1 The FOIA requires each public authority to produce and maintain a Publication Scheme. This details all the information readily accessible from the organisation, along with additional information relating to any fees that may be charged and contact details. It is the policy of NIAS to publish as much information about NIAS as is reasonably practical so that members of the public do not have to submit a formal FOI request. The NIAS scheme is based on the model developed by the Information Commissioner's Office (ICO) and is available on the NIAS web site [www.NIAS.nhs.uk](http://www.NIAS.nhs.uk). The scheme will be reviewed on a regular basis. How to access information under the EIR is also included within the Publication Scheme.

## 7. Legal Obligations – Freedom of Information Act 2000 and Environmental Information Regulations 2004

### *To respond to requests for information*

- 7.1 **FOIA** – NIAS will publish as much information as possible on its Publication Scheme. Any requests for information not available via this media must be made in writing to the IG Officer. 'Writing' includes letters, fax and emails but excludes text messaging. All requests must be dealt with within 20 working days of receipt. However, if a fee is required or additional information required to locate the required information, the 20 days will be suspended and re-commence from receipt of this or these.

**EIR** – NIAS will publish as much information as possible on its Publication Scheme. Any requests for information not available via this media must be made to the IG Officer. Requests **do not** have to be made in writing. Wherever possible, requests must be dealt with within 20 working days of receipt. However, if the request is considered complex and voluminous, this can be extended to 40 working days. The applicant should be informed of this as soon as possible. If additional information is required to locate the required

Freedom of Information Policy and Procedure		Page:	7 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

information, the 20 days will be suspended and re-commence from receipt of this.

*To provide advice and assistance with regard to requests under the Acts*

7.2 Public authorities have a duty to provide advice and assistance to applicants, or would-be applicants, for information. The procedure for dealing with requests is published in the NIAS Publication Scheme. The Publication Scheme will provide comprehensive information to assist an individual with locating the information they require. The IG Officer is also available to provide advice.

7.3 NIAS is committed to meeting these obligations.

## **8. Classes of Information**

8.1 The information in the Publication Scheme is grouped into broad categories as follows:

1. Who we are and what we do
2. What we spend and how we spend it
3. What our priorities are and how we are doing
4. How we make decisions
5. Our policies and procedures
6. List and registers
7. The services we offer

8.2 Further details of what can be found within each class can be found in Part 2 of the Publication Scheme. Any additions to the scheme will be placed in the most appropriate class and the Publication Scheme contents amended accordingly.

## **9. Charges and Fees**

9.1 No charge will be made for information provided in the form of:

Freedom of Information Policy and Procedure		Page:	8 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

- downloads or information taken from the NIAS website, although any charges for Internet Service provider and personal printing costs would have to be met by the individual
- email – unless it is for information not routinely published in the public domain
- leaflets and brochures
- access to any public registers or lists of environmental information

## 9.2 Charges may be incurred for the following:

- information provided on CD Rom or similar medium
- multiple copies of documents
- archived copies of documents that are no longer available on the NIAS website
- any information held by NIAS that is not routinely published in the public domain

Freedom of Information Policy and Procedure		Page:	9 of 15
		Version:	14.0
Date of Approval:	23 July 2020	Status:	Final
Approved by:	Information Governance Group	Next Review Date:	September 2021

- 9.3 Charges will be advised in advance and payment will be required before the information is released. Standard charges will be published on the Publication Scheme.
- 9.4 Charges will be reviewed regularly and be in line with The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004. Please note these Regulations do not apply to the EIR.

## 10. Identifying which Act to apply

The EIR specifically covers information on the state of the environment, and can be summarised as follows:

- the state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites and the interaction between these elements
- factors such as substances, energy, noise, radiation or waste affecting or likely to affect the elements of the environment
- measures such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect or protect the elements of the environment
- reports on the implementation of environmental legislation
- cost-benefit and other economic analyses and assumptions used within the framework of environmental measures and activities
- the state of human health and safety, including the contamination of the food chain, conditions of human life, cultural sites and built structures in as much as they are or may be affected by the state of the elements of the environment.

All other requests for non-personal information should be handled under the FOIA.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)	Page:	10 of 28
	Version:	1.0
Date of Approval:	Status:	Draft
Approved by:	Next Review Date:	

## 11. Conditions for non-disclosure

There are certain conditions whereby NIAS are not obliged to comply with an information request.

- 11.1 The duty to comply does not arise if the estimated cost of supplying the information exceeds the appropriate limit established in statutory Fees Regulations (£450.00 for HSC Trusts). However, NIAS will work with the applicant to keep costs to a minimum but reserves the right to refuse or charge for the communication of information that exceeds the limit. This does not apply to the EIR.

Under the EIR, there is no cost limit. However, requests that cost a disproportionate amount can be refused on the basis they are 'manifestly unreasonable' (see Exceptions section 12.6)

- 11.2 NIAS does not have to comply with a request if it is considered vexatious. NIAS will log all requests for monitoring purposes and will be able to identify repeated or vexatious requests.
- 11.3 The duty to comply does not arise if a fees notice has been issued to an applicant and said fees are not paid within three months of the date of the notice.
- 11.4 NIAS will redact material which cannot be disclosed when it appears within the content of an otherwise disclosable document.
- 11.5 Both the FOIA and the EIR set out a series of exemptions (FOIA) and exceptions (EIR) which amount to valid reasons why information cannot be disclosed. The exemptions are separated into 'absolute' and 'qualified', whilst the exceptions are all 'qualified'.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	11 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	229	Next Review Date:	

## 12. Qualified Exemptions/Exceptions (FOIA & EIR)

These exemptions require the 'public interest test' to be applied to them. Information that falls within this particular category will have to be disclosed unless it can be successfully argued that the public interest in withholding it is greater than the public interest in releasing it.

## 13. Absolute Exemptions (FOIA only)

13.1 These exemptions do not contain the above requirement. Where information falls within the terms of an absolute exemption, NIAS may withhold this without applying the public interest test.

13.2 When information is withheld due to an exemption, the applicant must be informed of this.

13.3 The full list of exemptions is as follows:

### Qualified Exemptions (FOIA)

Section 22 Information intended for future publication  
Section 22a Research  
Section 24 National Security  
Section 26 Defence  
Section 27 International Relations  
Section 28 Relations within the United Kingdom  
Section 29 The economy  
Section 30 Investigations and proceedings conducted by public authorities  
Section 31 Law enforcement  
Section 33 Audit functions  
Section 35 Formulation of government policy etc.  
Section 36 Prejudice to effective conduct of public affairs  
Section 37 Communications with Her Majesty, etc. and honours  
Section 38 Health and safety

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	12 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	230	Next Review Date:	



Section 40 Some Personal information  
 Section 42 Legal professional privilege  
 Section 43 Commercial interests

### Absolute Exemptions (FOIA)

Section 21 Information accessible to applicant by other means  
 Section 23 Information supplied by, or relating to, bodies dealing with security matters  
 Section 32 Court records etc.  
 Section 34 Parliamentary privilege  
 Section 36 Prejudice to effective conduct of public affairs  
 Section 40 Personal Information  
 Section 41 Information provided in confidence  
 Section 44 Prohibitions on disclosure where a disclosure is prohibited by an enactment or would constitute a contempt of court.

Further details about these exemptions can be found in the relevant section of the Act as listed above.

### Exceptions (EIR)

Regulation 12(4) (a) Does not hold that information when an applicant's request is received  
 Regulation 12(4) (b) is manifestly unreasonable  
 Regulation 12(4) (c) Is formulated in too general a manner (providing assistance has been given to the applicant with a view to re-framing the request)  
 Regulation 12(4) (d) Relates to unfinished documents or incomplete data  
 Regulation 12(4) (e) Would involve disclosure of internal communications

And if disclosure would adversely affect:

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)	Page:	13 of 28
	Version:	1.0
Date of Approval:	Status:	Draft
Approved by:	Next Review Date:	

- Regulation 12(5) (a) International relations, defence, national security or public safety
- Regulation 12(5) (b) The course of justice, fair trial, conduct of a criminal or disciplinary inquiry
- Regulation 12(5) (c) Intellectual property rights
- Regulation 12(5) (d) Confidentiality of public authority proceedings when covered by law
- Regulation 12(5)(e) Confidentiality of commercial or industrial information, when protected by law to cover legitimate economic interest
- Regulation 12(5) (f) Interests of the person who provided the information
- Regulation 12(5) (g) Protection of the environment
- Regulation 13 Personal data

## 14. Refusal of Requests and Right to Appeal

If a request for information has been refused or the applicant is not satisfied with the information disclosed to them, they have the right to appeal. In the first instance, the applicant should write to the IG Officer. The applicant may request an internal review. Under EIR the applicant's request for an internal review must be made within 40 working days of the date of the refusal letter. The appeal must then be dealt with within 40 working days by NIAS. There are no such timelines dictated under the FOIA. However, good practice would be to follow the same timescales as under the EIR. If the applicant remains dissatisfied with the outcome, they may refer the matter to the ICO who will investigate the issue and advise accordingly. These steps are in line with guidance issued by the ICO. NIAS reserves the right to seek legal advice if deemed necessary.

## 15. Advice and Assistance

NIAS will endeavour to provide advice and assistance to anyone requesting information when it is unclear what is

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)	Page:	14 of 28
	Version:	1.0
Date of Approval:	Status:	Draft
Approved by:	Next Review Date:	

requested or if there is a cost implication. If clarification of the request is needed, this must be requested promptly and, in any event, no later than 20 working days. If the request exceeds the Fees Regulations (FOIA) or is too complex or large, NIAS should work with the applicant to try to explore ways in making the request more reasonable.

## **16. Personal Information**

16.1 Personal information contained within disclosures under the FOIA and EIR should be redacted if they relate to the private life of the individual detailed. This is in accordance with Data Protection legislation. However, personal details pertaining to an individual who is mentioned in their official capacity may be released. This is in accordance with the ICO Awareness Guidance (no.1).

16.2 Personal details should not be released if there is any evidence that damage or distress may be caused to the individual being named, or their safety may be compromised. However, this does not include withholding details to prevent potential embarrassment being caused because of the disclosure.

16.3 Staff should be informed that information and documents they may have contributed to in their professional capacity, may be disclosable.

## **17. Consultation with Third Parties**

17.1 Where information has been obtained from a third party in confidence, NIAS will make every effort to consult with the third party with a view to obtaining consent for disclosure. However, if a third party does not respond or they refuse to consent, this does not automatically mean information will be withheld. The final decision as to whether the information should be disclosed will lie with NIAS.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	15 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	233	Next Review Date:	

## 18. Public Sector Contracts

- 18.1 In deciding whether any information may be exempt from disclosure because it may involve a breach of confidentiality imposed by a third party or it may breach a trade secret, or it may prejudice the commercial interest of any party, NIAS will consider current guidance issued by the ICO or the Department of Constitutional Affairs. Contractors should be advised to include FOIA or EIR disclosure clauses within their contracts.

## 19. Records Management

- 19.1 NIAS follows an Information Lifecycle Management Policy and Retention and Disclosure of Information Schedule. These comply with the Lord Chancellor's Code of Practice on the Management of Records (under Section 46 of the Act) and the Records Management Code of Practice for health and Social Care 2016. These policies will address issues of active records management, including the creation, retention, maintenance and disposal of records, according to the legal requirements placed upon NIAS.

## 20. Additional Assurances

NIAS will make further assurances in order to support its commitment to the obligations of the Acts.

- An appropriately trained individual or individuals will have specific responsibility for FOIA and EIR within NIAS. The management and maintenance of the Publication Scheme, monitoring of compliance and the management of responses to the majority of requests are the responsibility of the IG Officer. A member of the Communications Team will be involved in the drafting of replies for FOI requests submitted by the media. The final agreed response will be sent by the IG Officer.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	16 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	234	Next Review Date:	

- Everyone handling information is appropriately trained to do so. All aspects of IG, including FOI, are covered in the induction and essential training programmes.
- Policies are in place regarding the management of information and the retention and disposal of records held, including any legal obligations.
- Everyone is aware of the need to manage their information in accordance with NIAS policies and HSC guidelines.
- Requests for information are handled promptly and in accordance with the timescales detailed in the FOIA and EIR.
- Everyone is aware of the procedure for handling requests for information.
- All staff have access to a copy of the 'Confidentiality and Security Handbook'.
- Applicants will be invited to provide feedback on how their request for information was handled.
- The IG Officer will liaise with other FOI colleagues when requests are identified as 'round robin' i.e. sent to several other HSC Trusts to ensure consistency in responses made.

## 21. Consultation

21.2 This policy will be presented to the IG Group for consultation. The Group has delegated authority to approve this document

## 22. Monitoring Compliance and Effectiveness of the Policy

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	17 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	235	Next Review Date:	

22.1 The Head of IG and DPO will monitor the implementation of this policy and procedure, and take an assurance report to the IG Group. This report will sent on an annual basis. In addition, monitoring reports will be presented to the IG Group periodically to advise of any compliance issues.

FOI requests and questions surrounding FOI issues can be emailed to [Informatics.Department@Nias.hscni.net](mailto:Informatics.Department@Nias.hscni.net)

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	18 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	236	Next Review Date:	

## Appendices

### Appendix 1

#### Procedure for Handling Requests for Information

This procedure follows the same path as the flowchart drawn up to illustrate the information flow in diagrammatical format. The flowchart is attached for reference at **Appendix 2**.

Although the official deadline for handling FOI and EIR requests is 20 working days, it is considered prudent to work to a deadline of 15 days. This is to ensure that the final checking process can be completed and any additional material/information gathered if necessary. The IG Officer will request progress reports on the 5<sup>th</sup> and 10<sup>th</sup> day.

A request for information is received.

1. The IG Officer will assess whether the request is valid (e.g. written for FOI) and under which legislation the request is to be responded to.
2. If the request is for personal information, this is passed to the Corporate Services Manager and dealt with as a right of access by the data subject request under Data Protection legislation.
3. The IG Office will enter FOI and EIR requests into the FOI Log
4. The IG Officer will assess whether any additional information is required to respond to the request. If further details or clarification are required, the applicant will be contacted as soon as possible.
5. The IG Officer will send an acknowledgement letter to the applicant.
6. The IG Officer will determine whether the non-personal information requested can be disclosed.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	19 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	237	Next Review Date:	

7. **Yes**, the information can be disclosed - the request is passed to the relevant individual to gather the information. Continue from step 11.

The responsibility for responding to the request remains with the IG Officer (unless step 10 applies). For more complex requests, the disclosures will be checked by the Corporate Services Manager or Head of IG and DPO prior to release.

8. **No**, the information cannot be released – if the information cannot be released at the present time, is it due to be released at a later date? If so, a letter must be sent to the applicant advising when the information will be available and to re-contact NIAS at that time.

If the information cannot be released now or at any time in the future, a letter must be sent to the applicant advising of this. They must be given an explanation as to why the request has been refused. If an exemption or exception has been relied upon, this must be stated. (See Exemptions/Exceptions section of Policy)

9. **Unsure** – If the IG Officer is unsure whether the information requested can be released, advice will be sought from the Corporate Services Manager or Head of IG and DPO in the first instance. If still unsure, advice will be sought from the relevant Director. The procedure will then be followed as described in the 'Director's flowchart' in Appendix 3.
10. A member of the Communications Team may be involved in drafting the response, where appropriate.

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	20 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	238	Next Review Date:	



11. The IG Officer will determine whether a fee is payable for the information based on a pre-determined scale of charges and set criteria (as stated in the Publication Scheme.)
12. If a fee is not required, the information can be released. This must be done within 20 working days of receipt of the request. A feedback form is available to applicants on the NIAS website which can be used to identify any areas of concern/good practice.
13. If a fee is required, the IG Officer will write to the applicant and the information released only on receipt of this payment. The deadline of 20 working days is suspended until the payment has been received.
14. If the fee is not received within 3 months, the request can be closed.
15. If the information being requested impacts on another HSC organisation, the IG Officer will forward a request to the FOI lead of that Trust suggesting a meeting to discuss possible implications. If this meeting is declined, a copy of the disclosure will be sent to the Trust at the same time as it is sent to the applicant.
16. If advice has been sought from a Director as to whether information can be released, and the Director is unsure, further advice can be taken from the Chief Executive. If a decision is reached at this stage, the procedure should continue from step 7 ('yes the information can be released') or step 8 ('the information cannot be released').
17. If further advice is required by the Chief Executive, this should be sought from the NIAS solicitors. A decision must be made at this stage as to whether the information requested can be

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	21 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	239	Next Review Date:	

released or not. If it can, continue the process from step 7, if not, continue from step 8.

It is important that the FOI spreadsheet is completed showing action taken and dates in order that requests can be monitored for compliance.

A set of standard response letters has been developed (following Ministry of Justice guidelines) which should be used to respond to applicants.

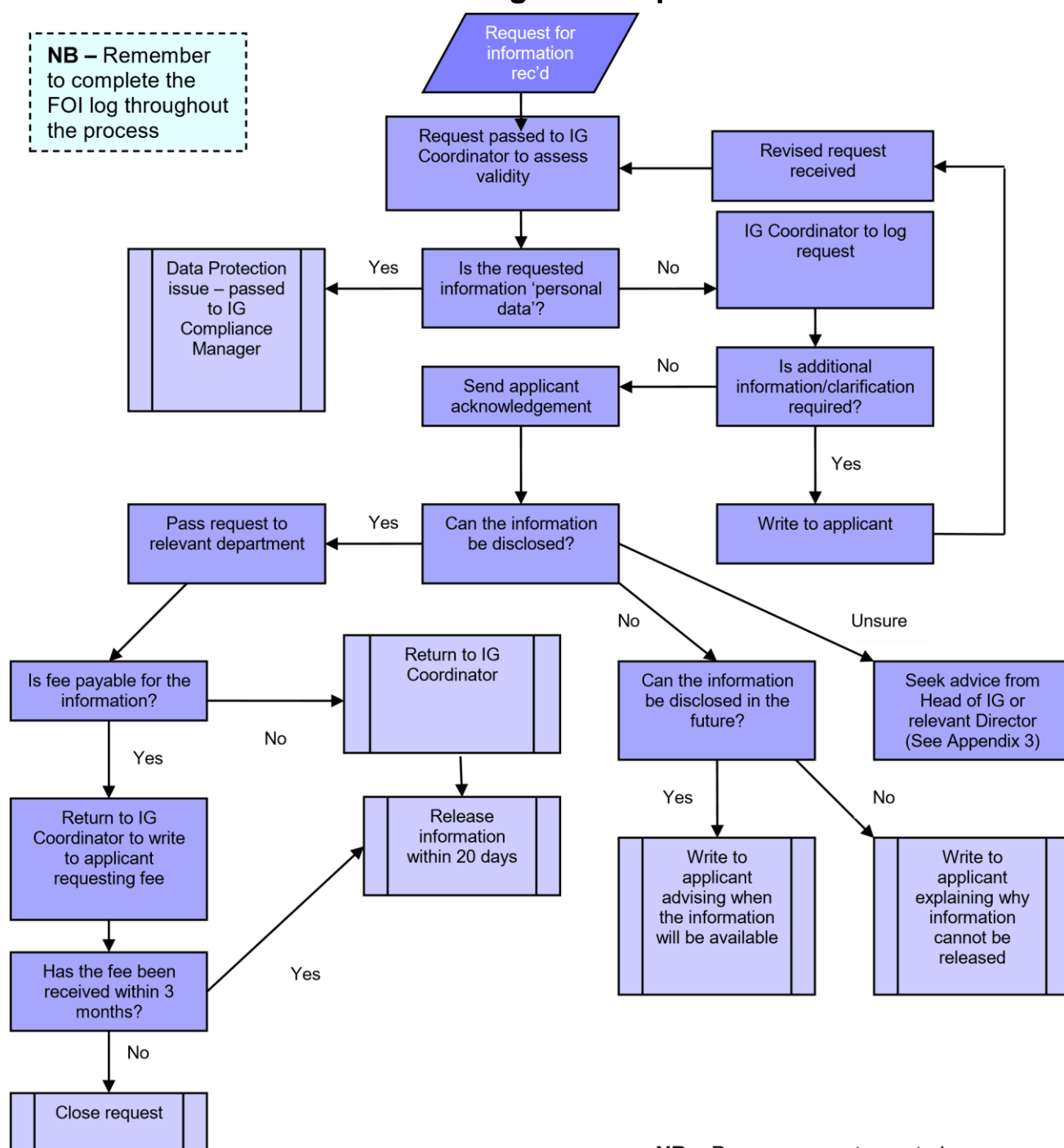
Further advice and assistance can be obtained from the Head of IG and DPO, Corporate Services Manager or IG Officer – [Informatics.Department@hscni.net](mailto:Informatics.Department@hscni.net)

## **Appendix 2**

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	22 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	240	Next Review Date:	

## Procedure for Dealing with Requests for Information

**NB** – Remember to complete the FOI log throughout the process



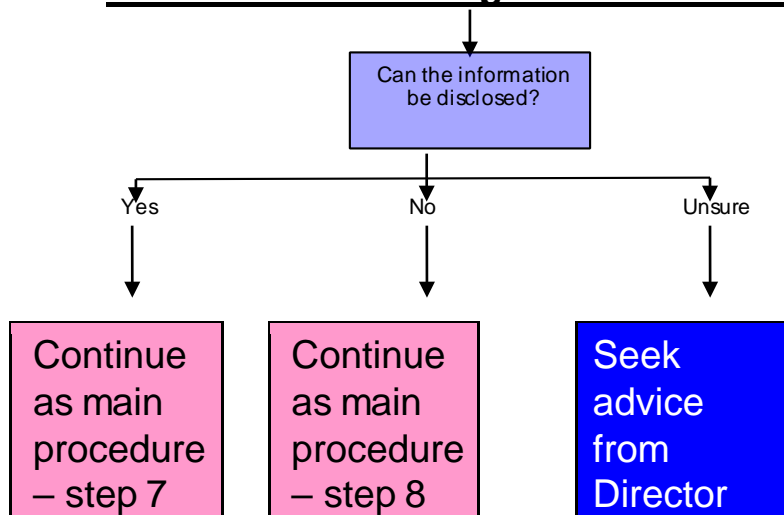
**NB** – Progress reports are to be requested on the 5<sup>th</sup> and 10<sup>th</sup> day

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	23 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	241	Next Review Date:	

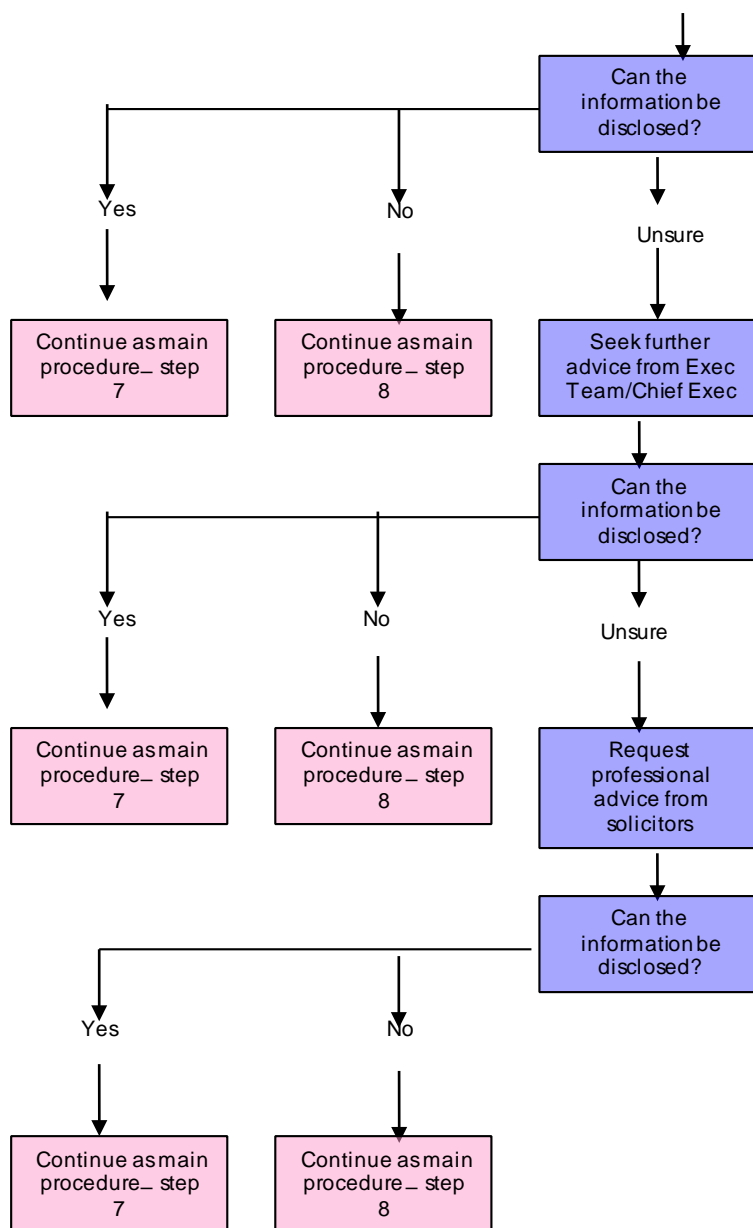
**NB** – If information release impacts on another HSC Trust, request meeting to discuss

### Appendix 3

#### Procedure for Dealing with more Complex Requests



Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	24 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	242	Next Review Date:	



Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	25 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

## Appendix 4

### Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Freedom of Information Policy and Procedure</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead: Print name, title and contact details</b>	<b>Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@NIAS.Hscni.net</b>
<b>Previous document already being used?</b>	<b>Yes</b>		
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	Staff have a responsibility to ensure that any requests for information are handled in accordance with the relevant legislation. Although requests under the Freedom of Information Act for non-personal information are managed centrally within the IM&T Team, all staff must be aware of the processes involved to ensure compliance is maintained.		

