



Title:	Surveillance / CCTV Camera Policy (excluding Body Worn Video)		
Author(s):	<div>██████████</div> Fire & Security Advisor <div>██████████</div> Risk Manager		
Ownership:	<div>██████████</div> Director of Planning, Performance & Corporate Services		
Date of SMT Approval:	14 th March 2023	Date of ARAC Approval:	30 th March 2023
Operational Date:	30 th March 2023	Review Date:	March 2026
Version No:	1.0	Supersedes:	N/A
Key Words:	CCTV, surveillance camera, body worn video, images, vehicle CCTV, video evidence, Data Protection Act, UK GDPR, Freedom of Information, subject access request, Data Protection Privacy Impact Assessment (DPIA), legitimate interest assessment		
Links to Other Policies / Procedures:	Security Policy, Management of Aggression Policy & Procedures, Corporate Risk Management Policy and Strategy, Health and Safety Policy and Procedures, Risk Assessment Procedure, Information Governance Policies and Procedures, PPI Strategy, Learning From Serious Adverse Incidents (SAIs) Procedure, Incident Reporting Procedure. Image and telematics data procedures.		

Version Control:			
Date:	Version:	Author:	Comments:
January 2023	0.10	Risk Manager	UNITE comments
August 2022	0.9	Risk Manager	Hol / BLS comments
April 2022	0.8	Risk Manager	Complaints comments
March 2022	0.7	Risk Manager	West SO comments
March 2022	0.6	Risk Manager	NIPSA comments
March 2022	0.5	Risk Manager	Ops Business Improvement Lead comments
September 2021	0.3	Risk Manager	Fleet & EP comments
September 2021	0.2	Risk Manager	Initial review
June 2021	0.1	Fire & Security Advisor	Initial draft

1.0 INTRODUCTION:

This Policy provides a framework for the planning, installation, maintenance and management of surveillance camera systems including Closed-Circuit Television (CCTV) and Digital Video Recording (DVR) on sites and vehicles owned or occupied (long term) by the Northern Ireland Ambulance Service Health and Social Care Trust (NIAS). Body worn video / cameras and associated systems are excluded from this Policy (separate Policy in place).

It aims to ensure that arrangements are in place to ensure legislative compliance at each of the above stages, and that staff involved in the management and operation of such systems have the necessary information, instruction and training to ensure that they discharge their responsibilities as required.

1.1 Background:

The Trust is responsible for a considerable amount of people, property and resources including specialist medical equipment and controlled drugs. The Trust employs approximately 1600 staff and the installation of surveillance equipment is necessary in order to assist in the safety and protection of staff, assets, the general public, patients / clients / service users and visitors. The Trust uses surveillance camera systems in three distinct areas:

- Sites including ambulance stations, vehicle storage and maintenance sites (images only).
- In ambulance / emergency response vehicles (images only).
- In relation to staff, i.e. body worn video (audio and video) – separate Policy in place.

The Trust also uses surveillance systems during major incidents, where the Hazardous Area Response Team (HART) may use more sophisticated and protected equipment such as command and control vehicles with additional heat seeking and infrared equipment.

In the implementation of this Policy, the Trust will ensure adherence to the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018, Human Rights Act 1998, the Freedom of Information (FOI) Act 2000 the Information Commissioner's Office CCTV Code of Practice 2017, and the Surveillance Camera Code of Practice 2013.

1.2 Purpose:

This Policy establishes a robust framework for the planning, installation, use and maintenance of surveillance cameras / systems within the Trust. Its purpose is to ensure that the operational use of surveillance systems are proportionate, legitimate and necessary; that they will be only used when deemed necessary for legitimate purposes, by trained staff in accordance with legislation, Policy and procedures. It sets out roles and responsibilities, provides staff with the correct processes for collecting, downloading, processing and presenting video evidence, appropriate retention etc. If offsite or remote viewing is to be undertaken, then secure protocols or encryption needs to be utilised.