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	26 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

<p><b>Proposed methods of dissemination:</b></p> <p><b>Including who will disseminate and when</b></p> <p>Some examples of methods of disseminating information on procedural documents include:</p> <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Freedom of Information Policy and Procedure provides staff with the detail and guidance required on how a request for non-personal information is managed in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

Freedom of Information Policy and Procedure (Including Environmental Information Regulations)		Page:	27 of 28
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:	245	Next Review Date:	





## INFORMATION ASSET POLICY

### Links

The following documents are closely associated with this policy:

- Information Risk Management Policy
- Data Protection legislation (see 'definitions' section 4)
- Data Security and Protection Toolkit
- Data Protection Policy
- Data Protection Rights Procedure
- Data Quality Policy
- Information Disclosure and Transfer Policy
- Information Governance Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New Policy and Procedure for NIAS

## Contents

1. Introduction .....	<b>Error! Bookmark not defined.</b>
2. Objectives .....	<b>Error! Bookmark not defined.</b>
3. Scope.....	<b>Error! Bookmark not defined.</b>
4. Definitions .....	<b>Error! Bookmark not defined.</b>
4.1 Data Protection Legislation....	<b>Error! Bookmark not defined.</b>
5. Responsibilities .....	<b>Error! Bookmark not defined.</b>
5.1 Chief Executive Officer.....	<b>Error! Bookmark not defined.</b>
5.2 Senior Information Risk Owner (SIRO)....	<b>Error! Bookmark not defined.</b>
5.3 Caldicott Guardian .....	<b>Error! Bookmark not defined.</b>
5.4 Head of Information Governance .....	<b>Error! Bookmark not defined.</b>
5.5 Data Protection Officer (DPO).....	<b>Error! Bookmark not defined.</b>
6. Schedule.....	<b>Error! Bookmark not defined.</b>
7. Consultation .....	<b>Error! Bookmark not defined.</b>
8. References.....	<b>Error! Bookmark not defined.</b>
9. Monitoring Compliance and Effectiveness of the Policy ...	<b>Error! Bookmark not defined.</b>
Plan for Dissemination of Procedural Document	<b>Error! Bookmark not defined.</b>

## **1. Introduction**

- 1.1 Northern Ireland Ambulance Service HSC Trust (NIAS) is committed to meeting Information Governance requirements. A fundamental aspect is to ensure that Information Assets (IA) are managed appropriately to ensure the protection, confidentiality and integrity of information.
- 1.2 The purpose of this policy is to provide assurance to the Senior Information Risk Owner (SIRO) that appropriate frameworks are in place to support robust information security, information risk, business continuity and data quality.
- 1.3 This policy provides a mechanism by which NIAS IAs will be managed and protected. All major IAs must be identified and an Information Asset Owner (IAO) assigned to ensure the asset is managed and any information contained adequately protected.

## **2. Objectives**

- 2.1 To manage NIAS IAs
- 2.2 To protect NIAS, its patients, staff and stakeholders from inappropriate access and poor-quality information
- 2.3 To ensure that all new IAs are identified and logged in the Information Asset Register.
- 2.4 To provide assurance to the SIRO that IAs are being managed appropriately and that all necessary safeguards are in place to protect them.
- 2.5 To meet the requirements of the DSP Toolkit thereby supporting the Information Governance Assurance Statement.
- 2.6 To support the assurance provided through the Statement of Internal Controls, that all risks, including those relating to information, are effectively managed and mitigated.

## **3. Scope**

- 3.1 This policy covers all aspects of information within NIAS including:

- Patient information
  - Staff information
  - Organisational information
- 3.2 This policy covers IAs utilised by NIAS, and the information contained within.
- 3.3 This policy and procedure applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who may have a responsibility for an IA.

## 4. Definitions

- 4.1 **Senior Information Risk Owner (SIRO):** ensures that identified information security risks are identified and managed
- 4.2 **Information Asset (IA):** an identifiable and definable asset which is 'valuable' to the business.
- 4.3 **Information Asset Owner (IAO):** assigned owner of an information asset who reports to the SIRO
- 4.4 **Information Asset Administrator (IAA):** will provide support to the IAO
- 4.5 **Information Asset Register (IAR):** a register of all information assets
- 4.6 **Critical Information System:** a system that is critical to the core business of NIAS i.e. CAD and telephony
- 4.7 **Data Protection legislation:** legislation including, but not limited to, the General Data Protection Regulation (GDPR) and the Data Protection Act 2018

## 5. Responsibilities

- 5.1 The **Chief Executive Officer** is the NIAS Accounting Officer and has overall accountability and responsibility for Information Governance (IG).

- 5.2 The **Senior Information Risk Owner (SIRO)** will oversee information risk.
- 5.3 The **Head of Information Governance and Data Protection Officer** will manage the day to day IG agenda and provide assurance to the Board on compliance with the DSP Toolkit.
- 5.4 The mandatory role **Data Protection Officer (DPO)** will ensure NIAS can demonstrate compliance with Data Protection legislation
- 5.5 The **Information Security Manager** ensures NIAS complies with information security requirements and relevant legislation and guidance relating to the security of information.
- 5.6 **Information Asset Owners (IAO)** are directly accountable to the SIRO and will provide assurance that information risk is being managed for their assigned information assets through quarterly assessments.
- 5.7 **Information Asset Administrators (IAA)** will assist the IAOs and have day to day responsibility for the management of information risks for their assigned information asset.
- 5.8 **All staff** will have a responsibility to comply with legislation and guidance relating to IG and identify and report any risks or areas of concern.

## 6 General Policy

### 6.1 Role Description and Requirements

- 6.1.1 The Trust Director of Planning, Performance and Corporate Services has been assigned the role of **Senior Information Risk Owner (SIRO)**. The SIRO is responsible for overseeing Information Risk.

The SIRO will take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.

The SIRO will review and agree actions in respect of identified information risks as identified through quarterly IA audits.

The SIRO will provide a focal point for the resolution and/or discussion of information risk issues

The SIRO will ensure the NIAS Board is adequately briefed on information risk matters.

6.1.2 An **Information Asset Owner** (IAO) will be identified for each information asset.

The Cabinet Office 'Guidance on the IAO Role' identifies that, in order to meet the requirement of the Security Policy Framework, IAOs will:

- Lead and foster a culture that values, protects and uses information for the public good
- Know what information the asset holds, and what enters and leaves it and why
- Know who has access and why, and ensure their use of the asset is monitored
- Understand and address the risks to the asset, and provide assurance to the SIRO
- Ensure the asset is fully used for the public good, including responding to access requests

Providing assurance to the SIRO on the security and use of the asset will be via the IG Group at least annually.

The IAO will nominate an IAA to deputise in the event of the IAO being unavailable due to long-term absence and advise the Head of IG and DPO of such.

6.1.3 One or more **Information Asset Administrators** (IAAs) will be identified for each information asset. The IAAs will ensure that the policies and procedures relevant to their asset are followed.

The IAA will report any potential or actual security incidents or breaches.

## **6.2 Audits**

6.2.1 Regular audit reports will be completed by the IAOs and/or IAAs. These will provide assurance to the IG Group that all IAs are compliant with IG requirements

6.2.2 An annual report will be compiled by the Head of IG and DPO using information from the regular audits. This will form part of the evidence for the annual DSP Toolkit submission.

## **6.3 Information Asset Register**

6.3.1 An Information Asset Register (IAR) will be maintained by the Head of IG and DPO and contain information sufficient to provide assurance that all information is being processed within relevant legislation.

## **6.4 New Information Assets**

6.4.1 IAOs will be identified when a new IA is introduced within NIAS. The Manager / Project Team Leader responsible for procuring the asset will also be responsible for identifying the IAO.

6.4.2 The IAO will be responsible for advising the Head of IG and DPO of the 'new' asset and will supply sufficient details to complete the IAR.

## **6.5 Data Quality**

6.5.1 Access to high quality data is essential for patient care and effective performance management.

6.5.2 Each IAO will ensure that their IA can demonstrate adequate data quality assurance.

6.5.3 IAOs or IAAs will provide evidence of data quality checks as part of the audit process.

## **6.6 Business Continuity**



- 6.6.1 IAOs will ensure that their IA has a Business Continuity Plan (BCP) in place to safeguard the information contained within.
- 6.6.2 BCPs will be tested on a regular basis and findings detailed in the IAO audit.

## **6.7 Information Security**

- 6.7.1 Information security exists to safeguard the confidentiality, integrity and availability of information from threats whether deliberate or accidental.
- 6.7.2 IAOs will ensure that adequate access controls are in place for their IA e.g. password protection
- 6.7.3 Access controls will be documented for each IA
- 6.7.4 All breaches of information security will be reported to the Information Security Officer
- 6.7.5 All breaches of IG will be reported to the Head of IG and DPO.

## **6.8 Information Risk**

- 6.8.1 The IAO is responsible for information risk management for their IA, with support from the IAA, Information Security Officer and Head of IG and DPO.
- 6.8.2 Identified information risks will be logged in an appropriate risk register

## **6.9 Training**

- 6.9.1 The SIRO will complete annual Information Risk Management / SIRO, either by using material developed by HSC Digital or via other approved material or provider.
- 6.9.2 The IAOs and IAAs will complete annual Information Risk Management training, either by using material developed by HSC Digital or via other approved material or provider.

6.9.3 IAOs will ensure that new users are trained before allowing access to the IA and the information contained within.

## **7. Financial risks**

The Information Commissioner's Office (ICO) has the power to impose a financial penalty on an organisation for breaches of Data Protection legislation. There are two tiers of fine with the level of fine imposed dependent upon the breach. Tier one breaches can attract a fine of up to €10 mill or 2% of turnover and tier two a fine of up to €20 mill or 4% of turnover. Failing to manage information assets and the information processed within could attract a tier two fine. For further information on financial penalties, please refer to the Data Protection Policy.

## **8. Consultation**

This policy has been presented to the IG Group for consultation. The group has delegated authority to approve this document

## **9. References**

'Guidance on the IAO Role' (Cabinet Office, 2013) available from [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/365742/Guidance\\_on\\_the\\_IAO\\_Role.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365742/Guidance_on_the_IAO_Role.pdf)

## **10. Monitoring Compliance and Effectiveness of the Policy**

10.1 This policy will be reviewed annually by the Head of IG and DPO and approved by the IG Group, which reports to Governance and Audit Committee, a committee of the Board.

## Plan for Dissemination of Procedural Document

Title of document:	Information Asset Policy		
Version Number:	1.0	Dissemination lead: Print name, title and contact details	Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@nias.hscni.net
Previous document already being used?	No		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	SIRO, Information Asset Owners, Information Asset Administrators	
	Awareness for Reference Purposes	All staff	
	Awarenessto inform staff / other stakeholders	All staff	
Who does the document need to be disseminated to?	All staff have a responsibility to ensure that any new processes, systems or changes are implemented with regard to impact on personal information and confidentiality in accordance with legislation and national guidance therefore, all need to be aware of this policy.		
Proposed methods of dissemination: Including who will disseminate and when  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"><li>Information cascade by managers</li><li>Communication via Management/</li></ul>		<ul style="list-style-type: none"><li>Information cascade by managers</li><li>Notification via articles in bulletins</li><li>Posting on the intranet</li></ul>	

<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Data Protection Impact Assessment Policy and Procedure provides staff with the detail and guidance required on how to complete a DPIA at the beginning of a project to ensure that privacy and confidentiality issues are identified and addressed in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## INFORMATION DISCLOSURE AND TRANSFER POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation (see 'definitions' section 4)
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Information and Information Governance Strategy
- Information Governance Policy
- Confidentiality Code of Conduct
- Data Protection Policy
- Data Protection Rights Procedure
- Freedom of Information Policy and Procedure
- Information Lifecycle Management Policy
- Safe Haven Policy
- Information Sharing Policy
- Information Governance Review (aka Caldicott 2)
- Data Protection Impact Assessment Policy and Procedure

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

### This document has been published on the:

Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New Policy and Procedure for NIAS

## Contents

1. Introduction.....	4
2. Objectives.....	4
2.1 Openness.....	4
2.1 Confidentiality .....	4
3 Scope.....	5
4 Definitions.....	5
4.1 Personal information .....	5
4.2 Confidential information.....	5
4.3 Data Subject.....	5
4.4 Data Protection legislation.....	5
5 Responsibilities.....	6
5.1 Chief Executive Officer.....	6
5.2 Senior Information Risk Owner (SIRO) .....	6
5.3 Caldicott Guardian .....	6
5.4 Data Protection Officer.....	6
5.5 Head of Information Governance .....	6
5.6 Corporate Information Team.....	6
5.7 All staff.....	7
6 General Policy .....	7
7. Consultation.....	12
8. Monitoring Compliance and Effectiveness of the Policy.....	12
<b>Appendix 1</b> .....	1
Plan for Dissemination of Procedural Document.....	1

## **1. Introduction**

- 1.1 Northern Ireland Ambulance Service HSC Trust (NIAS) is committed to handling personal and non-personal information efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service. Information Governance (IG) gives assurances that NIAS will uphold this commitment.
- 1.2 This policy will detail what type of information may be disclosed and under what circumstances. This will provide all NIAS staff with comprehensive guidance on this area of IG compliance.

## **2. Objectives**

### **2.1 Openness**

NIAS recognises the need to maintain an appropriate balance between openness and confidentiality in the management and use of information. By being open about our activities and decision, making NIAS believes that stakeholders and the public will have greater confidence in the work undertaken. In addition, this may also lead to valuable feedback that may in turn improve NIAS's effectiveness.

### **2.1 Confidentiality**

NIAS fully acknowledges its obligation to be publicly accountable; however, we also place importance on the confidentiality and safeguarding of personal information relating to staff and patients and commercially sensitive information. NIAS regards all patient identifiable information as confidential. All staff personal information is considered confidential except where statutory obligations exist to disclose for the purposes of accountability.

NIAS will have clear procedures and arrangements for liaising with the press and broadcasting media. Issues arising from this aspect should be referred to the Deputy Director of Communications and Engagement.



### **3 Scope**

- 3.1 This policy applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who access personal and non-personal information.
- 3.2 This policy covers all aspects of information within NIAS including:
- Patient information
  - Staff information
  - Organisational information
- 3.3 All types of information are covered by this policy, including:
- Paper structured records
  - Electronic structured records
- 3.4 This policy covers all systems utilised by NIAS, the information contained within, and any individual employed, in any capacity, by us.

### **4 Definitions**

#### **4.1 Personal information**

Information that can identify an individual

#### **4.2 Confidential information**

Information that when provided was done so in the expectation it would be treated in confidence

#### **4.3 Data Subject**

The data subject is the individual who is the subject of the personal information

#### **4.4 Data Protection legislation**

Legislation, including, but not limited to the GDPR 2016 and UK Data Protection Act 2018

## **4.5 National Data Opt-Out**

4.5.1 The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes

## **5 Responsibilities**

### **5.1 Chief Executive Officer**

The Chief Executive Officer is the NIAS accounting officer and has overall accountability and responsibility for IG.

### **5.2 Senior Information Risk Owner (SIRO)**

The Senior Information Risk Owner will oversee information risk.

### **5.3 Caldicott Guardian**

The Caldicott Guardian will act as the 'guardian' of patient identifiable information and will oversee the use and sharing of patient information.

### **5.4 Data Protection Officer**

The Data Protection Officer will ensure NIAS can demonstrate its compliance with the Data Protection legislation

### **5.5 Head of Information Governance**

The Head of IG will manage the day to day IG agenda and provide assurance to the Board on compliance levels with associated policies.

### **5.6 Corporate Information Team**

The Performance Management Information Team (PMIT) will work closely with the Head of IG to ensure information sharing agreements are in place where necessary prior to sharing information

## **5.7 All staff**

All staff have a responsibility to comply with legislation and policy relating to IG and to identify and report any areas of concern.

## **6 General Policy**

### **6.1 Patient and Personal Information**

6.1.1 Specific HSC guidance has been developed to control the use of patient identifiable information (PII). The Information Governance Review (aka Caldicott 2) states that PII should be handled in accordance with the following principles:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary
- Use the minimum necessary personal confidential information
- Access to personal confidential data should be on strict need to know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality

6.1.2 The processing of personal information, relating to living individuals, is governed by the legislation. The processing of personal information can only proceed if one of the following conditions has been satisfied:

- Processing with the consent of the data subject
- Processing is necessary for the performance of a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of the data subject

- Processing is necessary for the performance of a task carried out in the public interest

6.1.3 However, under the legislation, medical information is classed as 'special category data' and affords even greater protection. Therefore, one of the following conditions will also need to be satisfied before processing can take place:

- Processing with the *explicit* consent of the data subject
- Processing is necessary for the purposes of carrying out obligation in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or another person, where it is not possible to gain consent
- Processing is carried out in the course of legitimate activities by a non-profit making organisation
- Processing relates to personal data which is manifestly made public by the data subject
- Processing is necessary for the purpose of, or in connection with, legal proceedings
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for medical or social care purposes and is undertaken by a health professional or a person owing a duty of confidence equivalent to that of a health professional.
- Processing is necessary for reasons of public interest in the area of public health.
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes

6.1.4 However, there may be circumstances when NIAS is obliged by law to disclose personal information. As listed in the legislation, these include:

- National security
- Defence
- Public security

- The prevention, investigation, detection or prosecution of criminal offences
- Important public interests – economic/financial interests (taxation matters), public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection or regulatory functions connected to the exercise of official authority (security, defence, crime/ethics prevention)
- The protection of the individual or the rights and freedoms of others
- The enforcement of civil law matters

6.1.5 The Access to Health Records Act 1990 relates specifically to records created by health professionals and includes those of deceased patients.

6.1.6 If appropriate, every effort will be made to obtain consent from the subject of the information prior to the disclosure.

## **6.2 Public Availability of Information**

6.2.1 NIAS is committed to making general information public, in accordance with the Freedom of Information Act 2000.

6.2.2 NIAS acknowledges that there are circumstances where information will not be made publicly available. These are:

- If the disclosure is considered exempt under the Freedom of Information Act 2000
- If the disclosure contravenes staff confidentiality
- If the disclosure contravenes patient confidentiality
- If the disclosure contravenes third party confidentiality
- If the disclosure could endanger an employee or partner of NIAS
- If the disclosure of the information may significantly affect NIAS's ability to achieve an objective

6.2.3 Where NIAS feels that it is unable to disclose information upon a request to do so, an explanation will be provided.

## **6.3 Responding to Information Requests**

### **6.3.1 Personal Information**

Personal information can be accessed by submitting a subject access request. This includes both staff and patient information. Further details on how to submit a request can be found in the Data Protection Rights Policy. Requests can only be accepted from the following:

- The data subject themselves
- The data subject's legal representative (with the data subject's consent)
- If the data subject is a minor, the legal guardian
- If the data subject is not capable of making a request, the person appointed to manage the data subject's affairs (power of attorney required)
- If the data subject is deceased, their personal representative, in accordance with the Health Records Act 1990.

The request will be handled in accordance with the subject access requirements as detailed in the legislation.

### **6.3.2 Requests from the Police**

Requests for personal information are often made by external bodies, in particular the police. Under the legislation, disclosure is appropriate if the information required is to assist with:

- The prevention or detection of an unlawful act
- The prevention of fraud

Procedures are in place for these and requests for patient information must be made on an official police data protection form sent to [NIAS.sd@nhs.net](mailto:NIAS.sd@nhs.net)

### 6.3.3 Non-Personal Information

Routine non-personal information can be obtained from NIAS under the Freedom of Information Act 2000.

Requests can be sent via email and a central email address is available:

[Informatics.department@nias.hscni.net](mailto:Informatics.department@nias.hscni.net)

## 6.4 Information Sharing Agreements

6.4.1 NIAS will sign up to information sharing agreements with other HSC and non-HSC bodies if it is felt appropriate and there is a legal basis to do so. These documents will clearly state the purpose for the agreement and how the information shared between the agencies will be managed and kept secure. Copies of these documents will be made available via the NIAS fair processing notices. A Data Protection Impact Assessment may also be required if the disclosure involves identifiable information. Reference should be made to the Data Protection Impact Assessment Policy and Procedure.

## 5.8 Transfers

6.5.1 Transfers of personal and patient information must be undertaken in a secure manner.

6.5.2 Emails – personal or patient information should not be sent  
Via email unless the following conditions are met:

- An hscni.net
- Official government body e.g. psni, gov.uk
- The file is encrypted – recommended to AES 256 bit

6.5.3 Post – bulk personal or patient information should only be sent through the post if the following conditions are met:

- The data is downloaded to a CD and encrypted using 256 bit encryption.

- The password is to be provided to the recipient upon receipt of the CD
- The CD is to be sent via recorded delivery

6.5.4 Fax – personal, patient or confidential information should only be sent to a secure fax machine unless additional steps are taken to protect the information.

- Telephone the intended recipient to inform them a fax is being sent
- Ask the recipient to wait by the fax machine while the fax is sent and then confirm receipt.
- Double check the fax number – use pre-programmable numbers wherever possible.
- Always use an NIAS fax cover sheet

6.5.5 Additional guidance on Safe Haven procedures can be found in the Safe Haven Policy and Procedure

## **6.6 Training**

6.6.1 Annual mandatory training in IG is included within the Corporate Induction and in the essential training programme for NIAS employees. This will ensure that staff are aware of their responsibilities with regard to the disclosure of information. In addition, this policy will be made publicly available and publicised in NIAS wide publications.

## **7. Consultation**

This policy will be presented to the IG Group for consultation. The group has delegated authority to approve this document

## **8. Monitoring Compliance and Effectiveness of the Policy**

The Head of IG will monitor the implementation of this policy and take assurance to the IG Group. This report will be sent on an annual basis. However, if the on-going monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent sooner. The Head of IG will also monitor information sharing agreements and instigate reviews when appropriate.



## Plan for Dissemination of Procedural Document

Title of document:	Information Disclosure & Transfer Policy		
Version Number:	13.0	Dissemination lead:	Janette Kirk, Head of IG and Data Protection Officer, janette.kirk@NIAS.nhs.uk
Previous document already being used?	Yes	Print name, title and contact details	
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	All staff	
	Awareness for Reference Purposes	All staff	
	Awareness to inform staff / other stakeholders	All staff	
Who does the document need to be disseminated to?	All staff have a responsibility to ensure information is disclosed and transferred appropriately and in accordance with legislation and national guidance therefore, all need to be aware of this policy.		
Proposed methods of dissemination: Including who will disseminate and when  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"><li>Information cascade by managers</li><li>Communication via Management/ Departmental/Team meetings</li><li>Notice board administration</li></ul>		<ul style="list-style-type: none"><li>Information cascade by managers</li><li>Notification via articles in bulletins</li><li>Posting on the intranet</li></ul>	

<ul style="list-style-type: none"> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<b>Summary for inclusion on the Class Publishing Applications system</b>	The Information Disclosure & Transfer Policy provides staff with the detail and guidance required on how and when to disclose and transfer information in accordance with legislation and national requirements.

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## INFORMATION GOVERNANCE POLICY

### Links

The following documents are closely associated with this policy:

- General Data Protection Regulation 2018
- Data Protection Act 2018
- Freedom of Information Act 2000
- Information Lifecycle Management Policy
- Information Disclosure and Transfer Policy
- Data Protection Policy
- Data Protection Rights Procedure
- Information Asset Policy
- Freedom of Information Policy
- IM&T Security Policy
- Confidentiality Code of Conduct

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	--

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				Rewritten in Corporate Template

## Contents

1.	Introduction.....	4
2.	Objectives.....	4
3.	Scope.....	4
4.	Definitions.....	5
4.1	Information Governance (IG) .....	5
4.2	Freedom of Information Act 2000.....	5
4.3	Data Protection Legislation .....	5
4.4	Information Asset.....	5
5	Responsibilities.....	5
5.1	Chief Executive Officer.....	6
5.2	Senior Information Risk Owner (SIRO) .....	6
5.3	Caldicott Guardian .....	6
5.4	Head of Information Governance.....	6
5.6	Information Asset Owners (IAO) .....	6
5.7	Information Asset Administrators (IAA) .....	6
5.8	All staff.....	7
6	Policy .....	7
6.1	Openness.....	7
6.2	Legal Compliance .....	7
6.3	Information Security .....	8
6.4	Information Quality Assurance.....	8
6.5	Records Management.....	9
7	Yearly Assessment.....	9
8	Caldicott Function.....	9
9	Training.....	9
10	Consultation .....	10
11	Monitoring Compliance and Effectiveness of the Policy .....	10
	<b>Plan for Dissemination of Procedural Document.....</b>	<b>11</b>

## **1. Introduction**

- 1.1. Northern Ireland Service HSC Trust (NIAS) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. Information plays a vital part in clinical governance, service planning and performance management.
- 1.2. Information Governance (IG) gives assurances that NIAS handles personal and non-personal information efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service.
- 1.3. NIAS will establish and maintain policies and procedures to ensure compliance with Information Governance requirements.

## **2. Objectives**

The key objectives of this policy are:

- 2.1 To provide assurance to the NIAS Board that we have a robust IG system in place.
- 2.2 To minimise the risks associated with the incorrect processing and management of information.
- 2.3 To ensure that NIAS meets its statutory obligations with regard to the processing and management of information.
- 2.4 To set out the responsibilities of NIAS staff with regard to IG.

## **3. Scope**

- 3.1 This policy covers all aspects of information within NIAS including:
  - Patient information
  - Staff information
  - Organisational information
- 3.2 All aspects of handling information are covered by this policy, including:

- Paper and electronic structured record systems
- The transmission of information via mail, e-mail, fax, instant messaging, video conferencing and telephone

3.3 This policy covers all information assets utilised by NIAS.

3.4 Responsibility for IG is contained within the remit of the Head of IG and overseen by the Director of Strategy and Transformation. However, complying with the requirements of IG is an organisation wide responsibility.

3.5 This policy applies to all employees of NIAS, including permanent, temporary, voluntary and contract staff, who come into contact with personal and non-personal information.

## **4. Definitions**

### **4.1 Information Governance (IG)**

4.1.1 Provides assurance that information, both personal and non-personal, is processed and managed in accordance with relevant guidance and legislation.

### **4.2 Freedom of Information Act 2000**

4.2.1 Provides the legal basis for responding to requests for non-personal information from Public Authorities.

### **4.3 Data Protection Legislation**

4.3.1 Legislation including, but not limited to, the General Data Protection Regulation (GDPR) and UK Data Protection Act 2018.

### **4.4 Information Asset**

4.5.1 Are assets that are owned or contracted by NIAS which have value. They are likely to include computer systems, information, software and staff.

## **5 Responsibilities**

## **5.1 Chief Executive Officer**

- 5.1.1 The Chief Executive Officer is the Accounting Officer of NIAS and has overall accountability and responsibility for IG.

## **5.2 Senior Information Risk Owner (SIRO)**

- 5.2.1 The Senior Information Risk Owner (SIRO) will oversee the development of the Information Risk Management Policy and take ownership of the risk assessment process for information risk. The SIRO is the Director of Strategy and Transformation.

## **5.3 Caldicott Guardian**

- 5.3.1 The Caldicott Guardian will act as the 'guardian' of patient identifiable information and will oversee the use and sharing of patient information. The Caldicott Guardian is the Medical Director.

## **5.4 Head of Information Governance**

- 5.4.1 The Head of IG will manage the day to day IG agenda and provide assurance to the Board on compliance.

## **5.5 Corporate Services Manager**

- 5.5.1 The Corporate Services Manager will manage requests for information and provide assurance to the Head of IG on the records management function

## **5.6 Information Asset Owners (IAO)**

- 5.6.1 The Information Asset Owners (IAO) are directly accountable to the SIRO and will provide assurance that information risk is being managed for their assigned information assets to the IG Group.

## **5.7 Information Asset Administrators (IAA)**

- 5.7.1 The Information Asset Administrators (IAA) will assist the IAOs and have day to day responsibility for the management of information risks for their assigned information asset.



## **5.8 All staff**

- 5.8.1 All staff will have a responsibility to comply with legislation and guidance relating to IG and identify and report any risks or areas of concern.

## **6 Policy**

### **6.1 Openness**

- 6.1.1 NIAS fully acknowledges its obligation to be publicly accountable; however, we also place importance on the confidentiality and safeguarding of personal information relating to staff and patients and commercially sensitive information while maintaining an appropriate balance between openness and confidentiality.
- 6.1.2 NIAS will have clear procedures and arrangements for liaison with the press and broadcasting media.
- 6.1.3 Patients will have access to information relating to their own health care, and there will be a clear procedure for handling personal information requests. Reference should be made to the Data Protection Rights Procedure.

### **6.2 Legal Compliance**

- 6.2.1 NIAS regards all identifiable personal information relating to patients as confidential, and all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
- 6.2.2 Non-personal, non-confidential information on NIAS and its services should be available through a variety of media in line with our Freedom of Information Publication Scheme.
- 6.2.3 NIAS will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000, the Data Protection legislation and other relevant legislation relating to the security and use of both personal and non-personal information.

6.2.4 NIAS will ensure that any transfers of personal information outside of the European Economic Area are only affected when sufficient security exists within the receiving country.

6.2.5 NIAS will establish and maintain policies for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act etc.)

6.2.6 NIAS will undertake or commission regular audits to assess its compliance with legal requirements.

### **6.3 Information Security**

6.3.1 NIAS will establish and maintain policies for the effective and secure management of its information assets and resources.

6.3.2 NIAS will undertake or commission regular audits to assess information and security arrangements.

6.3.3 NIAS will promote effective confidentiality and security practice to its staff through policies, procedures and training.

6.3.4 NIAS's incident reporting system will be used to report, monitor and investigate all breaches of confidentiality and security. Reference should be made to the Untoward Incident Reporting Policy.

### **6.4 Information Quality Assurance**

6.4.1 NIAS will establish and maintain policies for information quality assurance and the effective management of records.

6.4.2 IAOs will be expected to take ownership of, and seek to improve, the quality of information within their services.

6.4.3 Wherever possible, information quality will be assured at the point of collection.

6.4.4 NIAS will promote data quality through policies, procedures / user manuals and training.

## **6.5 Records Management**

- 6.5.1 NIAS will establish and maintain policies and procedures for the effective management of both clinical and corporate records, encompassing the whole process from creation to disposal

## **7 Yearly Assessment**

- 7.1 A self-assessment of compliance with requirements will be undertaken annually.

A number of requirements will be externally audited on an annual basis to ensure that submission rates are supported by adequate and appropriate evidence.

## **8 Caldicott Function**

- 8.1 The Caldicott function is overseen by the Caldicott Guardian.

- 8.2 The key responsibilities of the Caldicott function are to:

- Support the Caldicott Guardian
- Ensure the confidentiality and data protection work programmes are implemented and monitored
- Ensure that staff are aware of their responsibilities through policy, procedure and training
- Provide routine reports to the IG Group on confidentiality and data protection issues or areas of concern
- Support appropriate sharing of patient information in accordance with the National Data Guardian's consultation response review (Caldicott 3)

## **9 Training**

- 9.1 IG is included in the NIAS induction and essential learning programmes. Training can be requested at the discretion of a manager, or by an individual wanting personal development.
- 9.2 Further guidance and information relating to IG issues will be distributed periodically via various media including pay slip bulletins and NIAS newsletters.

## **10 Consultation**

- 10.1 This policy will be presented to the IG Group for consultation. The Group has delegated authority to approve this document.

## **11 Monitoring Compliance and Effectiveness of the Policy**

- 12.1 The Head of IG will monitor the implementation of this policy and take an assurance report to the IG Group. This report will be sent on an annual basis. However, if the on-going monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the Group sooner.

## Plan for Dissemination of Procedural Document

Title of document:	Information Governance Policy		
Version Number:	1.0	Dissemination lead: Print name, title and contact details	Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@nias.hscni.net
Previous document already being used?	Yes		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	All staff	
	Awareness for Reference Purposes	All staff	
	Awarenessto inform staff / other stakeholders	All staff	
Who does the document need to be disseminated to?	All staff have a responsibility to ensure information is managed and processed in accordance with legislation and national guidance therefore, all need to be aware of this policy.		

Data Quality Policy		Page:	11 of 14
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

<p><b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b></p> <p>Some examples of methods of disseminating information on procedural documents include:</p> <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Information Governance Policy provides staff with the detail and guidance required on how to manage and process information in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## **National Data Guardian Data Security Standards**

1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligations to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.
4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year at a minimum, with a report to senior management.
8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Quality Policy		Page:	13 of 14
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	

9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

10 IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Data Quality Policy		Page:	14 of 14
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	



## INFORMATION LIFECYCLE MANAGEMENT POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation (see 'definitions' section 4)
- Freedom of Information Act 2000
- Records Management Code of Practice for Health and Social Care 2016
- The Information Governance Review (AKA Caldicott 2)
- NIAS Retention & Disposal of Information Schedule
- Public Records Act 1958
- NIAS Confidentiality Code of Conduct
- Archive Procedure
- NIAS Disciplinary Procedure
- Policies, Strategies and Procedures Policy
- Information Sharing Policy
- Data Protection Policy
- Data Protection Rights Procedure
- Freedom of Information Policy and Procedure

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

### This document has been published on the:

Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<p><b>Document Location</b></p> <p>If using a printed version of this document ensure it is the latest published version.</p> <p>The latest version can be found on the Trust's Intranet site.</p>
------------------------	--

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy. Combines previous Records Management Policy, Retention and Disposal of Information Policy and Archive Policy and Procedure

## Contents

1. Introduction.....	4
2. Objectives.....	5
3. Scope.....	6
4. Definitions.....	6
4.1 NIAS.....	6
5. Types of Information.....	6
6. Data Protection legislation.....	6
7. Responsibilities.....	6
7.1 Chief Executive Officer.....	7
7.2 Senior Information Risk Owner (SIRO).....	7
7.3 Head of Information Governance.....	7
7.4 Data Protection Officer.....	7
7.5 Information Asset Owner (IAO).....	7
7.6 Information Asset Administrators (IAA).....	7
7.7 Medical Director.....	7
7.8 Corporate Services Manager.....	8
7.9 All NIAS staff.....	8
7.10 Operational staff.....	8
7.11 Information Governance Team.....	8
7.12 Duties Relating to Confidentiality and Data Protection:.....	8
8. Legal Obligations.....	8
9. Information Quality Assurance.....	9
10. Record Creation.....	10
11. Naming Records.....	10
12. Record Keeping.....	10
13. Tracking and Tracing.....	11
14. Review of Records.....	11
15. Access to Copies of PRFs.....	11
16. Disclosure and Transfer of Records.....	12
17. Storage and Retention of Records.....	12
18. Archiving Paper Records.....	13
19. Retrieval of Records.....	14
20. Rules on Disposal.....	14
21. Freedom of Information Requests.....	15
22. Additional Assurances.....	16
23. Consultation.....	16
24. Monitoring Compliance and Effectiveness of the Policy.....	16
Appendix 1.....	17

Information Lifecycle Management Policy		Page:	3 of 17
Document ID:	FN.08/18	Version:	8.0
Date of Approval:		Status:	Draft
Approved by:	Information Governance & Security Group	Date of Review:	July 2019

## 1. Introduction

- 1.1 Information Lifecycle Management (ILM) expands upon records management as it encompasses the whole process from the creation of records through to their ultimate disposal, and includes the security, disclosure, retention and archiving aspects.

A record can be defined as:

*‘A permanent account of something that is kept for evidence or information’* (source Oxford English Dictionary)

The key elements of ILM are:

- Record creation
  - Record keeping
  - Record maintenance
  - Information quality
  - Information disclosure and transfer
  - Information storage
  - Retention of information
  - Archiving of information
  - Disposal of information
- 1.2 Records are a valuable resource because of the information they contain, and high-quality information underpins the delivery of a high-quality service. Information is of the greatest value when it is accurate, up to date and accessible when it is needed. Effective records management ensures that information is properly managed and available when required:
- to support the day to day business of NIAS
  - to support patient care
  - to support evidence based clinical practice
  - to meet legal requirements
  - to support administrative and management procedures and decision making
  - to assist clinical and other audits
  - to support improvements in clinical effectiveness
  - to support access to records (e.g. for Freedom of Information requests)
  - to support archival functions

- to ensure external compliance with awarding bodies
- 1.3 As all HSC records are categorised as public records, NIAS has a duty under the Public Records Act 1958 to plan for the safekeeping and eventual disposal of all types of records. Data Protection legislation and the Freedom of Information Act 2000 (repealed 5 of the Public Records Act 1958) also place statutory obligations on the processing of information.
- 1.4 The destruction of records is an irreversible act that must not be taken lightly. However, the fifth principle of the Data Protection legislation (Article 5 1(e)) states personal data shall be:

*‘Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.....’*

The minimum retention periods for records can be found in the ‘Retention and disposal of information schedule’

- 1.5 The process for archiving records can be found in the ‘Archiving procedure’
- 1.6 NIAS is committed to the practice of effective information lifecycle management.

## **2. Objectives**

2.1 The key objectives of this policy document are:

- To ensure that all staff are aware of the importance of effective records management and its associated components.
- To ensure the legal obligations of the Public Records Act 1958 (excl. S5), Data Protection legislation and the Freedom of Information Act 2000 are adhered to.
- To provide a consistent approach to the way personal and non-personal information is processed, from creation through to destruction.
- To provide a consistent approach to the way records are kept

### **3. Scope**

- 3.1 This policy applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who come into contact with personal and non-personal information.

### **4. Definitions**

#### **4.1 NIAS**

- 4.1.1 Northern Ireland Ambulance Service HSC Trust

### **5. Types of Information**

- 5.1 This policy covers the following types of information and records:

- Patient Report Forms (PRFs & ePRFs) – both electronic and paper-based
- Incident logs (obtained from the Computer Aided Dispatch (CAD) system – both electronic and paper-based
- Non-emergency patient transport records – both electronic and paper-based
- Administrative records (including personnel, estates, finance, complaints etc.
- Audio and video tapes, cassettes, CD-ROM etc.
- E-mails
- Digital records
- Computerised records
- Scanned records
- CCTV images

This list is not exhaustive and will include any media where information, either personal or non-personal, is recorded electronically or in paper format.

### **6. Data Protection legislation**

- 6.1 Legislation including, but not limited to, the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018

### **7. Responsibilities**

## **7.1 Chief Executive Officer**

- 7.1.1 The Chief Executive Officer has overall responsibility for Information Lifecycle Management (ILM).

## **7.2 Senior Information Risk Owner (SIRO)**

- 7.2.1 The **Senior Information Risk Owner** (SIRO) is the accountable officer for NIAS and is responsible for ensuring appropriate mechanisms are in place to support the ILM function.

## **7.3 Head of Information Governance**

- 7.3.1 The ILM function should be recognised as a specific corporate responsibility within NIAS. The Head of Information Governance (IG) has been designated as the member of staff with lead responsibility for this function.

## **7.4 Data Protection Officer**

- 7.4.1 The DPO is a mandatory role that will ensure NIAS can demonstrate its compliance with Data Protection legislation.

## **7.5 Information Asset Owner (IAO)**

- 7.5.1 An Information Asset Owner (IAO) will be identified for each information asset (system). These will have overall responsibility for managing the risks to the assets. Assurance will be provided, via the self-assessment checklist, to the IG Group.

## **7.6 Information Asset Administrators (IAA)**

- 7.6.1 Information Asset Administrators (IAA) will be identified for information assets (systems). IAOs may delegate responsibility for managing the information risks to the IAAs, however, overall responsibility remains with the IAO.

## **7.7 Medical Director**

- 7.7.1 Overall responsibility for the management of clinical records lies with the Medical Director.

## **7.8 Corporate Services Manager**

- 7.8.1 The Corporate Services Manager is responsible for providing advice on the records management process and for conducting records audits.

## **7.9 All NIAS staff**

- 7.9.1 All NIAS staff, whether clinical or administrative, who create, receive and use records have responsibilities for ILM. In particular all staff must ensure that they keep appropriate records of their work in NIAS and manage those records in keeping with this policy and any legal requirements.

## **7.10 Operational staff**

- 7.10.1 Operational staff, both A&E and PTS, are responsible for the safe and secure keeping of PRFs and ePRFs and patient journey logs while in their possession or in station. They have a duty to ensure these records remain secure and confidential.

## **7.11 Information Governance Team**

- 7.11.1 The Governance team will be responsible for ensuring the policy library is kept up to date with the latest version of each NIAS policy, standing operating procedure etc.

## **7.12 Duties Relating to Confidentiality and Data Protection:**

- 7.12.1 All HSC bodies have a common law duty of confidence to patients and staff alike. Everyone working for NIAS who records, handles, stores or otherwise comes across patient or personal information has a duty to maintain this confidentiality. This includes selecting a method of storage and ultimate disposal that will uphold this obligation.

## **8. Legal Obligations**

- 8.1 All staff must be aware of the need to manage records in accordance with legislation and guidance produced. These include:



- The Data Protection Act 2018
- UK GDPR 2021
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Caldicott Principles 2013

8.2 NIAS operates separate policies in the areas of Data Protection and Freedom of Information and The NIAS Code of Conduct for Confidentiality incorporates Caldicott guidance. Reference should be made to these documents.

8.3 It is a legal requirement that HSC records, which have been selected as archives, should be held in a repository that has been approved for the purpose by the National Archives. The document 'Records Management Code of Practice for Health and Social Care 2016 contains details on these recommended repositories.

## **9. Information Quality Assurance**

9.1 Effective information is that which is of the highest quality. It is essential that all staff responsible for the creation of records are fully aware of their obligation to ensure their integrity is maintained. Therefore, records should be:

- factual, consistent and accurate
- recorded as soon as possible after an event has occurred, therefore providing current information
- Recorded in such a way that any alterations, deletions or additions are annotated with details of when these were done and by whom.
- recorded in such a way that any inaccuracies, as indicated by the data subject, can be corrected in a timely manner with details of any amendments annotated
- free of jargon, abbreviations (unless officially accepted), meaningless phrases, offensive language or comments, irrelevant speculation or unsupported opinions
- readable on any scanned or photocopied images
- Filed in a way that supports the ability to readily identify and retrieve information where and when it is needed.

## **10. Record Creation**

Record creation is one of the most important processes in records management, and the aim should be to create good records in an effective system.

- 10.1 Reference should be made to the Policies, Strategies and Procedures Policy when creating corporate records.
- 10.2 Records should be created in a manner that reflects the corporate style and HSC branding, using corporate templates where appropriate, and standard version control used.
- 10.3 Records should be filed in a way that allows for them to be tracked. This includes the archiving process.
- 10.4 A protective mark should be applied if appropriate.
- 10.5 The record should be allocated a meaningful name which closely reflects the records contents, allowing for easy location.

## **11. Naming Records**

- 11.1 Records should be given meaningful names reflecting the content
- 11.2 A record should be given a unique name
- 11.3 Records that are linked should be given similarly structured and worded names e.g. earlier and later versions

## **12. Record Keeping**

- 12.1 Each directorate will ensure that records are kept and maintained effectively. Sufficient information should be logged to ensure that records can be retrieved, archived and disposed of as necessary. The record keeping system should include a set of rules for referencing, titling and indexing, and if appropriate, the protective marking of documents. The movement and location of records should be controlled to provide an auditable trail.
- 12.2 PRFs will be delivered to the Information Governance Department where they will be scanned and verified.

### **13. Tracking and Tracing**

13.1 There should be tracking and tracing procedures in place that enable the movement and location of records to be controlled and provide an auditable trail of record transactions. The tracking system should include:

- An identifier for the record e.g. name, unique number
- A description of the record
- The person who has requested the record, and who has been provided with that record
- The date the record was accessed and returned (if physically removed)
- For paper records, a location card should be placed in the space where the record has been removed from.

### **14. Review of Records**

14.1 Review dates should be allocated to all policies and procedures. It is essential that these are adhered to in order to meet the Governance requirements. Details of all policies, including their review dates, will be contained in a central electronic file accessible by all staff.

14.2 Following review, superseded policies will be placed in a limited access electronic file by the Governance Team, to facilitate possible future claims, coroners' requests or to support other legal obligations.

### **15. Access to Copies of PRFs**

15.1 Access to electronic PRFs (ePRFs) is controlled via Position Based Access Control (PBAC) codes allocated to an individual's Smartcard.

15.2 Printing unanonymised ePRFs is strictly prohibited. Web viewer allows a member of staff, with the required access rights, to print an anonymised copy of an ePRF. Unauthorised copying is deemed a breach of confidentiality and a disciplinary offence (as per the NIAS Disciplinary Procedure). Access to ePRFs will be monitored as will any unauthorised printing.

- 15.3 Photocopying unanonymised paper PRFs is strictly prohibited. Unauthorised copying is deemed a breach of confidentiality and a disciplinary offence (as per the NIAS Disciplinary Procedure). Copies of these records can be requested in writing from the Clinical Audit Department using the recognised request form CL3.

## **16. Disclosure and Transfer of Records**

- 16.1 The disclosure, or non-disclosure, and transfer of information/clinical records is subject to legislation. Reference should be made to the following:
- All information – Information Disclosure and Transfer Policy / Information Sharing Policy
  - Personal information – Data Protection Policy
  - Non-personal information – Freedom of Information Policy and Procedure
  - Specific information – Code of Conduct for Confidentiality

## **17. Storage and Retention of Records**

- 17.1 To ensure compliance with this policy, each department should have in place an effective records management system. This should cover filing, archiving and disposal and should enable staff to access records, archive when necessary and ultimately dispose of them (in line with the Retention and Disposal of Information Schedule). It is essential that records are easily accessible (both Computerised and manual) for the purposes of access requests under Data Protection legislation and the Freedom of Information Act 2000.
- 17.2 Records should be stored securely, when not in use, in lockable desk drawers, cabinets or safes within a locked room. The accommodation should comply with health and safety requirements have proper environmental controls and adequate protection against fire, flood and theft. Please refer to the IM&T Security Policy for further information.
- 17.3 Retention periods for records are detailed in the Retention and Disposal of Information Schedule. The schedule takes account of

the retention periods as detailed in the Records Management Code of Practice for Health and Social Care 2016.

17.4 Patient Report Forms (PRFs), once scanned, will be destroyed securely by cross shredding. Scanned images will be copied on to virtual WORM (Write Once Read Many) media. This ensures that the information contained cannot be altered. These images will be backed up on a monthly basis. Retention of these records will be in accordance with the Retention and Disposal of Information Schedule. Reference should also be made to the NIAS 'Clinical Record Keeping Policy'

17.5 Back-up Tapes - NIAS IT information systems will be backed up daily and stored on-site in a secure access controlled safe. Monthly back-ups will be undertaken, and the tapes stored in a secure safe off-site, but still on NIAS premises. Retention of the records contained on the tapes will be retained in accordance with the Retention and Disposal of Information Schedule.

#### 17.6 Additional Guidance

- The minimum retention periods should be calculated from the beginning of the year after the last date on the record
- The provisions of Data Protection legislation must be complied with
- Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Local business requirements/instructions must be considered before activating retention periods as detailed in the Retention and Disposal of Information Schedule.

### 18. Archiving Paper Records

18.1 Records destined for archiving must be done so in accordance with the NIAS Archiving Procedure.

18.2 The archiving process will be managed by the Corporate Services Manager, who will oversee the archive and retrieval of paper records.

18.3 The archive process will be fully auditable.

## 19. Retrieval of Records

- 19.1 Retained records must be created and stored in a manner that allows for ease of retrieval whilst ensuring the records remain secure.
- 19.2 A tracking system should be in place for all paper records, and electronic systems should have audit facilities.
- 19.3 PRFs will be scanned into a Clinical Audit system with a unique identifier automatically allocated.

## 20. Rules on Disposal

- 20.1 Disposal does not necessarily mean destruction. For example, a record considered to have historical value may be disposed of by storing it at an off-site archival facility.
- 20.2 As most HSC records, including administrative ones, contain sensitive or confidential information, those that are destroyed must have their confidentiality safeguarded. Therefore, the method used to dispose of the records must be fully effective in securing their illegibility. Further guidance can be obtained from the Corporate Services Manager.
- 20.3 **PRFs** - PRFs retained in paper format will be destroyed by shredding once their retention period has passed. The shreds are then to be disposed of in a confidential waste sack. Confidential waste boxes should not be used to dispose of these records unless the record has been shredded first. Those that have been scanned to non-re-writable media will be destroyed by shredding once the scanning and save process has been completed.

**NB** Clinical **Audit** use Canon confidential waste sacks whereby records do not require pre-shredding.

- 20.4 Identifiable and Confidential Information - Records containing sensitive personal details e.g. medical, should be disposed of by shredding. Information considered able to identify its subject, both patient and staff, should be disposed of by using the confidential waste bins (situated at some NIAS sites) or confidential waste

sacks. Likewise, non-personal information considered to be confidential must be disposed of in this way.

20.5 Non-Identifiable and Non-Confidential Information - Paper records containing no person identifiable information or that is considered to contain no confidential non-personal information can be disposed of in the paper recycling bins situated at some NIAS sites, or in the everyday waste bins.

20.6 Information held on Computer Hard Disks - Information held on the hard disk of a computer must be disposed of by an approved specialist company. A confidentiality agreement must be signed by the destruction company and a 'certificate of proof of destruction' obtained on completion of the 'cleaning' of the computer equipment.

**Note – the destruction of any computer hardware can only be authorised by the IM&T Department.**

20.7 CCTV Images - Guidance on the overwriting of CCTV tapes can be found in the NIAS Policy on the Use of CCTV Systems.

20.8 Internet and Intranet - Information on the NIAS Internet and Intranet is also covered by this policy and documents retained on these media should be disposed of in accordance with the Retention and Disposal of Information Schedule.

20.9 Any queries in relation to retention periods or disposal methods should be directed to the Corporate Services Manager.

## **21. Freedom of Information Requests**

21.1 If a record due for destruction is known to be the subject of an information request, destruction should be delayed until disclosure has taken place. However, if NIAS has decided not to release the information, the record should be retained until any resultant complaint and/or appeal has been concluded.

21.2 If a record has been accidentally destroyed, prior to its recommended disposal date, the individual concerned should be offered advice on this policy and records management procedures. If it is found that records have been destroyed inappropriately, unlawfully or maliciously, disciplinary action may be initiated.



- 21.3 Should the destroyed information become the subject of a Freedom of Information request the applicant should be advised of the complaints procedure to follow.

## **22. Additional Assurances**

- 22.1 The creation of clinical records will be done so in accordance with the Clinical Record Keeping Policy
- 22.2 An appropriately trained individual will have specific responsibility for the ILM function.
- 22.3 Everyone handling information will be appropriately trained to do so in accordance with legal requirements and national guidance. All NIAS staff must comply with the essential training matrix requirement in connection with the training and education on IG, including Records Management. Training will be included within the Essential Education programme and in the Induction training for new starters.
- 22.4 It is important that everyone is aware of the need to manage their information in accordance with relevant legislation, NIAS policies and HSC guidelines. NIAS publications will be used to embed the policies, procedures etc.
- 22.5 Standard version control will be used on all policy and procedure documents.
- 22.6 All staff have been provided with or have access to a copy of the 'Confidentiality and Security Handbook'
- 22.7 Everyone creating records is aware of the standards expected.

## **23 Consultation**

- 23.1 This policy will be presented to the Information Governance Group for consultation. The group has delegated authority to approve this document.

## **24 Monitoring Compliance and Effectiveness of the Policy**



24.1 The Head of IG and DPO will monitor the implementation of this policy, and take an assurance report to the IG Group. This report will be sent on an annual basis. However, if the ongoing monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the group sooner.

## Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Information Lifecycle Management Policy</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead:</b>	<b>Tracy Avery, Head of IG and Data Protection Officer, Tracy.avery@NIAS.hscni.net</b>
<b>Previous document already being used?</b>	<b>No</b>	<b>Print name, title and contact details</b>	
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	Staff have a responsibility to ensure that any information is appropriately managed from creation to disposal in accordance with the relevant legislation.		
<b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b>  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/</i></li> </ul>		<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>	

<p><i>Departmental/Team meetings</i></p> <ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Information Lifecycle Management Policy provides staff with the detail and guidance required on how to manage information from creation of a record through to its ultimate disposal in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*



## INFORMATION RISK MANAGEMENT POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation
- Freedom of Information Act 2000
- Health Records Act 1990
- Information and Information Governance Strategy
- Information Governance Policy
- Risk Management Policy
- Information Asset Policy
- Information Asset Owners and Administrators Handbook

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New Policy and Procedure for NIAS

## Contents

1. Introduction .....	4
2. Objectives .....	4
3. Scope.....	4
4. Definitions .....	5
4.1 Risk .....	5
4.2 Consequence.....	5
4.3 Likelihood .....	5
4.4 Risk Assessment .....	5
4.5 Risk Management.....	5
4.6 Information Asset.....	6
4.7 Data Protection legislation.....	6
5. Responsibilities .....	6
5.1 Chief Executive Officer.....	6
5.2 Senior Information Risk Owner (SIRO).....	6
5.3 Head of Information Governance (IG).....	6
5.4 Data Protection Officer.....	6
5.5 Information Asset Owners (IAO).....	6
5.6 Information Asset Administrators (IAA) .....	7
5.7 All staff.....	7
6. Role Description and Requirements .....	7
7. Information Governance Risk Register .....	8
8. Information Assets .....	9
9. Information Asset Register .....	9
10. Information Asset Audits .....	9
11. Information Risk Assessment and Management Programme	10
12. Training .....	10
13. Consultation.....	11
15. References .....	11
16. Monitoring Compliance and Effectiveness of the Policy.....	11
Plan for Dissemination of Procedural Document .....	12
<i>Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.....</i>	13

## **1. Introduction**

- 1.1 Northern Ireland Ambulance Service HSC Trust (NIAS) is committed to handling personal and non-personal information efficiently, securely, effectively and in accordance with relevant legislation, with the objective of delivering the best possible care and service. Information Governance (IG) gives assurances that we will uphold this commitment.
- 1.2 NIAS has approved the introduction and embedding of information risk management into approval processes and business functions. This reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and NIAS itself.
- 1.3 Information risk is inherent in all functions undertaken by NIAS and everyone working for them continuously manages this risk. It is widely accepted that the aim of information risk is not to eliminate risk, but rather to provide a structural means to identify, prioritise and manage these risks.

## **2. Objectives**

- 2.1 To manage the information risks identified through day to day functions, approval, change and review processes and audit programmes.
- 2.2 To protect NIAS, its patients and staff from information risks that may have a significant consequence or likelihood of occurrence.
- 2.3 To provide a consistent risk management framework whereby information risks can be identified and addressed in approval, change, review and audit processes.
- 2.4 To meet legal or statutory requirements
- 2.5 To assist in safeguarding NIAS's information assets

## **3. Scope**

- 3.1 This policy covers all aspects of information within NIAS including:



- Patient information
- Staff information
- Organisational information

3.2 All types of information are covered by this policy, including:

- Paper structured records
- Electronic structured records

3.3 This policy covers all systems utilised by NIAS, and the information contained within.

3.4 This policy applies to all employees of NIAS, including permanent, temporary, voluntary and contract staff, who may come into contact with information.

## **4. Definitions**

### **4.1 Risk**

4.1.1 The chance of something going wrong; that danger, injury or damage will occur. Uncertainty of outcome, whether positive opportunity or negative threat.

### **4.2 Consequence**

4.2.1 The outcome of an event or situation, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.

### **4.3 Likelihood**

4.3.1 A qualitative description for probability or frequency

### **4.4 Risk Assessment**

4.4.1 The evaluation of risk with regard to the impact if the risk is realised and the likelihood of the risk being realised.

### **4.5 Risk Management**

- 4.5.1 All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

## **4.6 Information Asset**

- 4.6.1 An identifiable and definable asset which is 'valuable' to the business.

## **4.7 Data Protection legislation**

- 4.7.1 Legislation including, but not limited to, the General Data Protection Regulation 2016 and Data Protection Act 2018

## **5. Responsibilities**

### **5.1 Chief Executive Officer**

- 5.1.1 The Chief Executive Officer is the Accounting Officer of NIAS and has overall accountability and responsibility for IG.

### **5.2 Senior Information Risk Owner (SIRO)**

- 5.2.1 The Senior Information Risk Owner (SIRO) will oversee the development of the Information Risk Policy and Strategy and take ownership of the risk assessment process for information risk. The SIRO is the Director of Planning, Performance and Corporate Services.

### **5.3 Head of Information Governance (IG)**

- 5.3.1 The Head of Information Governance (IG) will manage the day to day IG agenda and provide assurance to the Board on compliance.

### **5.4 Data Protection Officer**

- 5.4.1 The Data Protection Officer (DPO) will ensure NIAS can demonstrate its compliance with Data Protection legislation

### **5.5 Information Asset Owners (IAO)**

- 5.5.1 Information Asset Owners (IAO) are directly accountable to the SIRO and will provide assurance that information risk is being managed for their assigned information assets through quarterly assessments.

## **5.6 Information Asset Administrators (IAA)**

- 5.6.1 Information Asset Administrators (IAA) will assist the IAOs and have day to day responsibility for the management of information risks for their assigned information asset.

## **5.7 All staff**

- 5.7.1 All staff will have a responsibility to comply with legislation and guidance relating to IG and identify and report any risks or areas of concern.

## **6. Role Description and Requirements**

- 6.1 The NIAS Director of Planning, Performance and Corporate Services has been assigned the role of SIRO. The SIRO is responsible for overseeing the development of the Information Risk Management Policy.

The SIRO will take ownership of the risk assessment process for information risk, including review of the annual information risk assessment to support and inform the Statement of Internal Control.

The SIRO will review and agree action in respect of identified information risks.

The SIRO will provide a focal point for the resolution and/or discussion of information risk issues

The SIRO will ensure the NIAS Board is adequately briefed on information risk matters.

- 6.2 An IAO will be identified for each information asset.

The Cabinet Office 'Guidance on the IAO Role' identifies that, in order to meet the requirement of the Security Policy Framework, IAOs will:

- Lead and foster a culture that values, protects and uses information for the public good
- Know what information the asset holds, and what enters and leaves it and why
- Know who has access and why, and ensure their use of the asset is monitored
- Understand and address the risks to the asset, and provide assurance to the SIRO
- Ensure the asset is fully used for the public good, including responding to access requests

Providing assurance to the SIRO on the security and use of the asset will be via the IG Group at least annually.

- 6.3 One or more IAAs will be identified for each information asset. The IAAs will ensure that the policies and procedures relevant to their asset are followed.

The IAA will report any potential or actual security incidents or breaches.

- 6.4 The Head of IG will develop the Information Risk Management Policy.

The Head of IG will monitor and maintain the IG risk register and provide reports to the IG Group on risks identified and actions taken and provide assurance to the SIRO that these have been assessed and addressed appropriately.

- 6.5 The Information Security Manager will work closely with the IM&T infrastructure team to ensure that all information assets are protected through technical solutions e.g. virus protection, firewalls, encryption etc. The Information Security Manager will also support the Business Continuity function thereby ensuring continuity of service.

## **7. Information Governance Risk Register**

- 7.1 A dedicated risk register is used to log, assess and manage information risks. This will be managed by the Head of IG. The Finance and Performance Committee will receive assurance on the management of the identified risks.
- 7.2 A risk matrix is used to assess the level of risk. The matrix can be found in the Risk Management Policy.

## **8. Information Assets**

Although likely to include computer systems and network hardware and software, an information asset is not limited to technical solutions. Other categories of information asset could include:

- 8.1 *Information* - Includes: Database, system documents and procedures, paper records etc.
- 8.2 *Software* – Includes: Application programs, system development tools and utilities
- 8.3 *Physical* – Includes: Infrastructure, equipment, furniture etc.
- 8.4 *Services* – Includes: Computing and communications, heating, lighting, power, air conditioning used for data processing
- 8.5 *People* – Includes: Qualifications, skills and experience in use of information systems
- 8.6 *Intangibles* – Includes: Public confidence in NIAS's ability to ensure the confidentiality, integrity and availability of personal data

## **9. Information Asset Register**

- 9.1 NIAS will maintain an up to date information asset register, to include the details of the IAO and IAAs for each.
- 9.2 The information asset register should link all the relevant components as listed in section 8 thereby giving a complete picture of each asset, its owner, policies etc.

## **10. Information Asset Audits**

- 10.1 Information assets will undergo regular audits to ensure they are compliant with IG arrangements and to minimise risk. Information will be gathered via templates and results reported to the IG Group.

## **11. Information Risk Assessment and Management Programme**

- 11.1 Information risks can be identified by any member of staff. However, IAOs and IAAs will have responsibility for identifying risks within their 'own' information asset.
- 11.2 Information risks are included within the IG risk register. Reports are provided to the IG Group (bi-monthly) on the current status of these risks. Their level of risk will be assessed and agreed by the SIRO.
- 11.3 The Finance and Performance Committee receives a report from the SIRO on the risks within the IG risk register.
- 11.4 Information risks that are identified as having a greater impact on NIAS, as a whole, will be escalated to the corporate risk register.
- 11.5 Spot check security audits are undertaken by the Information Security Manager, with support from the Head of IM&T to ensure the following:
- the integrity of the information is upheld
  - access controls are in operation for electronic files
- 11.6 The results of the spot check audits are presented to the Information Security Group to provide assurance around the level of security for information and information assets.
- 11.7 Information security concerns and issues are reported to the Information Security Group
- 11.8 The Head of IG will work closely with the IAOs to ensure that the information assets remain compliant with IG requirements.

## **12. Training**

- 12.1 The SIRO is required to complete information risk management training on an annual basis.
- 12.2 The IAOs, IAAs and Head of IG should complete information risk management training regularly

### **13. Consultation**

- 13.1 This policy will be presented to the IG Group for consultation.  
The Group has delegated authority to approve this document

### **15. References**

‘Guidance on the IAO Role’ (Cabinet Office, 2013) available from [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/365742/Guidance\\_on\\_the\\_IAO\\_Role.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365742/Guidance_on_the_IAO_Role.pdf)

### **16. Monitoring Compliance and Effectiveness of the Policy**

- 16.1 The Head of IG will monitor the implementation of this policy, and take an assurance report to the IG Group. This report will be sent on an annual basis.
- 16.2 In addition, monitoring reports will be presented to the IG Group to advise on current and new information risks identified.

## Plan for Dissemination of Procedural Document

Title of document:	Information Risk Management Policy		
Version Number:	1.0	Dissemination lead: Print name, title and contact details	Tracy Avery, Head of IG and DPO, Tracy.Avery@nias.hscni.net
Previous document already being used?	No		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	Information Asset Owners and Information Asset Administrators	
	Awareness for Reference Purposes	All staff	
	Awareness to inform staff / other stakeholders	SIRO	
Who does the document need to be disseminated to?	All information asset owners and administrators and the SIRO.		

Data Quality Policy		Page:	12 of 13
		Version:	1.0
Date of Approval:		Status:	Draft
Approved by:		Next Review Date:	



<p><b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b></p> <p>Some examples of methods of disseminating information on procedural documents include:</p> <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>
<p><b>Summary for inclusion on the Class Publishing Applications system</b></p>	<p>The Information Risk Management Policy provides information asset owners and administrators with the information they require to support their responsibilities for the system they 'own'.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## INFORMATION SHARING POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation (see 'definitions' section 4)
- Freedom of Information Act 2000
- Information Governance Policy
- Information Disclosure and Transfer Policy
- Data Protection Policy
- Data Protection Rights Policy and Procedure
- Data Security and Protection Toolkit
- ICO: Data Sharing Code of Practice (May 2011)
- Complaints Policy
- Research, Management and Governance Policy
- Induction Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Informatics and Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	NIAS Trust

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New policy and Procedure for NIAS

## Contents

1. Introduction.....	4
2. Objectives.....	4
3. Scope .....	4
4. Definitions.....	5
5. Responsibilities.....	6
6. The Information Commissioner's Data Sharing Code of Practice (May 2011).....	7
7. Data Sharing and the Law.....	7
8. Factors to Consider before Sharing.....	7
9. Information Sharing for Direct Care.....	8
10. Consent.....	8
11. Fair Processing Notices.....	9
12. Security .....	9
13. Data Sharing Agreements .....	10
14. Right of Access by the Data Subject.....	11
15. Specific Information Sharing.....	11
16. Issues to Avoid.....	11
17. Information Commissioner's Powers and Penalties .....	12
18. Caldicott Function .....	12
19. Training .....	13
20. Consultation.....	13
21. References .....	13
22. Monitoring Compliance and Effectiveness of this Policy .....	14
Plan for Dissemination of Procedural Document.....	15
<b>Data Sharing Checklist – Systematic Data Sharing .....</b>	<b>17</b>

Information Lifecycle Management Policy		Page:	3 of 17
Document ID:	FN.08/18	Version:	8.0
Date of Approval:		Status:	Draft
Approved by:	Information Governance & Security Group	Date of Review:	July 2019

## **1. Introduction**

- 1.1. Northern Ireland Ambulance Service HSC Trust (NIAS) recognises the importance of sharing information for the purposes of direct care, if it is in the vital interests of the patient or if statute dictates. However, NIAS is also mindful of its responsibilities with regards to complying with relevant legislation and national guidance.
- 1.2. This policy links closely to the Information Commissioner's 'Data Sharing Code of Practice' (May 2011), and good practice taken from this document has been included.
- 1.3. This policy will ensure that information sharing is undertaken in accordance with the law.
- 1.4. This policy should be read in conjunction with the Information Disclosure and Transfer Policy to ensure that information is shared in a secure manner.

## **2. Objectives**

The key objectives of this policy are:

- 2.1 To provide assurance to the Board that NIAS has a managed information sharing process in place.
- 2.2 To minimise the risks associated with the incorrect or unlawful sharing of information.
- 2.3 To ensure that NIAS meets its statutory obligations with regard to the sharing of information.
- 2.4 To set out the responsibilities of NIAS staff with regard to information sharing.
- 2.5 To ensure that flows of personal confidential data (PCD) are underpinned by a legal basis

## **3. Scope**

- 3.1 This policy covers all types of information within NIAS including:
  - Patient information

- Staff information
  - Organisational information
  - Statistical information
- 3.2 Information sharing is covered in the Information Governance (IG) agenda, responsibility for which is contained within the remit of the Head of IG and Data Protection Officer (DPO) and overseen by the Director of Strategy and Transformation. However, complying with the requirements of this policy is an organisation wide responsibility.
- 3.3 This policy applies to all NIAS employees, including permanent, temporary, voluntary and contract staff, who come into contact with personal and non-personal information.

#### 4. Definitions

- 4.1 **Information Sharing:** The disclosure of information from one organisation to another third-party organisation, or the sharing of information between different parts of an organisation.
- 4.2 **Systematic Information Sharing:** routine sharing of data sets between organisations for an agreed purpose
- 4.3 **Ad hoc or 'one off' Information Sharing:** Sharing of information not covered by an information sharing agreement.
- 4.4 **Information Governance:** Provides assurance that information, both personal and non-personal, is processed and managed in accordance with relevant guidance and legislation.
- 4.5 **Freedom of Information Act 2000:** Provides the legal basis for responding to requests for non-personal information held by Public Authorities.
- 4.6 **Data Protection Legislation:** Legislation including, but not limited to, the General Data Protection Regulation (GDPR) 2016 and Data Protection Act 2018, which provides the legal basis for the processing of and access to personal information of living individuals.

- 4.7 **Data Security and Protection Toolkit:** Provides assurance at a national level that NIAS is complying with pre-set requirements (further detail in section 9.0)
- 4.8 **Human Rights Act 1998:** Provides the legal basis for ensuring specified human rights are respected.
- 4.9 **Consent:** ‘Any freely given specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.’ (GDPR)
- 4.10 **Data Protection Impact Assessment:** A process to help you identify and minimise the data protection risks of a project.

## 5. Responsibilities

- 5.1 The **Chief Executive Officer** is the NIAS Accounting Officer and has overall accountability and responsibility for IG.
- 5.2 The **Senior Information Risk Owner (SIRO)** will oversee the development of the Information Risk Policy and Strategy and take ownership of the risk assessment process for information risk.
- 5.3 The **Caldicott Guardian** will act as the ‘guardian’ of patient identifiable information and will oversee the use and sharing of patient information.
- 5.4 The **Head of Information Governance and Data Protection Officer** will manage the day to day IG agenda, including information sharing and provide assurance to the Board on compliance with the Data Security and Protection Toolkit (DSPT).
- 5.5 The mandatory role of **Data Protection Officer** will ensure NIAS can demonstrate its compliance with Data Protection legislation
- 5.6 The **Information Governance and Compliance Manager** will manage requests for information, both personal and non-personal, and provide assurance to the Head of IG and DPO that legislation is being complied with.
- 5.7 **Information Asset Owners (IAO)** are directly accountable to the SIRO and will provide assurance, via the self-assessment

checklist, that information risk is being managed for their assigned information assets, including ensuring information sharing is appropriate. Assurance will be given at the IG Group.

- 5.8 **Information Asset Administrators (IAA)** will assist the IAOs and have day to day responsibility for the management of information risks for their assigned information asset, including ensuring information sharing is appropriate.
- 5.9 **All staff** have a responsibility to comply with legislation and guidance relating to information sharing and identify and report any risks, non-compliance or areas of concern.

## **6. The Information Commissioner's Data Sharing Code of Practice (May 2011)**

- 6.1 The code was developed by the Information Commissioner and explains how Data Protection legislation applies to the sharing of personal data. It also provides good practice advice to assist organisations when considering sharing information.
- 6.2 The Information Commissioner published the code under section 52 of the Data Protection Act 1998, however, its application and principles still apply to current Data Protection legislation.

## **7. Data Sharing and the Law**

- 7.1 Before sharing any personal data, it is important to consider all the legal implications, and to identify and document the legal basis for doing so. As well as the requirements of the Data Protection legislation, there may be other considerations to take account of, e.g. copyright restrictions or a duty of confidentiality.
- 7.2 The Human Rights Act 1998, Article 8, gives everyone the right to respect for his private and family life, his home and correspondence. This has particular relevance to the sharing of personal data.

## **8. Factors to Consider before Sharing**

- 8.1 There are several factors to consider before entering into any information sharing in order to assess the objective and any



potential benefits or risks of deciding to share the information or not:

- What is the sharing meant to achieve?
- What information **needs** to be shared?
- Who requires access to the shared personal information?
- How will the information be shared?
- What is the legal basis for sharing? (if PCD)
- What, if any, risks does sharing the information pose?
- Could the objective be achieved without sharing personal information?
- Will any of the information being shared be transferred to an area without adequate Data Protection legislation?

8.2 Consideration should be given to whether a Data Protection Impact Assessment (DPIA) is required. This would need to be completed if the sharing is likely to result in a high risk to individuals. Further guidance can be found in the Information Commissioner's guidance and in the NIAS Data Protection Impact Assessment Policy and Procedure

8.3 Before sharing information, refer to the checklists found in Appendix 2 (Systematic Data Sharing) and Appendix 3 (one off requests).

8.4 A data sharing flow chart can be found in Appendix 4

## **9. Information Sharing for Direct Care**

9.1 The Information Governance Review 2013 (aka Caldicott 2) identified an additional principle: 'The duty to share information can be as important as the duty to protect patient confidentiality'

## **10. Consent**

10.1 Consent is one of the conditions for processing within the Data Protection legislation which allows for the legitimate sharing of personal information. Whilst consent will provide a basis for sharing information, it is recognised that this is not always achievable or desirable. There are a number of other conditions for processing that should be looked at before opting for consent. Reference should be made to the Data Protection Policy.

10.2 Due to the following considerations, relying on consent as the legal basis for processing can prove difficult.

- Consent means offering individuals real choice and control
- Consent requires a positive and recorded opt-in
- Explicit consent requires a very clear statement as to what the individual is consenting to and who their information may be shared with
- Consent should be made easy to withdraw

## **11. Fair Processing Notices**

11.1 Data Protection legislation requires that individuals are informed of the reasons why their personal information may be processed. Specifically, it says that the information you provide to people about how you process their personal data must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge

11.2 Fair Processing Notices (FPNs) must contain information including details about what information is processed, for what purpose and who it may be shared with. Please refer to the Data Protection Policy for a comprehensive list of requirements.

11.3 Whenever possible, individuals should be informed about how their information could be shared at the point it is collected. It is accepted that it not feasible to provide this information to emergency patients. However, FPNs should be made available to the public via the website and other means considered suitable.

## **12. Security**

12.1 GDPR Article 5 1(f) states: *'personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using*

*appropriate technical or organisational measures ('integrity and confidentiality').'*

12.2 In order to support good practice, the following measures should be taken in respect of information being shared with others and information others are sharing with NIAS:

- Review what information is being shared with other organisations to ensure that there is an appropriate sharing agreement or a statutory obligation in place.
- Regular information mapping exercises will be conducted to establish information flows both to and from NIAS and to show the legal basis for any flows involving PCD. IAOs will be involved in this process.
- 'Need to know' principles need to apply – as per Caldicott2 – to ensure only those requiring legitimate access are given this. Access controls should be in place for all information assets.
- Abide by the Safe Haven Policy and Information Disclosure and Transfer Policy when deciding on a method of disclosure.

### **13. Data Sharing Agreements**

13.1 Data sharing agreements (DSAs) should include details of the following:

- The purpose(s) of the sharing
- The legal basis for sharing
- The potential recipients of the information
- The data to be shared
- Data quality
- Data security
- Method of sharing
- Retention period of the shared information
- Individuals rights – in particular subject access requests
- Termination of the agreement
- Sanctions for failure to comply

13.2 Information sharing agreements will be monitored and reviewed annually by the Head of IG and DPO.

## **14. Right of Access by the Data Subject**

- 14.1 Individuals have the right of access to their personal information held by an organisation. This right can also be used by a third party if they are acting on behalf of the individual (with their written consent or a legal power of attorney) or if they are the parent or legal guardian of a minor.
- 14.2 Further guidance on Subject Access Requests can be found in the Data Protection Rights Policy and Procedure.

## **15. Specific Information Sharing**

- 15.1 The following are a number of specific situations whereby personal information may be shared in accordance with Data Protection legislation:
- Right of Access by the Data Subject – see section 14.0
  - Requests from the Police – allowed under the crime and taxation exemption in the Data Protection legislation. Requests must be made on the official police Data Protection form and signed by a senior officer.
  - Requests from Solicitors (non-claims) – allowed if the subject of the information has provided written consent
  - Requests from Solicitors (claims) – are allowed under Article 6 of the GDPR as follows:  
*(c) Legal obligation: processing is necessary for you to comply with the law.*
  - Information can be shared if there is a suspected child safeguarding issue – allowed under the Children Act 2004
  - Information can be shared if there is a suspected risk to someone's life as follows:  
*(d) Vital interests: the processing is necessary to protect someone's life*

There is other legislation that allows for the sharing of PCD. Examples can be found in Appendix 5. The Head of IG and DPO should be consulted if unsure as to whether to share or not.

## **16. Issues to Avoid**

16.1 The following practices must be avoided as they could lead to regulatory action being taken (see section 17.0):

- Not informing individuals you intend to share their personal data as you think they may object.
- Sharing information that is excessive or not relevant to the purpose for which the information is being shared.
- Sharing personal information when there is no need to do so e.g. when anonymised statistical information is sufficient.
- Not taking reasonable steps to ensure that the information is accurate before it is shared.
- Using an incompatible method of sharing the information, possibly resulting in a loss or degradation of the information
- Having inappropriate or inadequate security measures in place.

## **17. Information Commissioner's Powers and Penalties**

17.1 The Information Commissioner (ICO) has several powers and penalties it can impose on organisations who do not comply with Data Protection legislation:

- Information Notice: this requires the organisation to provide the ICO with specific information within a specified period of time
- Audits: The ICO can conduct unannounced audits
- Enforcement Notice: This compels an organisation to take the action specified in the notice to bring about compliance with Data Protection. Failure to comply with an Enforcement Notice can be a criminal offence.
- Monetary Penalty Notice: The ICO has the power to impose a monetary penalty of a maximum of either €10,000,000 (2% of annual turnover) or €20,000,000 (4% of annual turnover) dependent on the level of non-compliance / breach. Details of the infringements can be found in the Data Protection Policy

## **18. Caldicott Function**

18.1 The Caldicott function is overseen by the Caldicott Guardian. The Caldicott Guardian for NIAS is the Medical Director.

18.2 The key responsibilities of the Caldicott function are to:

- Support the Caldicott Guardian
- Ensure the confidentiality and Data Protection work programmes are implemented and monitored
- Ensure that staff are aware of their responsibilities through policy, procedure and training
- Provide routine reports to the Information Assurance Group on confidentiality and Data Protection issues or areas of concern

## **19. Training**

19.1 IG is included in the NIAS induction programme. Training can also be requested at the discretion of a manager, or by an individual wanting personal development.

19.2 In addition, IG training is included within the essential education mandatory training programme which all staff are required to undergo on an annual basis. The training is provided via the national training tool available on the HSC Digital hub. In addition, a hardcopy workbook is available for staff with limited access to the online material. Completion of this training is monitored by the Head of IG and DPO.

19.3 Further guidance and information relating to IG issues will be distributed periodically via various media including NIAS newsletters.

## **20. Consultation**

20.1 This policy has been presented to the IG Group for consultation. The Group has delegated authority to approve this document.

## **21. References**

Information Commissioner's Office Data Sharing Code of Practice (2011) available from:

[http://www.ico.org.uk/for\\_organisations/data\\_protection/topic\\_guides/data\\_sharing](http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing)

Information Commissioner's Guide to Data Protection Impact Assessments:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/>

## **22. Monitoring Compliance and Effectiveness of this Policy**

- 22.1 The Head of IG and DPO will monitor the implementation of this policy, including the minimum requirements for the DSP Toolkit, and take an assurance report to the IG Group. This report will be sent on an annual basis. However, if the on-going monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the group sooner.

## Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Information Sharing Policy</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead:</b>	<b>Tracy Avery, Head of IG and Data Protection Officer, Tracy.Avery@nias.hscni.net</b>
<b>Previous document already being used?</b>	<b>No</b>	<b>Print name, title and contact details</b>	
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Who does the document need to be disseminated to?</b>	Staff have a responsibility to ensure that any requests to share information are handled in accordance with the relevant legislation.		
<b>Proposed methods of dissemination:</b>  <b>Including who will disseminate and when</b>  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> </ul>		<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>	



<ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<b>Summary for inclusion on the Class Publishing Applications system</b>	<p>The Information Sharing Policy provides staff with the detail and guidance required on how to handle requests to share information in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

## **Data Sharing Checklist – Systematic Data Sharing**

Scenario: You want to enter into an agreement to share personal data on an on-going basis

### **Is the sharing justified?**

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?
- Is there a legal basis to share?
- Is a Data Protection Impact Assessment required?

### **Do you have the power to share?**

Key points to consider:

- The type of organisation you work for
- Any relevant functions or powers of your organisation
- The nature of the information you have been asked to share (for example was it given in confidence?)
- Any legal obligations to share information (for example a statutory requirement or a court order)

### **If you decide to share**

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared
- The organisations that will be involved
- What you need to tell people about the data sharing and how you will communicate that information
- Measures to ensure adequate security is in place to protect the data
- What arrangements need to be in place to provide individuals with access to their personal data if they request it
- Agreed common retention periods for the data
- Processes to ensure secure deletion takes place



## **Data Sharing Checklist – one off requests**

Scenario: You are asked to share personal data relating to an individual or 'one off' circumstances

### **Is the sharing justified?**

Key points to consider:

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the Data Protection legislation to share?
- Is there a legal basis to share?
- Has consent been obtained?
- Has a DPIA been completed and approved if required

### **Do you have the power to share?**

Key points to consider:

- The type of organisation you work for
- Any relevant functions or powers of your organisation
- The nature of the information you have been asked to share (for example was it given in confidence?)
- Any legal obligation to share information (for example a statutory requirement or a court order)

### **If you decide to share**

Key points to consider:

- What information do you need to share?
  - Only share what is necessary
  - Distinguish fact from opinion
- How should the information be shared?
  - Information must be shared securely
  - Ensure you are giving information to the right person
- Consider whether it is appropriate /safe to inform the individual that you have shared their information

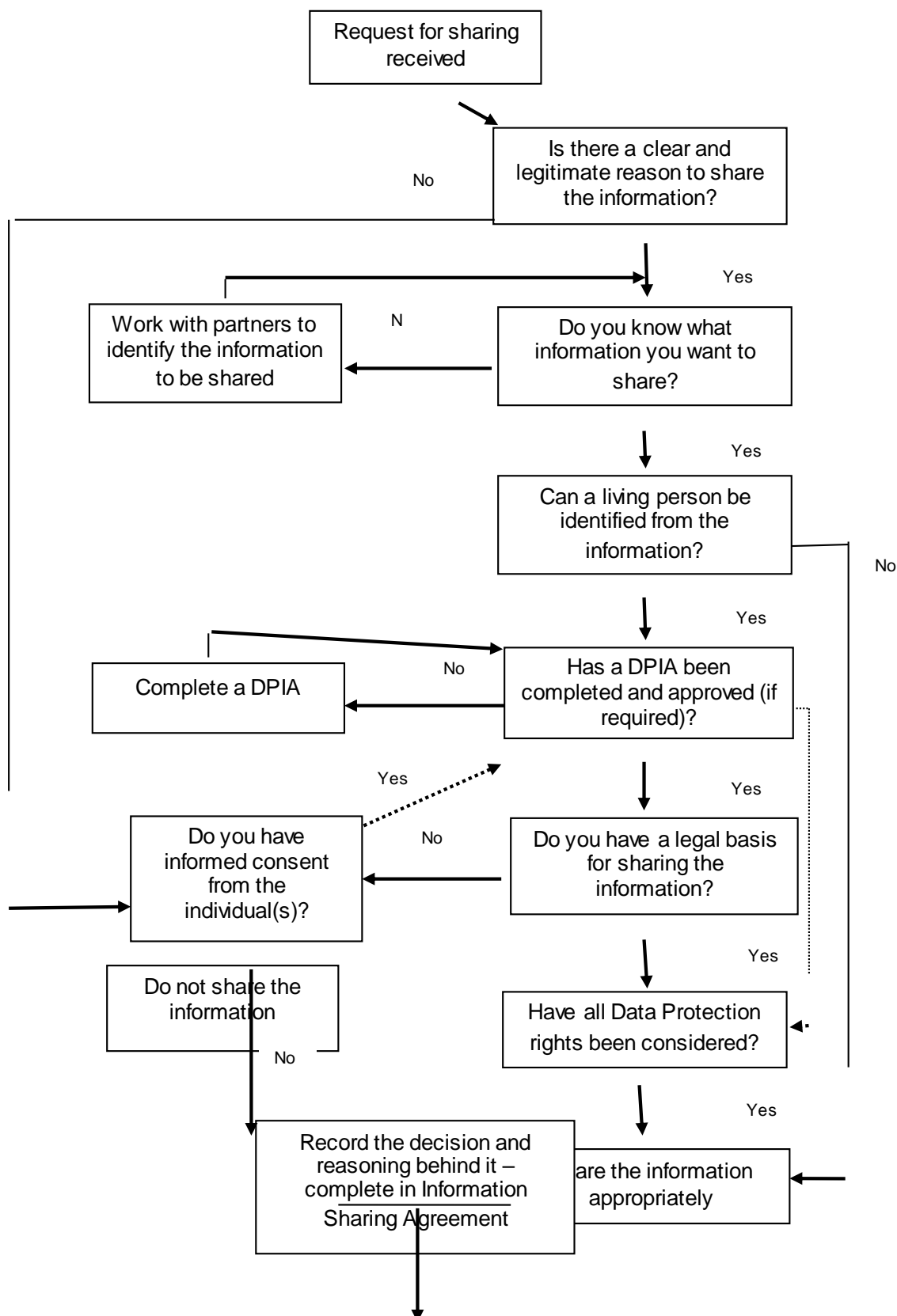
### **Record your decision**

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose
- Who it was shared with
- When it was shared
- Your justification for sharing
- Whether the information was shared with or without consent

## Information Sharing Flow Chart – deciding the legal basis





**Examples of legislation supporting sharing of PCD**

- The Children Act 2004
- Education Act 2002
- Learning and Skills Act 2000
- Education (SEN) Regulations 2001
- Children Leaving Care Act 2000
- Mental Capacity Act 2005
- Mental Capacity Act 2005 – Code of Practice
- Immigration and Asylum Act 1999
- Local Government Act 2000
- Criminal Justice Act 2003
- Crime and Disorder Act 1998
- The Police and Justice Act 2006 and the Crime and Disorder (Overview and Scrutiny) Regulations 2009
- Criminal Justice and Court Service Act 2000
- National Health Service Act 2006
- The Adoption and Children Act 2002
- Localism Act 2011
- Welfare Reform Act 2012
- The Care Act 2015
- Health and Social Care, Safety and Quality, Act 2015

NB – this list is not exhaustive





## RETENTION AND DISPOSAL OF INFORMATION SCHEDULE

### Links

The following documents are closely associated with this document:

- Records Management Code of Practice for Health and Social Care (2016)
- Information Lifecycle Management Policy
- Data Protection Act 2018
- General Data Protection Regulation (2016/679)
- Freedom of Information Act 2000
- Personal File Management Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Records Management Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	

<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version can be found on the Trust's Intranet site.
------------------------	---

Version	Date Approved	Publication Date	Approved By	Summary of Changes
1.0				Retention and Disposal of Information Schedule rewritten in corporate format.

## Contents

1. Introduction.....	4
2. Objectives.....	4
3. Scope.....	5
4. Definitions.....	5
4.1 Data Protection Legislation .....	5
5. Responsibilities.....	5
5.1 Chief Executive Officer.....	5
5.2 Senior Information Risk Owner (SIRO) .....	5
5.3 Caldicott Guardian .....	5
5.4 Head of Information Governance .....	6
5.5 Data Protection Officer (DPO) .....	6
6. Schedule .....	6
7. Consultation.....	6
8. References .....	7
9. Monitoring Compliance and Effectiveness of the Policy.....	7
Plan for Dissemination of Procedural Document .....	8

## 1. Introduction

- 1.1 Records are a valuable resource because of the information contained within them. An effective records management system ensures that information is available:
- to support patient care
  - to support the day to day business which underpins delivery of patient care
  - to support sound administrative and managerial decision making
  - to meet legal requirements, including access to information as laid down in Government legislation
  - to assist clinical and financial audits
  - to ensure external compliance with awarding bodies
- 1.2 NIAS operates an Information Lifecycle Management Policy, which advises how information should be processed and managed.
- 1.3 The destruction of records is an irreversible act that must not be taken lightly. However, UK General Data Protection Regulation (UK GDPR) states:
- ‘Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed’*
- 1.4 This schedule sets out the **minimum** retention periods as approved by the National Archives and as listed in Records Management Code of Practice for Health and Social Care 2016.
- 1.5 All HSC bodies have a statutory duty to plan for the safekeeping and eventual disposal of their records.
- 1.6 This schedule should be read in conjunction with the Information Lifecycle Management Policy

## 2. Objectives

- 2.1 The key objectives of this policy are:

- to ensure that all staff are aware of the importance of effective records management, including their final destruction / disposal
- to ensure the legal obligations of the Data Protection legislation, the Freedom of Information Act 2000 and other relevant Acts of Parliament are adhered to regarding the retention and disposal of records
- to provide a consistent approach to the way records are retained and disposed of

### **3. Scope**

- 3.1 This policy applies to all NIAS employees including permanent, temporary, voluntary and contract staff, who access personal and non-personal information.

### **4. Definitions**

#### **4.1 Data Protection Legislation**

- 4.2.1 Legislation including, but not limited to, the General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 (DPA).

### **5. Responsibilities**

#### **5.1 Chief Executive Officer**

- 5.1.1 The Chief Executive Officer is the Accounting Officer of NIAS and has overall accountability and responsibility for IG.

#### **5.2 Senior Information Risk Owner (SIRO)**

- 5.2.1 The Senior Information Risk Owner (SIRO) will take ownership of the risk assessment process for information risk. This role is within the remit of the Director of Strategy and Transformation.

#### **5.3 Caldicott Guardian**

- 5.3.1 The Caldicott Guardian will act as the 'guardian' of patient identifiable information and will oversee the use and sharing

of patient information. This role is within the remit of the Medical Director.

## **5.4 Head of Information Governance**

- 5.4.1 The Head of Information Governance will manage the day-to-day IG agenda and provide assurance to the Board on compliance.

## **5.5 Data Protection Officer (DPO)**

- 5.5.1 The Data Protection Officer will ensure NIAS can demonstrate its compliance with Data Protection legislation. This role is included in the remit of the Head of IG

## **6. Schedule**

- 6.1 The minimum retention periods should be calculated from the beginning of the year after the last date on the record
- 6.2 The provisions of the Data Protection legislation must be complied with
- 6.3 Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Local business requirements/instructions must be considered before activating retention periods as detailed in Appendix 2.
- 6.4 It is a legal requirement that HSC records which have been selected, as archives should be held in a repository that has been approved for the purpose by the National Archives. The document 'Records Management Code of Practice for Health and Social Care 2016 contains details on these recommended repositories.
- 6.5 Schedule – see Appendix 2

## **7. Consultation**

- 7.1 This policy will be presented to the Information Governance Group for consultation. The Group has delegated authority to approve this document.

## **8. References**

- Records Management Code of Practice for Health and Social Care 2016. Available from:  
<https://digital.HSC.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>

## **9. Monitoring Compliance and Effectiveness of the Policy**

- 9.1 The Head of IG will monitor the implementation of this policy, including the minimum requirements for the DSPT, and take an assurance report to the IG Group. This report will be sent on an annual basis. However, if the ongoing monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the Group sooner.



## Plan for Dissemination of Procedural Document

<b>Title of document:</b>	<b>Retention and Disposal of Information Schedule</b>		
<b>Version Number:</b>	<b>1.0</b>	<b>Dissemination lead: Print name, title and contact details</b>	<b>Tracy Avery, Head of IG and Data Protection Officer, tracy.avery@ni.as.hscni.net</b>
<b>Previous document already being used?</b>	<b>Yes</b>		
<b>Reading Categories</b>  <i>List which document users fall within each category</i>	<b>Essential Reading</b>	All staff	
	<b>Awareness for Reference Purposes</b>	All staff	
	<b>Awareness to inform staff / other stakeholders</b>	All staff	
<b>Whom does the document need to be disseminated to?</b>	All staff may be required to dispose of information therefore; all need to be aware of the correct procedure to follow.		
<b>Proposed methods of dissemination: Including who will disseminate and when</b>  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"> <li>• <i>Information cascade by managers</i></li> <li>• <i>Communication via Management/ Departmental/Team meetings</i></li> </ul>		<ul style="list-style-type: none"> <li>• Information cascade by managers</li> <li>• Notification via articles in bulletins</li> <li>• Posting on the intranet</li> </ul>	

<ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<b>Summary for inclusion on the Class Publishing Applications system</b>	The Retention and Disposal of Information Schedule provides staff with the detail and guidance required on how and when to retain and / or dispose of information to ensure that legal obligations are adhered to.

*Note: Following approval of procedural documents, it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

Record Type	Retention Start	Retention Period	Action at end of Retention Period	Notes
<i>Care records with standard retention periods</i>				
Adult health records not covered by any other section in this schedule	Discharge or patient last seen	8 years	Review, and if no longer needed, destroy	Basic health and social care retention period – check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions. This includes medical illustration records such as x-rays and scans as well as video and other formats
Electronic Patient Records System	See notes	See notes	Destroy	Where the electronic system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain demonstrating that a record has been destroyed, then the code should be followed in the same way for electronic records as for paper records with a log being kept of the records destroyed. If the system does not have the capacity, then once the records have reached the end of their retention periods, they should be inaccessible to users of the system and upon decommissioning, the system (along with audit trails) should be retained for the retention period of the last entry related to the schedule.
<i>Pharmacy</i>				
Information relating to controlled drugs	Creation	See notes	Review and if no longer needed, destroy	HSC England and HSC BSA guidance for controlled drugs can be found at: <a href="http://www.HSCba.HSC.uk/PrescriptionServices/1120.aspx">http://www.HSCba.HSC.uk/PrescriptionServices/1120.aspx</a> and <a href="https://www.england.HSC.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf">https://www.england.HSC.uk/wp-content/uploads/2013/11/som-cont-drugs.pdf</a> The Medicines, Ethics and Practice (MEP) guidance can be found at the link (subscription required) <a href="http://www.rpharms.com/support/mep.asp#new">http://www.rpharms.com/support/mep.asp#new</a> Guidance from HSC England is that locally held controlled drugs information should be retained for 7 years.

				HSC BSA will hold primary data for 20 years and then review. HSC East and South East Specialist Pharmacy Services have prepared pharmacy records guidance including a specialised retention schedule for pharmacy. Please see: <a href="http://www.medicinesresources.HSC.uk/en/Communities/HSC/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/">http://www.medicinesresources.HSC.uk/en/Communities/HSC/SPS-E-and-SE-England/Reports-Bulletins/Retention-of-pharmacy-records/</a>
<i>Event and Transaction Records</i>				
Clinical Audit	Creation	5 years	Review and if no longer needed, destroy	
Chaplaincy Records	Creation	2 years	Review and consider transfer to a place of deposit	<i>See also Corporate Retention</i>
Clinical Protocols	Creation	25 years	Review and consider transfer to a place of deposit	Clinical protocols may have archival value. They may also be routinely captured in clinical governance meetings, which may form part of the permanent record (see Corporate Records).
Equipment Maintenance Logs	Decommissioning of the equipment	11 years	Review and consider transfer to a place of deposit	

Inspection of Equipment Records	Decommissioning of equipment	11 years	Review and if no longer needed, destroy	
<i>Telephony Systems &amp; Services (999 phone numbers, 111 phone numbers, ambulance, out of hours, single point of contact centres)</i>				
Recorded conversation which may later be needed for clinical negligence purpose	Creation	3 years	Review and if no longer needed, destroy	The period of time cited by the HSC Litigation Authority is 3 years
Recorded conversation which forms part of the health record	Creation	Store as a health record	Review and if no longer needed, destroy	It is advisable to transfer any relevant information into the main record through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record the recording must be considered as part of the record and retained accordingly
The telephony systems record (not recorded conversations)	Creation	1 year	Review and if no longer needed, destroy	This is the absolute minimum specified to meet the HSC contractual requirement
<i>Clinical Trials &amp; Research</i>				
Research data sets	End of research	Not more than 20 years	Review and consider transfer to place of deposit	<a href="http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf">http://tools.jiscinfonet.ac.uk/downloads/bcs-rrs/managing-research-records.pdf</a>

Research Ethics Committee's documentation for research proposal	End of research	5 years	Review and consider transfer to place of deposit	<p>Or details please see: <a href="http://www.htra.HSC.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/">http://www.htra.HSC.uk/resources/research-legislation-and-governance/governance-arrangements-for-research-ethics-committees/</a></p> <p>Data must be held for sufficient time to allow any questions about the research to be answered. Depending on the type of research, the data may not need to be kept once the purpose has expired. For example, data used for passing an academic exam may be destroyed once the exam has been passed and there is no further academic need to hold the data. For research that is more significant a place of deposit may be interested in holding the research. It is best practice to consider this at the outset of research and orphaned personal data can inadvertently cause a data breach</p>
Research Ethics Committee's minutes and papers	Year to which they relate	Before 20 years	Review and consider transfer to place of deposit	
<i>Corporate Governance</i>				
Board meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a place of deposit	
Board meetings (closed boards)	Creation	May retain for 20 years	Transfer to a place of deposit	Although they may contain confidential or sensitive material, they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.

Chief Executive records	Creation	May retain for 20 years	Transfer to a place of deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest
Committees listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a place of deposit	
Committees / Groups / Sub committees not listed in the Scheme of Delegation	Creation	6 years	Review and if no longer needed, destroy	Includes minor meetings/projects and departmental business meetings
Destruction certificates or Electronic metadata destruction stub or record of information held on destroyed physical media	Destruction of record or information	20 years	Consider transfer to place of deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument they must either be transferred to a place of deposit as a public record or destroyed 20 years after the record has been closed.
Incidents (serious)	Date of incident	20 years	Review and consider transfer to a place of deposit	

Incidents (not serious)	Date of incident	10 years	Review and if no longer needed, destroy	
Non-clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed, destroy	
Patient Advice and Liaison Service (PALS) Records	Close of financial year	10 years	Review and if no longer needed, destroy	
Policies, strategies and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to place of deposit	
<i>Communications</i>				
Intranet site	Creation	6 years	Review and consider transfer to a place of deposit	
Patient information leaflets	End of use	6 years	Review and consider transfer to	



			a place of deposit	
Press releases and important internal communications	Release date	6 years	Review and consider transfer to a place of deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Public consultations	End of consultation	5 years	Review and consider transfer to a place of deposit	
Website	Creation	6 years	Review and consider transfer to a place of deposit	
<i>Staff Records &amp; Occupational Health</i>				
Duty roster	Close of financial year	6 years	Review and if no longer needed, destroy	
Exposure monitoring information	Monitoring ceases	40 years / 5 years from the date of the last entry made in it	Review and if no longer needed, destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years

Occupational Health records	Staff member leaves	Keep until 75 <sup>th</sup> birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed, destroy	
Occupational Health report of staff member under health surveillance	Staff member leaves	Keep until 75 <sup>th</sup> birthday	Review and if no longer needed, destroy	
Occupational Health report of staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75 <sup>th</sup> birthday, whichever is longer	Review and if no longer needed, destroy	
Staff Record	Staff member leaves	Keep until 75 <sup>th</sup> birthday (see notes)	Create staff summary then review or destroy the main file	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75 <sup>th</sup> birthday, whichever is sooner, if a summary has been made

Staff Record summary	6 years after the staff member leaves	75 <sup>th</sup> birthday	Place of deposit should be offered for continued retention or destroy	Please see Appendix 3 for an example of a Staff Record summary used by an organisation
Timesheets (original) record)	Creation	2 years	Review and if no longer needed, destroy	
Staff Training Records	Creation	See notes	Review and consider transfer to a place of deposit	Records of significant training must be kept until 75 <sup>th</sup> birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 - Clinical training records – to be retained until 75 <sup>th</sup> birthday or 6 years after the staff member leaves, whichever is the longer, 2 - statutory and mandatory training records – to be kept for 10 years after training completed, 3 - Other training records – keep for 6 years after training completed
<i>Procurement</i>				
Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed, destroy	
Contracts – financial approval files	End of contract	15 years	Review and if no longer needed, destroy	

Contracts – financial approved suppliers documentation	When supplier finishes work	11 years	Review and if no longer needed, destroy	
Tenders (successful)	End of contract	6 years	Review and if no longer needed, destroy	
Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed, destroy	
<i>Estates</i>				
Building plans and records of major building works	Completion of work	Lifetime of the building or disposal of asset plus 6 years	Review and consider transfer to a place of deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit
CCTV		See ICO Code of Practice	Review and if no longer needed, destroy	ICO code of practice: <a href="https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf">https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf</a> The length of retention must be determined by the purpose for which the CCTV has been deployed. The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated
Equipment monitoring and testing and maintenance	Completion of monitoring or test	40 years	Review and if no longer	

work where asbestos is a factor			needed, destroy	
Equipment monitoring and testing and maintenance work	Completion of monitoring or test	10 years	Review and if no longer needed, destroy	
Inspection reports	End of lifetime of installation	Lifetime of installation	Review	
Leases	Termination of lease	12 years	Review and if no longer needed, destroy	
Minor building works	Completion of work	Retain for 6 years	Review and if no longer needed, destroy	
Photographic collections of service locations and events and activities	Close of collection	Retain for not more than 20 years	Consider transfer to a place of deposit	The main reason for maintaining photographic collections is for historical legacy of the running and operation of an organisation. However, photographs may have subsidiary uses for legal enquiries.
Surveys	End of lifetime of installation or building	Lifetime of installation or building	Review and consider transfer to place of deposit	

<i>Finance</i>				
Accounts	Close of financial year	3 years	Review and if no longer needed, destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Benefactions	End of financial year	8 years	Review and consider transfer to place of deposit	These may already be in the financial accounts and may be captured in other records / reports or committee papers. Where benefactions endowment trust fund / legacies – permanent retention
Debtor records cleared	Close of financial year	2 years	Review and if no longer needed, destroy	
Debtors records not cleared	Close of financial year	6 years	Review and if no longer needed, destroy	
Donations	Close of financial year	6 years	Review and if no longer needed, destroy	
Expenses	Close of financial year	6 years	Review and if no longer needed, destroy	

Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible
Financial records of transactions	End of financial year	6 years	Review and if no longer needed, destroy	
Petty cash	End of financial year	2 years	Review and if no longer needed, destroy	
Private Finance Initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to place of deposit	
Salaries paid to staff	Close of financial year	10 years	Review and if no longer needed, destroy	
Superannuation records	Close of financial year	10 years	Review and if no longer	

			needed, destroy	
<i>Legal, Complaints &amp; Information Rights</i>				
Complaints case file	Closure of incident (see notes)	10 years	Review and if no longer needed, destroy	<a href="http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf">http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf</a> The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Fraud case file	Case closure	6 years	Review and if no longer needed, destroy	
Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed, destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions
FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed, destroy	
Industrial relations including tribunal case records	Close of financial year	10 years	Review and consider transfer to a place of deposit	Some organisations may record these as part of the staff record but in most cases they will form a distinct separate record either held by the staff member / manager or by the payroll team for processing



Litigation records	Closure of case	10 years	Review and consider transfer to place of deposit	
Patents / trademarks / copyright / intellectual property	End of lifetime of patent or termination of licence / action	Lifetime of patent or 6 years from end of licence / action	Review and consider transfer to place of deposit	
Software licences	End of lifetime of licence	Lifetime of software	Review and if no longer needed, destroy	
Subject Access Requests (SAR) and disclosure correspondence	Closure of SAR	3 years	Review and if no longer needed, destroy	
SARs where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed, destroy	

**Staff record summary**

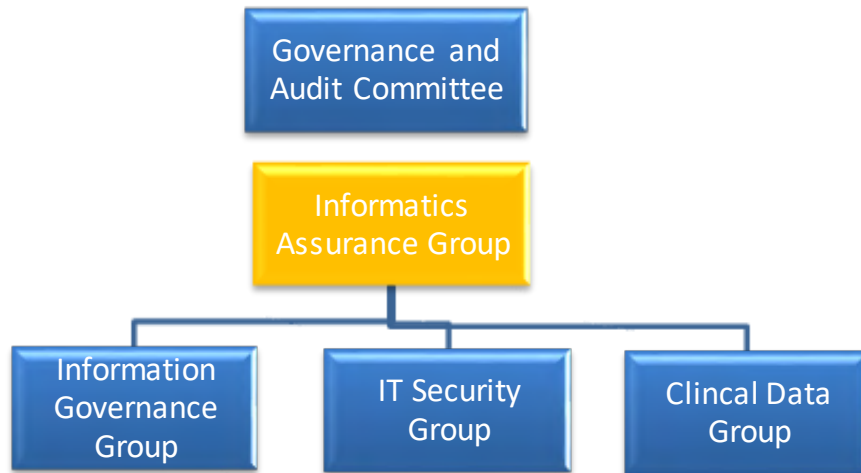
Where a summary of a staff record is made, it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work-related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- Professional training history and professional qualifications related to the delivery of care
- List of buildings where the member of staff worked and the dates worked in each location

Example of good practice for a staff summary record:

- Name
- Previous names
- Assignment number
- Pay bands
- Date of birth
- Addresses
- Positions held
- Start and end dates
- Reason for leaving
- Building or sites worked at




Terms of Reference	
<b>Title:</b>	Informatics Assurance Group
<b>Date Approved:</b>	
<b>Next review:</b>	
<b>Reporting to:</b>	The Governance and Audit Committee (Trust Committee)
<b>Accountability:</b>	 <pre> graph TD     GAC[Governance and Audit Committee] --&gt; IAG[Informatics Assurance Group]     IAG --&gt; IGG[Information Governance Group]     IAG --&gt; ITSG[IT Security Group]     IAG --&gt; CDG[Clinical Data Group] </pre>
<b>Purpose:</b>	<p>The IAG (Informatics Assurance Group) is a delegated authority group accountable to the Governance and Audit Committee.</p> <p>Its purpose is to support and drive the Trust wide informatics assurance agenda, and provide the Trust Board with the assurance that effective policies and processes are in place within NIAS in relation to the following discreet specialisms:</p> <ul style="list-style-type: none"> <li>• Data Quality and compliance.</li> <li>• Information Governance, including data protection, records management, Freedom of Information and UK GDPR.</li> <li>• Information security, including cyber security.</li> <li>• Information Management and Technology.</li> </ul> <p>It will consider and approve proposed changes to the technical controls in place to appropriately secure and manage the Trust's information Assets, the processing of data via those assets, and review compliance with national and local requirements relevant to the digital agenda and reporting requirements.</p> <p>It will also determine appropriate actions in respect of the Trusts strategic approach to informatics assurance as outlined in the 'Caring</p>

	<p>today, planning for tomorrow' NIAS transformation strategy 2020-2026. In particular the digital enablers as defined within the strategy.</p> <p>Manage all risks associated with Information Assets on behalf of NIAS. Proactively seek to develop and implement cultural awareness if <i>Information Governance</i> issues within the Trust.</p> <p>Three sub-groups; the Information Governance Group (IGG), Clinical Data Group (CDG) and the Information Technology Security Group (ITSG) will support the IAG. The purpose of these groups is to deal with the detail of each specialism, allowing the IAG to remain strategically focused.</p>
<b>Membership</b>	<p>Director of Planning, Performance &amp; Corporate Services, SIRO, Chair Head of Informatics, Chair of IGG, Deputy Chair of IAG Assistant Director of IT, Chair of ITSG Assistant Clinical Director (Paramedicine) Medical director – Caldicot Guardian Assistant Director Operations (Control Rooms) Assistant Director Operations (Areas) Emergency Planning Manager Risk Manager Assistant Director HR</p>
<b>Deputies</b>	<p>Attendance at meetings is mandatory by a member or nominated deputy.</p> <p>Deputies should only attend in exceptional circumstances. Deputies should have a full understanding of the group's terms of reference and papers being presented. Deputies shall be expected to make decisions in accordance with the terms of reference as may be appropriate</p>
<b>Authority</b>	<p>The IAG is authorised to:</p> <ul style="list-style-type: none"> <li>• Ratify policy, procedure and supporting strategies and action plans in the area of information management, data quality, information governance and information security and make recommendations to Governance and Assurance Committee for agreement / approval where required.</li> <li>• Report compliance in relation to information governance, information security and data quality to the Governance and Audit Committee.</li> <li>• Review learning outcomes from specific Informatics assurance related incidents requiring investigation and to ensure the implementation of any necessary remedial actions.</li> <li>• Provide assurance regarding information security matters that may affect NIAS; note that any matters having an implication for National Security or that relate to the CNI (Critical National Infrastructure) may take place in a closed session for the purposes of confidentiality.</li> </ul>

	<p>While the group will be updated accordingly, they will not be subject to full disclosure.</p> <ul style="list-style-type: none"> <li>• Ensure that annual returns are identified and submitted within the agreed timeframes.</li> <li>• In association with HSCNI, review controls utilised in England and implement best practice. i.e., DPST (Data Protection &amp; security Toolkit).</li> <li>• Receive assurance from the IGG regarding compliance in terms of data quality, FOI, UK GDPR, and aligned information management issues. Via the IGG, approve any changes to the reporting and recording of data, and ensure compliance with national and local requirements for data recording.</li> <li>• Receive assurance from the ITSG Group regarding compliance in terms of all IT and cyber security matters. This includes current threat assessment, security controls (firewalls etc), patch levels.</li> <li>• Receive assurance from the CDG Group regarding compliance in terms of terms of data quality, FOI, UK GDPR, and aligned clinical data issues.</li> <li>• Make recommendations for improvements that require out of budget funding, executive support or policy change.</li> <li>• Receive and approve / reject system accreditation statements.</li> <li>• Manage all associated information risks and ensure associated action plans are developed and progressed. Coordinate with Trust risk register.</li> <li>• Present meeting minutes to the Governance and Audit Committee.</li> <li>• Bi-Annually provide an assurance report, via the Governance and Audit Committee to the Trust Board.</li> </ul>
<b>Frequency</b>	<p>Bi-Monthly, coordinated to provide as timely reporting to the Governance And Audit Committee as possible.</p> <p>The sub-groups will meet on a monthly basis.</p>
<b>Standing Agenda Items</b>	<p><u>General items:</u></p> <ul style="list-style-type: none"> <li>• Introductions and Apologies for absence</li> <li>• Declarations of interest</li> <li>• Minutes of the last meeting</li> <li>• Action log</li> </ul> <p><u>Policies and decision making</u></p> <ul style="list-style-type: none"> <li>• As required</li> </ul> <p><u>Performance monitoring:</u></p> <ul style="list-style-type: none"> <li>• Information Governance report</li> </ul>



	<ul style="list-style-type: none"><li>• Information Security report</li><li>• Clinical Data Report</li><li>• Caldicott updates and log</li><li>• Risks</li><li>• Issues</li><li>• Records of business / escalations</li></ul>
--	---


Terms of Reference	
<b>Title:</b>	Information Governance Group
<b>Date Approved:</b> <b>Next review:</b>	
<b>Reporting to:</b>	The Informatics Assurance Group
<b>Accountability:</b>	 <pre> graph TD     AGC[Audit and Governance Committee] --&gt; IAG[Informatics Assurance Group]     IAG --&gt; IGG[Information Governance Group]           </pre>
<b>Purpose:</b>	<p>The IGG (Information Governance Group) is a delegated authority group accountable to the Governance and Audit Committee.</p> <p>Its purpose is to support and drive the information management and information governance agendas and provide the Trust Board with the assurance that effective policies and processes are in place within NIAS in relation to these fields.</p> <p>It will consider and approve proposed changes to the processing of data and review compliance with national and local requirements relevant to data processing</p>
<b>Membership</b>	<p>Head of Information, Chair of IGG,</p> <p>Corporate Services Manager</p> <p>Risk Manager</p> <p>HR Manager</p>
<b>Authority</b>	The IGG may make decisions within the remit set out in these terms of reference, as specified by the Trust's Scheme of Delegation or as delegated by the Trust Board.



	<p><u>Specific areas of responsibility:</u></p> <ul style="list-style-type: none"> <li>• Develop policy, procedure and supporting strategies and action plans in the area of information management and information governance for approval by the Governance and Audit Committee</li> <li>• Report compliance and areas of concern in relation to information governance to the Governance and Audit Committee</li> <li>• Make recommendations to Governance and Audit Committee or other appropriate committee for improvements that require out of budget funding, executive support or policy change.</li> <li>• As required, provide assurance regarding any national IG submissions</li> <li>• Manage and report internal and external audits relating to information management and information governance.</li> <li>• Promote a consistency of approach and share best practice between departments within NIAS in terms of compliance with information management and information governance</li> <li>• Ensure that an appropriate comprehensive information governance framework and systems are in place throughout NIAS, in line with national standards and guidelines</li> <li>• Manage and monitor the information governance policies and associated strategy and action plans</li> <li>• Ensure that the NIAS approach to information handling is communicated effectively to all staff and made available to the public where appropriate</li> <li>• Coordinate the activities of staff given information governance responsibilities including Data Protection, Freedom of Information, Data Quality and Records Management</li> <li>• Support and advise NIAS on the Caldicott and Data Protection functions and monitor compliance</li> <li>• Ensure specialist information governance training is provided for key staff including, Senior Information Risk Owner (SIRO), Caldicott Guardian, Information Asset Owners (IAO) and Information Asset Administrators (IAA) when required</li> <li>• Become the focal point for the discussion and resolution of information governance related issues</li> <li>• Perform the risk management function across the information governance agenda</li> <li>• Receive reports on themes and trends in information governance related incidents. Ensuring that appropriate mitigating actions are identified and implemented, and policies / procedure reviews undertaken where appropriate.</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>Provide a written report to each Governance and Audit Committee meeting</li> </ul>
<b>Frequency</b>	Meetings will occur monthly, coordinated to provide as timely reporting to the Governance and Audit Committee as possible.
<b>Standing Agenda Items</b>	<p>Updates from the last meeting</p> <p>Review of the Action Log</p> <p>Security Incident reporting</p> <p>Policy Review - Policies will be listed on the agenda, including review dates.</p> <p>New IT systems</p> <p>FOIA update/issues</p> <p>Data Quality update/issues</p> <p>Data Protection update/issues</p> <p>Risks</p> <p>Record of Business/Escalations Risks</p>



Terms of Reference	
<b>Title:</b>	IT Security Group
<b>Date Approved:</b> <b>Next review:</b>	
<b>Reporting to:</b>	The Informatics Assurance Group
<b>Accountability:</b>	 <pre> graph TD     AGC[Audit and Governance Committee] --&gt; IAG[Informatics Assurance Group]     IAG --&gt; ITSG[IT Security Group]           </pre>
<b>Purpose:</b>	The ITSG (Information Technology Security Group) will act as the management group for NIAS IT Security and provide specialist advice to the IAG (Informatics Assurance Group). The ITSG will work to recognised standards in the identification and management of all IT security related risks.
<b>Membership</b>	Assistant Director of IT, Chair of ITSG IT Manager IT Security Manager IT Network Manager Risk Manager
<b>Authority</b>	The ITSG may make decisions within the remit set out in these terms of reference, as specified by the Trust's Scheme of Delegation or as delegated by the Trust Board.  <u>Specific areas of responsibility:</u>

	<ul style="list-style-type: none"> <li>Consider all risks and issues impacting IT Security and decide appropriate course of action</li> <li>Produce IT security policies and processes aligned to ISO 27001 and present to IAG for approval</li> <li>Take actions in relation to established policy</li> <li>Make recommendations to IAG or other appropriate committee for improvements which require out of budget funding, executive support or policy change</li> <li>Consult on IT related policies and procedures</li> <li>Receive and approve/reject system accreditation statements and risk assessments.</li> <li>Manage &amp; monitor IT risks and issues</li> <li>Receive reports on themes and trends in information security related incidents ensuring that appropriate mitigating actions are identified and implemented, and policies / procedure reviews undertaken where appropriate</li> <li>As required, provide assurance regarding any national IT submissions</li> <li>Manage and report internal and external audits relating to IT security</li> <li>Provide documented assurance on IT security controls in particular: <ul style="list-style-type: none"> <li>Firewalls</li> <li>System patch levels</li> <li>Anti-virus implementation</li> </ul> </li> <li>Ensure that the NIAS approach to IT Security is communicated effectively to all staff and made available to the public where appropriate</li> <li>Manage security incidents in line with the HSCNI Cyber Security Incident Response Action Plan</li> <li>Provide a written report to each IAG meeting</li> </ul>
<b>Frequency</b>	Meetings will be held on a monthly basis, coordinated to provide as timely reporting to the IAG as possible.
<b>Standing Agenda Items</b>	<p>Updates from the last meeting</p> <p>Review of the Action Log</p> <p>Security Incident reporting</p> <p>Policy Review - Policies to be listed in the agenda, including review dates.</p> <p>New IT systems</p>



	<p>Risks</p> <p>NIS update</p> <p>Record of Business/Escalations Risks</p>
--	--





## SAFE HAVEN POLICY

### Links

The following documents are closely associated with this policy:

- Data Protection legislation (see 'definitions' section 4)
- Confidentiality Code of Conduct
- Information Governance Review (aka Caldicott 2) 2013
- Freedom of Information Act 2000
- Information Sharing Policy
- IM&T Security Policy

<b>Document Owner:</b>	Director of Planning, Performance and Corporate Services
<b>Document Lead:</b>	Head of Information Governance
<b>Document Type:</b>	Information Governance Policy
<b>For use by:</b>	All staff

This document has been published on the:	
Name	Date
SharePoint (Information Section)	
Intranet	



<b>Version Control</b>	<b>Document Location</b> If using a printed version of this document ensure it is the latest published version. The latest version is available on the Trust's Intranet site.
------------------------	--

<b>Version</b>	<b>Date Approved</b>	<b>Publication Date</b>	<b>Approved By</b>	<b>Summary of Changes</b>
1.0				New Policy and Procedure for NIAS

## Contents

1. Introduction.....	4
2. Objectives.....	4
3. Scope.....	5
4. Definitions.....	5
4.1 Patient Identifiable Information .....	5
4.2 Person Identifiable Information .....	5
4.3 Confidential Information.....	5
4.4 Data Protection legislation.....	5
5. Responsibilities.....	6
5.1 Chief Executive Officer.....	6
5.2 Senior Information Risk Owner (SIRO) .....	6
5.3 Caldicott Guardian .....	6
5.4 Head of Information Governance .....	6
5.5 Data Protection Officer .....	6
5.6 All staff.....	6
6. General Procedure.....	6
7. Fax Communications .....	6
7.1 Outgoing.....	7
7.2 Incoming.....	7
8. Postal Communications.....	8
8.1 Outgoing.....	8
8.2 Incoming.....	9
9. Email Communications .....	9
9.1 Outgoing.....	9
9.2 Incoming.....	10
10. Telephone Communication .....	11
11. Pseudonymisation .....	12
12. Informing Staff .....	13
13. Consultation .....	13
14. Monitoring Compliance and Effectiveness of the Policy .....	13
Plan for Dissemination of Procedural Document .....	14
Appendix 1 .....	14
Guidance on Sharing Personal and Confidential Information by Fax.....	15
Appendix 2 .....	15
Outgoing Faxes .....	15
Incoming Faxes .....	15
Appendix 3 .....	15
Appendix 4 .....	15

## **1. Introduction**

- 1.1 'Safe Haven' is a term recognised throughout the HSC to describe the administrative arrangements in place to safeguard the transfer of patient/person identifiable and other confidential information. In effect, a 'Safe Haven' is anywhere in the Trust where confidential information can be held and communicated safely.
- 1.2 Northern Ireland Ambulance Service HSC Trust (NIAS), as with all HSC organisations, has a duty of confidentiality to patients, this document aims to support this.
- 1.3 This document will detail the procedures for handling incoming and outgoing confidential information through any of the following means:
  - Fax
  - Post
  - Email
  - Telephone
- 1.4 When transferring personal and confidential information, adequate safe haven procedures should be in operation at the receiving point.
- 1.5 The Caldicott Guardian is ultimately accountable for the safe transfer of patient identifiable information (PII). However, each member of staff has a duty of confidence to patients, and contracts of employment contain details of their obligation to maintain this confidentiality.

## **2. Objectives**

- 2.1 The key objectives of this policy, and the associated procedure, are:

To ensure that PII is handled in accordance with the Caldicott Principles 2013:

- Justify the purpose(s)
- Don't use personal confidential data unless it is absolutely necessary

- Use the minimum necessary personal confidential information
- Access to personal confidential data should be on strict need to know basis
- Everyone with access to personal confidential data should be aware of their responsibilities
- Comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality
- To ensure that the legal obligations of Data Protection legislation are adhered to
- To provide a consistent approach to the way confidential information is handled

### **3. Scope**

- 3.1 This policy and procedure applies to all NIAS employees including permanent, temporary, voluntary and contract employees, who have access to personal and non-personal information.

### **4. Definitions**

#### **4.1 Patient Identifiable Information**

Information that can identify an individual patient

#### **4.2 Person Identifiable Information**

Information that can identify an individual.

#### **4.3 Confidential Information**

Information that when provided was done so in the expectation that it would be treated in confidence.

#### **4.4 Data Protection legislation**

Legislation, including, but not limited to the UK GDPR and UK Data Protection Act 2018.

## **5. Responsibilities**

### **5.1 Chief Executive Officer**

The Chief Executive Officer is the NIAS accounting officer and has overall accountability and responsibility for IG.

### **5.2 Senior Information Risk Owner (SIRO)**

The Senior Information Risk Owner will oversee information risk.

### **5.3 Caldicott Guardian**

The Caldicott Guardian will act as the 'guardian' of patient identifiable information and will oversee the use and sharing of patient information.

### **5.4 Head of Information Governance**

The Head of Information Governance will manage the day-to-day IG agenda and provide assurance to the Board on compliance levels with associated policies.

### **5.5 Data Protection Officer**

The Data Protection Officer will ensure NIAS can demonstrate its compliance with data protection legislation

### **5.6 All staff**

All staff have a responsibility to comply with legislation and policy relating to IG and to identify and report any areas of concern.

## **6. General Procedure**

All staff when handling PII and other confidential information should follow the procedures detailed within this section.

## **7. Fax Communications**

## **7.1 Outgoing**

7.1.1 A safe haven fax machine would be one situated in a secure location e.g. a locked office. When sending a fax containing PII or confidential information, a safe haven fax machine should be used. When this is not possible, additional steps should be taken to uphold the security of the information as follows:

- Telephone the intended recipient of the fax to let them know that you are going to send a fax containing confidential information
- Ask the recipient to wait by the fax machine while the fax is sent
- Ask the recipient to immediately acknowledge receipt of the fax
- Ensure the fax cover sheet clearly states the intended recipients name and contains a confidentiality disclaimer.
- Double check the fax number before pressing the 'send' button – use pre-programmable numbers for regular recipients
- Request a report sheet to confirm the transmission was successful

7.1.2 Do not send a fax to a destination that is not supervised. Additionally, you must ensure your presence while information is being transmitted.

## **7.2 Incoming**

7.2.1 Fax machines are situated at various locations throughout NIAS, where transmissions can be received for staff. As with outgoing messages, incoming ones must also be subject to secure handling procedures.

- The intended recipient of a fax should be contacted immediately a fax is received for them
- Whilst awaiting collection, the fax should be placed away from public view

- If a fax is not collected within the same day, it should be placed in a sealed envelope, marked 'confidential' and sent to the intended recipient.

7.2.2 Occasionally, confidential faxes will be received where the intended recipient is not clear. In these cases, they should be passed to a nominated person within each location. It is suggested that a senior manager should assume this responsibility within non-operational premises and the duty paramedic team leader on stations.

**Please note:** faxes are being phased out within the HSC and have been subject to removal within NIAS. However, it is considered prudent to include guidance on this method of communication.

## 8. Postal Communications

### 8.1 Outgoing

8.1.1 Wherever possible, PII or confidential information should be sent through the internal mail system, delivered personally or collected in person.

8.1.2 If it is necessary to send PII or confidential information via the Royal Mail, the following steps should be taken:

- Confirm the name, department (if applicable) and address of the intended recipient.
- Ensure the contents of the letter cannot be seen through the envelope
- Ensure the envelope is properly sealed
- Mark the envelope 'Private and confidential – to be opened by addressee only'
- Where possible PII should be sent via Recorded Delivery
- Bulk transfers of Person and Patient Identifiable Information **must** be sent via Recorded Delivery.
- Prior to sending bulk transfers via Royal Mail, contact the intended recipient to ensure they will be available

to sign for the Recorded Delivery communication when received.

- Request confirmation of receipt from the recipient.
- Electronic media should be encrypted with the password provided to the intended recipient via telephone or email separately from the information.

8.1.3 **NB** Information required by the police **must not** be sent via the Royal Mail.

## **8.2 Incoming**

8.2.1 Incoming mail should be opened away from public areas. Under no circumstances should the staff responsible for opening NIAS post open items addressed to an individual and marked 'Private and Confidential'.

8.2.2 Items marked to a Department, and not an individual, should be passed to the Head or Manager of that Department.

8.2.3 Items not marked with a name or department, and are not labelled 'Private and Confidential', should be opened by the post staff to establish to whom it belongs.

8.2.4 Any unmarked items that contain PII or confidential information should be placed in a sealed envelope and passed to the individual with Safe Haven responsibility (see 8.2.2).

## **9. Email Communications**

### **9.1 Outgoing**

9.1.1 PII or confidential information must not be transferred via external email unless sufficient encryption is in place. Another means of secure transfer must be used.

9.1.2 Emails containing confidential information must be clearly marked 'Confidential'.



9.1.3 Ensure the email is sent to recipients strictly on a 'need to know' basis

Password protect attachments if they contain PII or confidential information

9.1.5 Personal identifiers should be removed whenever possible

9.1.6 Personal identifiers should not be displayed in the email subject box

9.1.7 Email messages should contain a disclaimer in the event that they reach someone other than the intended recipient. A message is automatically attached to all NIAS email communications.

9.1.8 Emails sent between NIAS .nhs.uk addresses are deemed secure. However, the points mentioned in 9.1.2 – 9.1.6 should still be followed.

9.1.9 Emails sent between 'nhs.net' addresses are deemed secure.

9.1.10 Emails sent between hscni.net addresses and the following email addresses are deemed secure (as per BSO):

gov.uk

Please note that clinical information should only be sent to nhs.net or gsi addresses.

9.1.11 Please note: emails sent from NIAS .nhs.uk to nhs.net or one of the identified secure addresses as noted in 9.1.10 are not secure.

## **9.2 Incoming**

9.2.1 Although NIAS has little control over emails they receive, staff should remain aware of the dangers of opening messages from unknown or untrusted

sources. Please refer to the IM&T Security Policy for further guidance on email use.

9.2.2 Emails containing PII or confidential information, received in error, should be forwarded on to the correct location, if known, as soon as possible and deleted from the mailbox of the original receiver. The sender should be informed that this has happened.

9.2.3 If the intended recipient is not known to the receiver, the sender should be informed that the message has not reached its intended destination and has been deleted.

9.2.4 Enquiries received from members of the public, via email, requiring personal or confidential information, should almost certainly be replied to in writing – not electronically, as it is not possible to be certain the sender is who they say they are. If they still wish to receive a reply by email, the recipient should be fully informed of the possible risks and confirm their acceptance.

## **10. Telephone Communication**

10.1 PII or confidential information should not be discussed on telephone's that have 'hands free' capability unless they are situated in a single user office or car, and only those persons who need the information are present. Headsets should be used in the Emergency Operations Centre (EOC) so that only EOC staff are aware of the information being passed.

10.2 When taking a telephone call, be aware of the information that **cannot** be divulged over the telephone:

- Requests for information the Freedom of Information Act 2000 cannot be accepted over the telephone. The caller must be asked to make their request in writing.
- Information requested by the police must not be given over the telephone. Specific police procedures are in operation and requests must be made in writing using official paperwork. The request can be faxed through to a secure safe haven fax machine.

- Requests for information from the press or media must be forwarded on to an NIAS Communications Manager.

10.3 The following steps should be taken when PII or confidential information is requested over the telephone:

- Confirm the name of the person making the request along with their job title, department and organisation (if applicable).
- Establish the reason for the request.
- Take a contact telephone number. This should be a main switchboard number **not** a mobile or direct line number.
- If you are in any doubt of the caller's identity, call them back.
- If in doubt, check the information can be released and telephone the caller back. The Head of Information Governance will be able to provide advice.
- Provide the information only to the person making the request – do not leave a message with somebody else or on an answering machine.

## 11. Pseudonymisation

11.1 Pseudonymisation is concerned with enabling the HSC to undertake secondary use of patient data in a legal, safe and secure manner. The need to 'effectively anonymise' patient data can be found in the HSC policy and good practice guidance document 'Confidentiality: the HSC Code of Practice'.

11.2 This approach has been adopted in order to support the increasing direct flows between provider organisations and commissioners necessary for business purposes.

11.3 If it can be demonstrated that patient identifiable data is necessary for business purposes i.e. to resolve data quality issues, a 'safe haven' must be in place at the commissioning organisation. This must have restrictions and access controls in place where a limited number of staff will have access.

- 11.4 NIAS must be satisfied that the Safe Haven function is satisfactory prior to patient data being sent. The commissioning organisation will then be responsible for pseudonymising the data prior to it being used for purposes other than direct care for the patient.

## **12. Informing Staff**

- 12.1 It is essential that all staff who access PII or confidential information remain aware of the procedures contained within this document.

## **13. Consultation**

- 13.1 This policy will be presented to the Information Governance Group for consultation. The group has delegated authority to approve this document

## **14. Monitoring Compliance and Effectiveness of the Policy**

- 14.1 The Head of Information Governance will monitor the implementation of this policy and take an assurance report to the Information Governance Group. This report will be sent on an annual basis. However, if the on-going monitoring of this policy shows that there are significant implications for the implementation of this policy, then it will be sent to the group sooner.

## Plan for Dissemination of Procedural Document

Title of document:	Safe Haven Policy		
Version Number:	1	Dissemination lead: Print name, title and contact details	Tracy Avery Head of IG and Data Protection Officer, Tracy.Avery@hscni.net
Previous document already being used?	No		
Reading Categories  <i>List which document users fall within each category</i>	Essential Reading	All staff	
	Awareness for Reference Purposes	All staff	
	Awareness to inform staff / other stakeholders	All staff	
Whom does the document need to be disseminated to?	All staff have a responsibility to ensure information is disclosed and transferred appropriately and in accordance with legislation and national guidance therefore, all need to be aware of this policy.		
Proposed methods of dissemination: Including who will disseminate and when  Some examples of methods of disseminating information on procedural documents include: <ul style="list-style-type: none"><li>Information cascade by managers</li><li>Communication via Management/ Departmental/Team meetings</li></ul>		<ul style="list-style-type: none"><li>Information cascade by managers</li><li>Notification via articles in bulletins</li><li>Posting on the intranet</li></ul>	

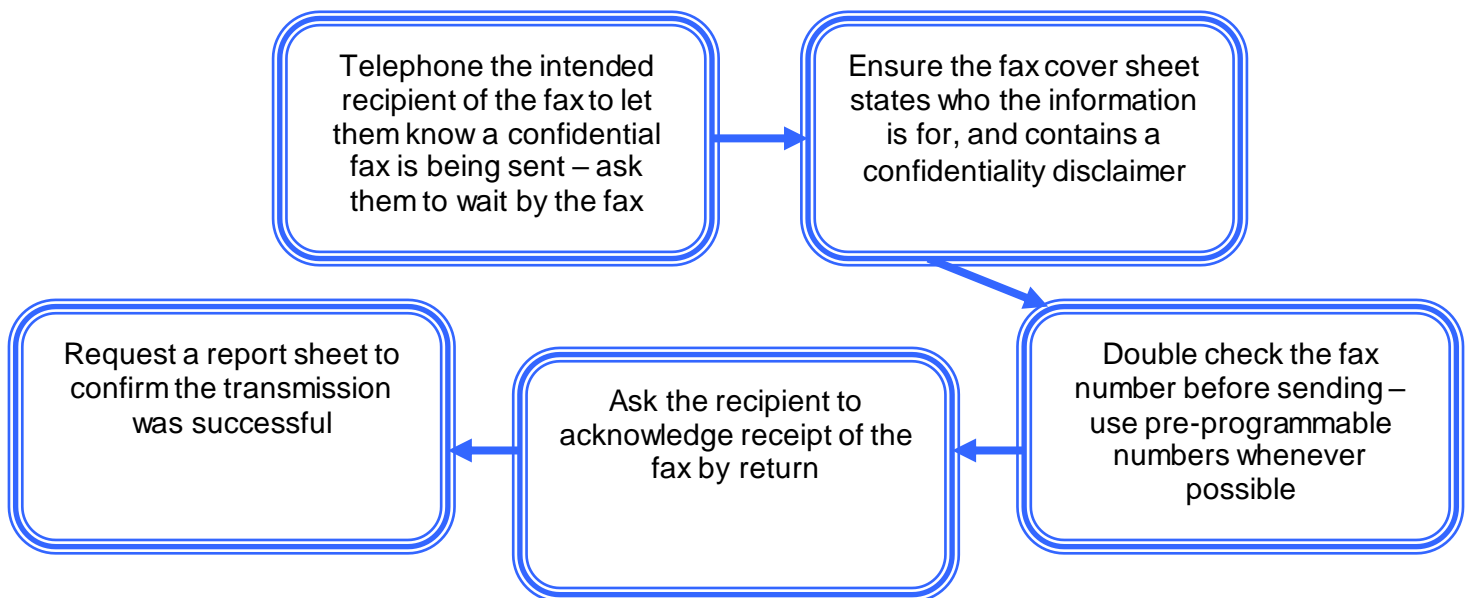
<ul style="list-style-type: none"> <li>• <i>Notice board administration</i></li> <li>• <i>Articles in bulletins</i></li> <li>• <i>Briefing roadshows</i></li> <li>• <i>Posting on the Intranet</i></li> </ul>	
<b>Summary for inclusion on the Class Publishing Applications system</b>	<p>Safe Haven Policy provides staff with the detail and guidance required on how and when to disclose and transfer information in accordance with legislation and national requirements.</p>

*Note: Following approval of procedural documents, it is imperative that all employees or other stakeholders who will be affected by the document are proactively informed and made aware of any changes in practice that will result.*

# Guidance on Sharing Personal and Confidential Information by Fax

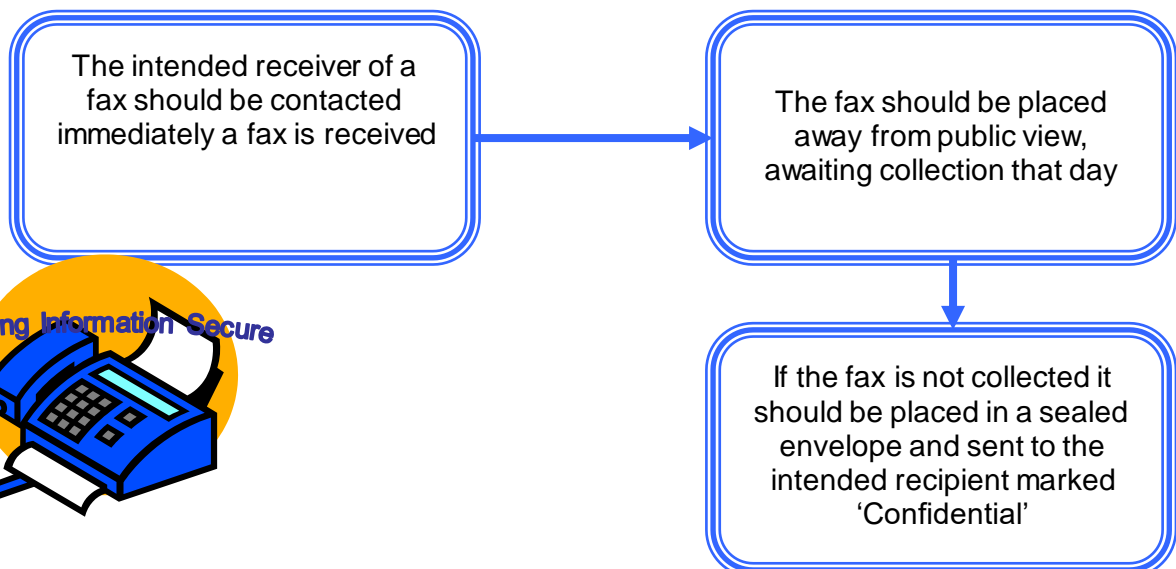
## Outgoing Faxes

IF YOU ARE NOT SENDING YOUR FAX TO A SECURE MACHINE, PLEASE FOLLOW THESE GUIDELINES:

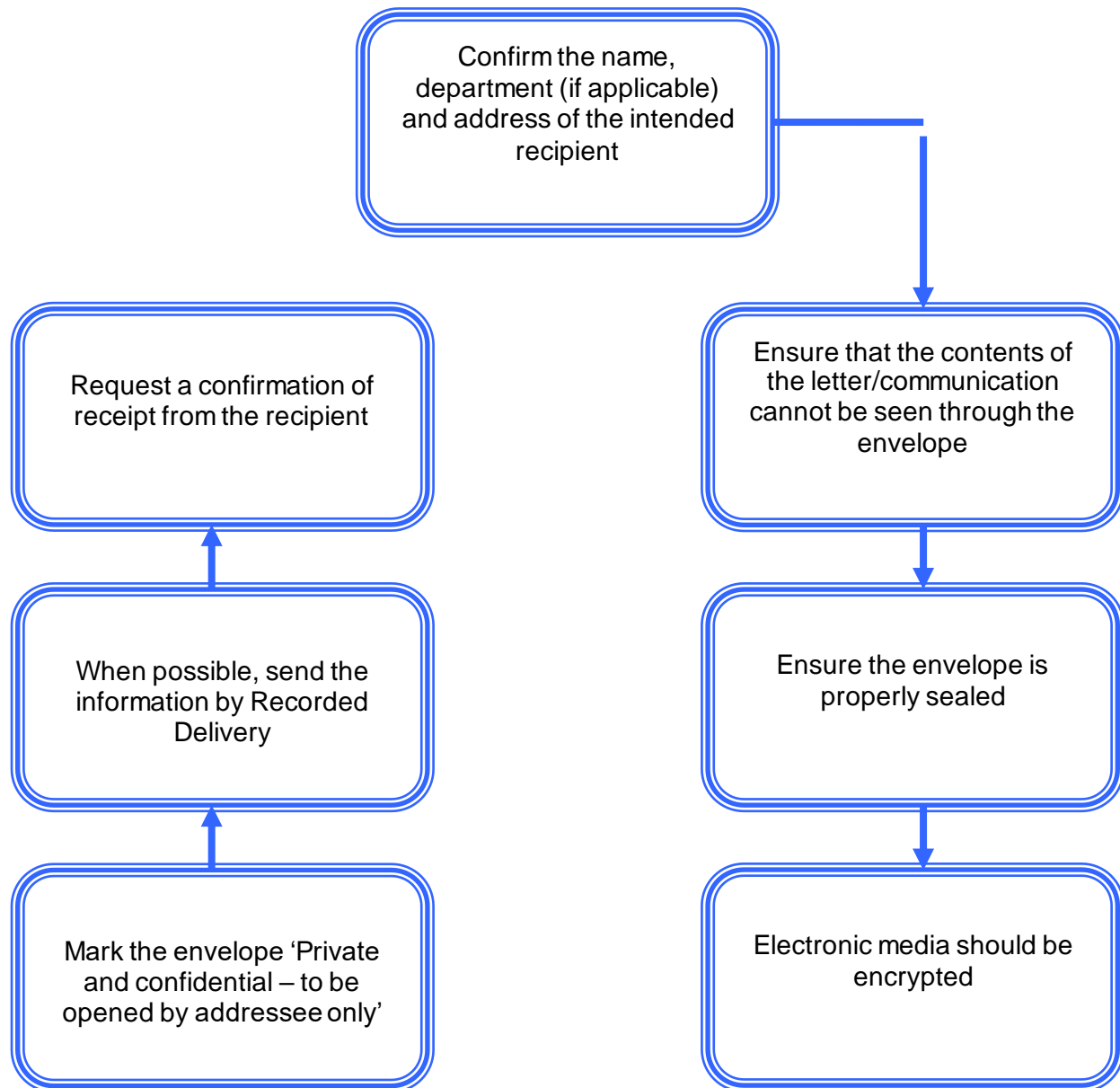


## Incoming Faxes

ANY FAXES RECEIVED THAT ARE NOT ADDRESSED TO A SPECIFIC PERSON THAT CONTAIN PERSONAL/CONFIDENTIAL INFORMATION, SHOULD BE PASSED TO THE HEAD OF INFORMATION GOVERNANCE



# GUIDANCE ON SHARING PERSONAL AND CONFIDENTIAL INFORMATION BY POST



## Keeping Information Secure



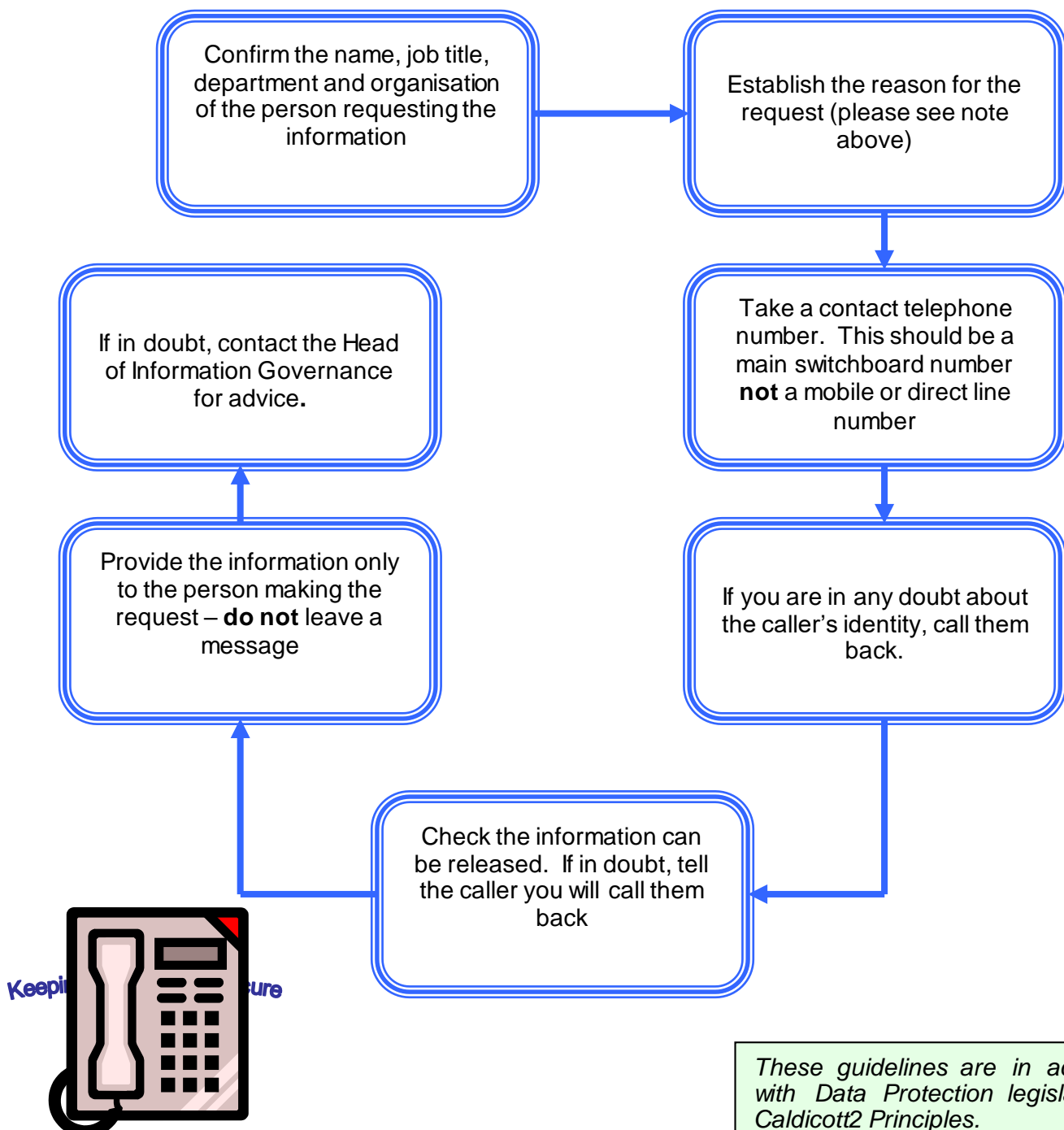
*These guidelines are in accordance with Data Protection legislation and Caldicott2 Principles.*

Any questions, contact EMAS Head of Information Governance [janette.kirk@emas.nhs.uk](mailto:janette.kirk@emas.nhs.uk) Tel: 0115 8845127




# GUIDANCE ON SHARING PERSONAL AND CONFIDENTIAL INFORMATION BY TELEPHONE

Requests for information under the Freedom of Information Act cannot be accepted over the phone. The caller must be asked to put their request in writing.



*These guidelines are in accordance with Data Protection legislation and Caldicott2 Principles.*

Terms of Reference	
<b>Title:</b>	Clinical Data Development Group
<b>Date Approved:</b> <b>Next review:</b>	
<b>Reporting to:</b>	Informatics Assurance Group
<b>Accountability:</b>	 <pre> graph TD     GAC[Governance and Audit Committee] --&gt; IAG[Informatics Assurance Group]     IAG --&gt; CDG[Clinical Data Development Group]           </pre>
<b>Purpose:</b>	<p>Act as an oversight governance group for the development and use of clinical data across the service. This meeting will feed into the wider clinical governance framework and will report into the NIAS clinical governance group.</p> <p>Three main development areas focus for the group:</p> <p><b>Data collection</b> Provide oversight for the maintenance and development of the EPR software. Act as the decision making group for change and proposal review.</p> <p><b>Data measurement</b> Develop the NIAS clinical measurement framework, balancing the clinical request with technical challenges. Approve new large clinical measurement or external data requests. Oversight of collaborative documents between clinicians and data analyst team; EG clinical</p>

	definitions document (defined numerators and denominators for clinical conditions).		
	<b>Data presentation and sharing</b>  Develop how this data is made available for use and feedback for the purposes of accountability and improvement. Investigate dashboard technology to allow for review of regional, sub region, station and ultimately individual level clinical data.		
<b>Membership</b>	<b>Name</b>	<b>Function</b>	
	Neil Sinclair	Chair	
	Tracey Avery	Information AD	
	Chris Clarke	AQI lead	
	David McCartney	EPR lead	
	Marianne Johnston	Business Manager	
	Data analyst	TBC	
	Project manager	TBC	
<b>Deputies</b>	Attendance at meetings is mandatory by a member or nominated deputy.  Deputies should only attend in exceptional circumstances. Deputies should have a full understanding of the group’s terms of reference and papers being presented. Deputies shall be expected to make decisions in accordance with the terms of reference as may be appropriate		
<b>Authority</b>			
<b>Frequency</b>	Monthly, coordinated to provide as timely reporting to the Governance And Audit Committee as possible.		
<b>Standing Agenda Items</b>	<ul style="list-style-type: none"><li>▪ Data Collection - EPR Issues, maintenance and development</li><li>▪ Data Measurement – CQI and professional standards framework - define, maintain and develop</li><li>▪ Data Sharing – Internal and external data sharing for accountability, improvement and research/development.</li></ul>		



**TB/04/03/2021/09**





**MINUTES OF THE AUDIT COMMITTEE HELD ON  
THURSDAY 29 OCTOBER 2020 AT 10AM BY ZOOM  
(DUE TO COVID-19)**

**PRESENT:** Mr W Abraham Non-Executive Director (Chair)  
Mr D Ashford Non-Executive Director

**IN**

**ATTENDANCE:** Mr B Clerkin ASM (External Auditors)  
Ms C McKeown Head of Internal Audit, BSO Internal Audit  
Mr S Knox Northern Ireland Audit Office  
Mr M Bloomfield Chief Executive  
Mr P Nicholson Interim Director of Finance  
Ms R O'Hara Programme Director Strategic Workforce Planning  
Dr N Ruddell Medical Director  
Mr A Phillips Assistant Director of Finance  
Ms T Steele Financial Accounts Manager  
Ms N Lappin Chair (observer)  
Mrs L Mitchell Independent Adviser to Committee  
Mrs C Mooney NIAS Board Secretary

**APOLOGIES:** Ms R Byrne Director of Operations  
Mr A Cardwell Non-Executive Director  
Ms L Charlton Director of Quality, Safety & Improvement  
Ms M Lemon Interim Director of Human Resources & Corporate Services  
Mr B McNeill CRM Programme Director  
Ms M Paterson Director of Planning, Performance & Corporate Services  
Ms A Quirk Board Apprentice

**Welcome, introduction and format of meeting**

The Chair welcomed everyone to the meeting and extended a particular welcome to the Trust Chair who would observe the meeting. The Chair

also welcomed Mrs Lesley Mitchell and said he would explain Mrs Mitchell's attendance later in the meeting.

33/20 **Apologies**

Apologies were noted as listed above.

34/20 **Declaration of Potential Conflict of Interest & Confirmation of Quorum**

The Trust Chair advised that she was also Chief Commissioner for the Charity Commission, and, as a result, declared a potential conflict of interest in the discussion around the External Audit Final Report To Those Charged With Governance which referred to NIAS Charitable Trust Funds.

The Chair also stressed the confidentiality of information presented.

35/20 **Previous Minutes (AC29/10/20/01)**

It was noted that the minutes of the previous meeting held on Thursday 2 July 2020 had been **APPROVED** by e-mail and reported to Trust Board on 27 August 2020.

36/20 **Matters Arising**

The Chair referred to the questions he had posed at the Committee meeting on 2 July 2020 and said that, while he appreciated the responses to the questions were included within the minutes, his preference would be to have a separate paper setting out the response against each question. He asked that this would be prepared for the next Committee meeting.

The Chair also referred to agenda items 7.2 and 7.3 and the questions posed within these documents to be considered by Audit Committees. He asked that Mr Nicholson prepare responses and suggested that it might be prudent to arrange an interim meeting to consider this depending upon Covid-19 concerns.



## 37/20 **Committee Chair's Business**

### **(i) Support for Audit Committee**

The Chair welcomed Mrs Lesley Mitchell to the meeting and explained that she would act as an Independent Adviser to the Audit Committee. He confirmed that, following discussions with the Trust Chair and Chief Executive, it had been felt that it would be helpful to bring in additional skills and experience to advise the Committee as provided for in the Terms of Reference.

The Chief Executive advised that, as the Trust revised its Committee structures, it would be important to ensure that the Committees had the necessary skills and experience to discharge their responsibilities as effectively as possible. He indicated that a similar arrangement had been put in place within the Safety Committee for a Senior Clinical Adviser with significant clinical background to provide support. Mr Bloomfield said that he very much looked forward to working with Mrs Mitchell.

Echoing the Chief Executive's comments, the Trust Chair said that Mrs Mitchell's background would be of significant value to the Committee. She added that it was not unusual to have an independent accountant in an advisory role on Audit Committees to assist members in discharging their functions. The Trust Chair advised that the DoH had also been keen to have additional independent accountancy experience on the Committee.

Mrs Mitchell provided members with a brief summary of her career to date and said the involvement of independent members only strengthened the importance of Audit Committees from a governance perspective. She added that she looked forward to working with members in the coming months.

### **(ii) Audit Committee Terms of Reference (AC29/10/2020/02)**

The Chair drew members' attention to the Committee Terms of Reference and, taking account of the establishment of the

People Committee, emphasised the importance of ensuring they all dovetailed. He suggested it would be helpful to consider the Terms of Reference and determine that they remained comprehensive and covered all elements of the Committee's business; whether any aspects of Committee business could be improved and identify any gaps/liaison items with other Committees.

The Chair also suggested that it would be important to take account of the Audit and Risk Assurance Committee Handbook (NI) 2018 while considering the Terms of Reference. At the Chair's request, Mrs Mooney undertook to circulate the Handbook and the Terms of Reference to members. He suggested that the interim meeting to be arranged could also consider revisions to the Terms of Reference.

The Chair indicated that Mrs Mitchell had identified some points for future discussion and he noted that he would circulate these to Committee members for information in due course.

Mr Ashford agreed with this approach and emphasised the importance of ensuring meaningful consideration of the various aspects of risk and where that risk sits. He stressed the importance of the Committee discharging its responsibilities and functions effectively and was of the view that Terms of Reference could be amended as necessary over time.

## 38/20 **Internal Audit**

### **(i) Progress Report (AC29/10/20/03)**

At the Chair's request, Ms McKeown took members through the detail of the Progress Report. She advised that, at the end of September, Internal Audit had completed 25% against the normal SLA figure. However she reminded the meeting that Internal Audit had stood down normal assurance work in Quarter 1 and had offered its services on an advisory basis. Ms McKeown pointed out that an element of this time had been under-utilised in NIAS. Therefore, taking into account

adjusted figures, Internal Audit had delivered 31% of SLA audit days to the end of Sept 2020.

Ms McKeown drew the Committee's attention to page 4 of the Report which set out progress against individual audit assignments approved by the Committee for the year.

She advised that the Risk Management Audit had received a satisfactory assurance with no significant findings identified and described the four key findings.

Mr Bloomfield welcomed the satisfactory assurance and said that the Trust would continue to work to progress the audit findings. He highlighted the challenge of staff, in particular Operational staff, undertaking e-learning over the coming months when one took account of the additional learning required in the context of Covid-19 around increased IPC requirements for example and believed it would be important to manage expectations.

Mr Ashford said that he would ensure the finding in relation to the reporting process of key risks to the Safety Committee was included in the next agenda. He referred to the revisions to the Committee structure and stressed the importance of ensuring the Framework to consider risk was improved where necessary.

Ms McKeown explained that page 11 of the Report concluded with a short briefing note on the advisory work carried out by Internal Audit across the six Trusts to develop a high level template around corporate Fraud Risk Assessment. She advised that the template, which had been agreed with Trust Assistant Directors of Finance, would assist Trusts in determining how directorate/service area level fraud risk assessments would be incorporated into the existing Directorate Risk Registers, or developed as a stand-alone Directorate Fraud Risk Assessment.

The Chair thanked Ms McKeown for her report which was **NOTED** by the Committee.

**(ii) Mid-Year Follow-up Review of Outstanding Internal Audit Recommendations 2020-21 (AC29/10/2020/04)**

Ms McKeown reported that, during September, Internal Audit had reviewed the implementation of the 132 outstanding audit recommendations and had determined that 65% of the total had now been fully implemented, with 34%, or 45 recommendations being partially implemented, and one percent (1%) yet to be implemented.

Ms McKeown advised that the oldest recommendation dating back to 2013-14 related to a Payroll audit and the AfC issue which should now be closed down by the year end. She indicated that Internal Audit had acknowledged the progress made against the 2016 Performance Management audit and was of the view that it was now a matter of implementing and embedding the decisions which had been made in terms of progressing performance management. Ms McKeown alluded to the recommendation made in 2019-20 around recruitment and the need to increase the numbers of staff sitting on job evaluation panels within the Trust. She acknowledged the impact of Covid-19 and the ability to source training at this time.

Ms McKeown confirmed that there was evidence of continued work in the majority of areas tested by Internal Audit and she said it was clear that Trust management were working to embed real change in these areas rather than merely implement the audit recommendation.

She referred the Committee to page 3 of the report and highlighted audit reports where she had given limited assurance: ICT 2017-18; Board Effectiveness 2018-19; Absence Management 2018-19; Complaints, Incidents and Claims Management 2018-19, noting that this audit area had recently received a satisfactory level of assurance; PCS 2019-20; Recruitment 2019-20 and said that she was content that work was ongoing in these areas.

The Chair referred to the fact one Internal Audit recommendation had related to the 'rejuvenation' of the Board

Governance Self-Assessment Tool and he sought further detail in relation to this.

Mr Bloomfield explained that work was being taken forward to explore whether the Self-Assessment Tool could be made more relevant by introducing a different tool. However he acknowledged that this work had been paused over the last 6-8 months in the context of Covid-19. Mr Bloomfield referred to recent correspondence from the DoH which had advised of a further pause in governance/sponsorship activities. He said that, while he considered the Self-Assessment tool to be included within such activities, it would still be important to progress the review of the effectiveness of the Board. He was of the view that the recommendation within the Audit Report to make the review meaningful was obligatory.

Mr Bloomfield reported that progress had been made around the recruitment of staff to participate in job evaluation panels. He acknowledged that there was a backlog in relation to such panels and said that a number of posts had been delayed due to lack of job evaluation panels.

Mr Bloomfield said that Ms McKeown had also highlighted the audit on Complaints, Incidents and Claims Management which had increased from a limited to satisfactory level of assurance. He said it was recognised that further work was required in relation to SAls and acknowledged the significant amount of work ongoing to address and improve SAls including clearing the backlog of investigations.

With regard to the PCS review, Mr Bloomfield reminded the meeting that he had asked Internal Audit to examine this area of work. He acknowledged that only eight recommendations had been partially implemented with no recommendations fully implemented as yet. Mr Bloomfield explained that the Trust had taken the view that to address the recommendations would not deliver the improvements required within the service and therefore it had been decided that it would be more prudent to undertake a review of PCS. To this end, he said, the Trust established a PCS Improvement Project led by Mr John Wright. Mr Bloomfield advised that the project had paused between March and July to allow Mr Wright return to his operational role within the Tactical Command centre. He

said that work on the review had now resumed and it was hoped that Mr Wright's role in the review would be protected through further surges of Covid-19.

Mrs Mitchell agreed with the approach outlined by Mr Bloomfield with regard to the Self-Assessment tool and the importance in ensuring the steps taken by the Trust were effective rather than address the audit recommendations from a purely academic perspective. She said it was important for all Board members to be fully involved and understand what was required collectively in order for improvements to be made.

Referring to the audit recommendation in relation to the Payroll report, Mr Nicholson reported that significant progress had been made in September with one-off payments made to EMTs. He further advised that current EMTs had yesterday been rebanded from Band 4 to Band 5 and Paramedics had also been rebanded from Band 5 to Band 6. He added that work now focussed on responding to queries from staff and he commended staff from Trust Finance and HR Directorates as well as colleagues from BSO Payroll in meeting the deadlines to ensure payments were made.

The Chair asked Mr Bloomfield to ensure the Committee's thanks were conveyed to all those involved working on such a significant achievement in relation to this long-standing issue.

Mr Bloomfield commented that the Agenda for Change issue had continued for a number of years and welcomed its resolution which he said would now allow the Trust to move forward.

Mr Ashford was of the view that the Self-Assessment Tool was not suitable and suggested that it might be helpful to have a facilitated discussion between Non-Executive Directors and SMT with a view to developing an action plan which could be used in responding to the next Self-Assessment Tool.

Mr Ashford referred to the PCS review and noted that the implementation timescale was 31 March 2021. He asked whether this timescale remained realistic and whether those

undertaking the review had access to external assurance, for example from AACE.

In response, Mr Bloomfield explained that the implementation date had been agreed at the time the Trust had reviewed and accepted the audit recommendations and he agreed that it would be prudent to revisit this. With regard to external support, he confirmed that Mr Wright had access to AACE and had availed of their support when developing the Project Initiation Document (PID).

Mr Bloomfield briefed members on the Trust's intention to develop its own project management capacity to support a number of ongoing programmes, thus allowing expertise to be retained within the Trust.

The Committee **NOTED** the Mid-Year Follow-up Review of Outstanding Internal Audit Recommendations 2020-21.

### **(iii) BSO Shared Service Update (AC29/10/2020/05)**

Ms McKeown advised that BSO Internal Audit carried out a programme of Shared Service audit assignments as part of the BSO Internal Audit Plan. She indicated that the recommendations in these reports were the responsibility of BSO Management to take forward and said that the reports had been presented to BSO Governance & Audit Committee in October 2020.

She advised that two areas had been audited: Accounts Payable and the Business Services Team, both of which were given a satisfactory level of assurance. She confirmed that there was nothing specific within the reports to draw the Committee's attention to.

The Committee **NOTED** the BSO Shared Service Update.

### **(iv) Head of Internal Audit Mid-Year Assurance Statement (AC29/10/2020/06)**

Ms McKeown explained that this agenda item was a summary of agenda items 6.1 and 6.2 and would ordinarily feed into the Trust's own Mid-Year Assurance Statement.



However, as members would be aware, the DoH had paused governance/sponsorship activities.

The Committee **NOTED** the HIA Mid-Year Assurance Statement.

**(v) Internal Audit Annual General Report 2019-20  
(AC29/10/2020/07)**

Ms McKeown explained that, to assist in sharing learning across the HSC, BSO Internal Audit had compiled the General Annual Report covering the period 2019-20. She drew the Committee's attention to page 4 of the report which summarised the common areas of limited or unacceptable assurances across the sector.

Ms McKeown highlighted some areas, for example clinical governance, procurement and contract management and payments which continued to show trends. She pointed to a number of elements which were relevant to the Trust in terms of corporate governance, for example staff and absence management, complaints management where there had been limited or unacceptable levels of assurance from Internal Audit.

The Chair welcomed the report and said it was useful to see other organisations' performance. He also pointed out that the report did not illustrate the fact that the Trust had been active in looking to identify areas where improvements were required and as such this had resulted in a number of limited assurances. However, the Chair agreed that the Trust had adopted a sensible approach to this work.

In terms of follow-up performance, the Chair referred to Mr Ashford's earlier point and noted that the number of partially implemented recommendations reflected the transitional nature of the work being taken forward by the management team.

Mr Bloomfield agreed with the points made by the Chair. He referred to the percentage of Trust audit findings, ie 14%, which had been deemed as unacceptable and felt that this had been borne out by the Trust's overall limited assurance



opinion. However, Mr Bloomfield pointed out that most of these audit findings, if not all, had been in areas which the Trust had highlighted and he welcomed the improvements and progress which had been made in the follow-up of recommendations.

In relation to the reference to a higher proportion of NIAS audit findings being unacceptable when compared to other HSC organisations, Mr Nicholson advised that the Trust was subject to significantly fewer audit assignments than other Trusts. This had the effect that any unacceptable finding created a higher proportion when compared to other organisations.

Ms McKeown accepted that this was an important point and explained that this percentage only related to one report.

The Committee **NOTED** the report.

### 39/20 **External Audit**

#### **(i) External Audit Final Report to Those Charged with Governance 2019-20 (AC29/10/20/08)**

Mr Nicholson advised those present that this was the final Report To Those Charged With Governance 2019-20 and pointed out that there had been no significant changes to the draft report reviewed by the Committee at its July meeting.

Mr Clerkin confirmed that there had been very few changes. He advised the Committee that Audit Office procedure required a change in audit partner every five years. Mr Clerkin explained that Ms Christine Hagan would now assume the role of ASM representative on the Committee and Ms Judith Shorthall would remain as senior manager. He indicated that Ms Hagan had significant experience in the health sector and currently attended the NIBTS, PHA and HSCB Audit Committees.

The Chair extended the Committee's thanks to Mr Clerkin for his contribution over the last five years and commended him on his attention to detail.

Mr Ashford referred to the further oversight required around Direct Award Contracts and asked how the Committee might achieve this.

The Chair explained that, in preparatory discussions with Mrs Mitchell, she had suggested that Direct Award Contracts become a standing item on the agenda to allow management to advise the Committee as appropriate.

**(ii) Guide for Audit and Risk Committees on financial reporting and management during Covid-19 – National Audit Office (AC29/10/2020/09)**

Mr Nicholson explained that the documents relating to this and the next agenda item had been included for completeness for the Committee. He said that the Committee would consider the same issues for the 2020-21 year and added that the document would prove helpful when the Committee started to consider its External Audit planning cycle at its next meeting.

Mr Nicholson advised that the Trust had carried out an initial assessment around Covid-19 risks and he referred to Ms McKeown's early reference to the Internal Audit work looking regionally at the controls in place. Mr Nicholson undertook to bring a formal Trust response to each of the areas outlined in both reports to a future meeting.

The Chair suggested that it might be helpful to convene an interim meeting involving Committee members and Trust officers only to ensure a full and comprehensive response to these areas depending upon Covid-19 constraints.

**(iii) Covid-19 Fraud Risks – NI Audit Office (AC29/10/2020/10)**

Discussion at (ii) above also refers.

40/20 **For Noting**

**(i) DoH correspondence re: Pause in Sponsorship and Governance Activities (AC29/10/2020/11)**

The Committee **NOTED** the correspondence dated 14 October 2020 from Ms La'Verne Montgomery, Director of Corporate Management, DoH, advising of a further pause in sponsorship and governance activities.

Mr Ashford referred to the correspondence and said he and other Non-Executive Director colleagues would be willing to assist in whatever way necessary.

The Chair alluded to DoH correspondence earlier in the year which had paused activities and which had asked Non-Executive Directors to assume greater involvement in overseeing governance arrangements. He said that great effort had been made to ensure the active engagement of Non-Executive Directors and referred to the arrangements which had been put in place at that time such as the regular meetings between the Chair, Chief Executive and Committee Chairs and the weekly e-mail updates on Covid-19.

**(ii) DoH correspondence re: NIAS Overall Limited Assurance (AC29/10/2020/12)**

The Committee **NOTED** the Permanent Secretary's correspondence dated 16 October.

**(iii) Annual Theft and Fraud Report 2018-19 (AC29/10/2020/13)**

Mr Nicholson explained that the Annual Theft and Fraud Report 2018-19 was for members' information. He advised that the report brought together the work carried out across the public sector in the 2018-19 year and said that Trust officers would review the documentation with a view to identifying any learning which could be applied within the Trust.

The Committee **NOTED** the Report.

#### **(iv) National Fraud Initiative – NI Report (AC29/10/2020/14)**

Mr Nicholson explained that the Report provided the outcome of the previous National Fraud Initiative and advised that the current National Fraud Initiative exercise had recently commenced. He said that the report would be examined with a view to identifying any potential exposures to fraud for the Trust.

Responding to a question from the Chair, Mr Nicholson clarified that the report encompassed the public sector and was not solely health focussed.

The Committee **NOTED** the Report.

#### **(v) Fraud Update – verbal report**

Mr Phillips updated the Committee on four fraud cases which, following enquiries, he had recommended to be closed due to no evidence having been identified. He advised that a further two anonymised cases had been received via the Counter Fraud website and said that preliminary enquiries were ongoing. He undertook to keep the Committee apprised.

Mr Phillips pointed out that the National Fraud Initiative was now on its seventh edition. He said that, whilst there had been no evidence of fraud, it provided an additional level of assurance to the Trust. Mr Phillips also referred to a meeting scheduled in the coming weeks with Counter Fraud and regional Fraud Liaison Officers around the completion of the fraud risk assessment template with a view to implementing this across Directorates in a meaningful way.

Responding to a question from the Chair as to whether any Whistleblowing reports had been received, Mr Phillips confirmed that the two most recent cases had been received anonymously through the Counter Fraud website.

The Chair referred to discussion with Mrs Mitchell around the role of the Committee in relation to receiving Whistleblowing reports as well as ensuring such issues were progressed through the revised Committee structure.

Mr Bloomfield agreed with this point and said that it would be important to ensure Committee members were content with Terms of Reference. He added that, if required, the Terms of Reference could be revised to ensure appropriate balance.

41/20 **Closed Meeting**

At this point in the meeting, Committee members met independently with the Internal and External Auditors in a closed meeting. This was facilitated through the use of a Zoom break-out room.

Upon their return to the meeting, the Chair advised that the general consensus had been that Mrs Mitchell, in her role as Independent Adviser to the Committee, should also attend the closed meeting. There were no other matters arising or actions required as a result of the closed meeting.

42/20 **Any Other Business**

Mr Bloomfield and Mr Nicholson extended their appreciation to Mr Clerkin and wished him well for the future.

43/20 **Date, time and venue of next meeting**

The next meeting of the Audit Committee would take place on Thursday 4 February 2021 at 10am (venue and arrangements to be confirmed)

The Chair thanked Mr Clerkin for his contribution to the Audit Committee over the last number of years and declared the meeting closed.

SIGNED: 

DATE: 19 February 2021



## ‘SAFETY’ COMMITTEE REPORT TO TRUST BOARD 21/1/21

The Safety, Quality, Patient Experience and Performance Committee met on Thursday 19 November 2020. Issues discussed included:

1	<u>Committee Terms of Reference</u> <ul style="list-style-type: none"> <li>Approved by Committee (and subsequently by November Trust Board) with a view to reviewing these in six months’ time.</li> </ul>
2	<u>NIAS Cat I Improvement Project</u> <ul style="list-style-type: none"> <li>The Committee received a presentation from Ms Ruth McNamara, Assistant Director Control &amp; Communications, EAC, and Mr Frank Rafferty, EAC Continuous Development Manager, on the work being taken forward to improve response times.</li> </ul>
3	<u>Development of enhanced clinical and professional leadership in NIAS</u> <ul style="list-style-type: none"> <li>The Committee received a presentation from Mr Neil Sinclair, Assistant Clinical Director (Paramedicine) on plans to develop enhanced clinical and professional leadership in the Trust which would, over time, strengthen governance arrangements within NIAS.</li> </ul>
4	<u>Regional Trauma Bypass Protocol</u> <ul style="list-style-type: none"> <li>The Committee was advised that the Protocol, which had been implemented on 26 October 2020, meant that ambulances within a 45 minutes – 1-hour drive from Belfast would go directly to the RVH with those patients who met the criteria for serious trauma.</li> </ul>
5	<u>RQIA Safeguarding Quality Improvement Plan – update on progress</u> <ul style="list-style-type: none"> <li>The Committee noted the significant progress made and that further work would be taken forward around statutory requirements.</li> </ul>
6	<u>Risk Management Progress Report including Corporate Risk Register</u> <ul style="list-style-type: none"> <li>New risks include outbreak of Covid-19 and organisational culture;</li> <li>Risk re operational impact of Covid-19 increased to reflect current situation;</li> <li>Risk re estate condition reduced due to increased level of statutory compliance;</li> <li>Total of 137 risks on the Corporate Risk Register;</li> <li>Work carried out to clarify the ‘age’ of each risk – however the mitigations employed and the treatment may be sufficient to manage that risk in the long-term if risk appetite is applied;</li> <li>Corporate Risk Register contained significant amount of information to allow members interrogate the Register. This information would evolve over time.</li> </ul>
7	<u>Adverse Incident Report</u> <ul style="list-style-type: none"> <li>The Committee welcomed the new format of report which provided an overview</li> </ul>



	<p>and associated learning;</p> <ul style="list-style-type: none"> <li>Managing and learning from adverse incidents is one of the key markers of success in relation to risk management, corporate and clinical and social care governance standards.</li> </ul>
8	<p><u>Board Assurance Framework</u></p> <ul style="list-style-type: none"> <li>Framework has been updated to take account of the Corporate Strategy and Plan;</li> <li>The revised format using the lines of defence model was used by the IHRD enquiry as well as complementing the Dear Accounting Officer correspondence and Treasury guidance;</li> <li>Acknowledgement that Framework was a working draft and further refinement would be necessary;</li> <li>Workshop to be organised to look at assurance specifically.</li> </ul>
9	<p><u>SA/Incidents – Learning Outcomes and Position</u></p> <ul style="list-style-type: none"> <li>Number of initiatives underway within the Trust to improve awareness of reporting which had resulted in an increase in SAs;</li> <li>The Committee noted the improved position in relation to outstanding SAs;</li> <li>While improvements have been made, the Trust continues to strive towards meeting the standard of reporting SAs within 72 hours;</li> <li>Work ongoing to examine how best to bring SAs to the attention of Trust Board;</li> <li>Emphasis has been placed on ensuring any learning is fed back into the organisation and actions taken as a result;</li> </ul>
10	<p><u>Complaints, Compliments and Care Opinion</u></p> <ul style="list-style-type: none"> <li>There are currently 102 open complaints;</li> <li>Trust received more complaints in August than it had in the previous two years;</li> <li>Trust examined trends identified from complaints and staff members were advised if a complaint had been received relating to them;</li> <li>Work ongoing to ensure stations scan and forward any cards/letters to HQ for inclusion in stats as well as ensuring any staff mentioned in these are advised;</li> </ul>
11	<p><u>Infection Prevention Control – Key Performance Indicators</u></p> <ul style="list-style-type: none"> <li>The Committee received a summary of the performance related to each of the IPC related KPIs for May-October 2020;</li> <li>It had not been possible to present data relating to hand hygiene audits as hand hygiene link staff within each Division had not been in a position to carry out the audits;</li> <li>Key appointments made, ie an IPC Practitioner and an Environmental Cleanliness Lead;</li> <li>The variances in the observational audits undertaken as well as the need to strengthen assurances around KPIs were acknowledged;</li> <li>The Committee noted the need for more independent audits to be undertaken as well as providing more training for staff.</li> </ul>
12	<p><u>The Management of Infection Prevention and Control Incidents and Outbreaks Policy</u></p> <ul style="list-style-type: none"> <li>The Committee was advised that it would be necessary to review the membership of Incident/Outbreak teams for the management of Covid-19 outbreaks due to the</li> </ul>





	<p>number of ongoing outbreaks. This reduced membership would only apply to Covid-19;</p> <ul style="list-style-type: none"><li>Any concern around the impact or severity of an outbreak of Covid-19 would be escalated to the Trust's Director of Quality, Safety &amp; Improvement by the Outbreak Control Group</li></ul>
13	<p><u>EU Exit</u></p> <ul style="list-style-type: none"><li>The Committee was advised on an issue relating to the supply of Entonox cylinders by BOC and the steps being put in place to resolve this.</li></ul>



Northern Ireland Ambulance Service Health and Social Care Trust

[www.nias.hscni.net](http://www.nias.hscni.net)