In order to lawfully process personal data using surveillance camera systems NIAS must have a lawful basis under the United Kingdom General Data Protection Regulation.

Our primary lawful basis for the purpose of processing CCTV data is:

Article 6 (1)(e) - the processing is necessary for the performance of a task carried out in the public interest under UK GDPR.

In addition, where we may process CCTV data outside the scope of our tasks as a public authority, but within our other legitimate purposes, such as protection of our staff car parks etc. we rely on Article 6(1)(f).

1.3 Objectives:

With regards to surveillance cameras / systems, this Policy seeks to ensure the following:

- Compliance with the appropriate legislation and guidance including requirements around privacy, data protection and freedom of information.
- That staff are trained and have detailed guidance on the collection, downloading, processing, presentation and retention of video / audio evidence.
- That surveillance cameras / systems are used correctly to maximise their benefit.
- A reduction in the risk of violence and aggression towards staff as surveillance systems should act as a deterrent (clearly demonstrating that actions may be recorded).
- Safeguarding of public assets.
- That the level of surveillance is kept under review with the Trust's Data Protection Officer and in line with Information Commissioners Office Guidance.
- The relevant Data Protection Privacy Impact Assessments (DPIAs) are conducted as any changes take place.

2.0 SCOPE:

This Policy applies to all Trust staff at all levels and any other persons working for, or on behalf of NIAS. This policy applies to all surveillance camera systems (CCTV and vehicle mounted) with the exception of body worn video / cameras (separate Policy in place).

The systems and its recorded material will be used by the Trust for the legitimate recording of activity in and around sites and vehicles to record certain interactions between staff and service users and / or other individuals in order to provide enhanced security and quality evidential recording of events. The Trust may use recorded material in connection with any of the purposes listed below:

- Protecting NIAS sites and vehicles from theft or damage, including equipment, controlled drugs and other Trust assets from theft or damage.
- Reducing risk / protecting staff / members of the public etc. through enhanced arrangements for health, safety and security to deter acts of violence and aggression (along with the provision of clear information to service users / public etc. that actions may be recorded, i.e. signage and privacy notices).
- In connection with the prevention, detection and investigation of crime and / or regulatory or enforcement activities such as those undertaken by the Police Service for Northern Ireland (PSNI), the Coroner, the Health and Safety Executive for Northern Ireland (HSENI), the Regulation and Quality Improvement Authority (RQIA) and / or any other

regulator because the law permits or requires release. When appropriate, the PSNI may show recorded material to the public to assist with their criminal investigations.

- In connection with the investigation of road traffic offences and collisions, ambulance vehicle incidents and road traffic incidents / complaints which involve Trust vehicles to establish an accurate account of events and / or to ensure appropriate driving standards in line with statutory requirements and training.
- In connection with civil or criminal proceedings, recorded material may be made available to third parties such as solicitors, insurers, Department of Health Legal Services staff etc.
- In relation to [a specific documented reason](#) (Appendix 1) with regards to incidents, serious adverse incidents, complaints, employment processes, Health and Care Professions Council (HCPC) investigations, General Medical Council (GMC) investigations etc. in cases of misconduct or alleged misconduct, where a potential criminal offence has occurred, or where there are other exceptional circumstances (determined by an incident review panel meeting attended by relevant Trade Unions, Data Protection Officer, Risk Management and the relevant Director / Assistant Director). Where misconduct / negligence has not yet been established but viewing of CCTV footage is deemed necessary, access may be provided a limited number of authorised colleagues, i.e. investigating officer / Line Manager (if appropriate).
- In relation to publicity / commercial purposes only if in the public interest.

This Policy is intended to reassure staff and the public that a standard is in place that controls the use of systems on Trust owned or occupied sites. Access to recorded material by Trust staff and third parties will only be granted as set out in this Policy.

3.0 ROLES AND RESPONSIBILITIES:

3.1 The Chief Executive is responsible for:

- Ensuring that there are suitable and sufficient arrangements in place for the management of surveillance camera systems within the Trust, including the necessary resources, monitoring processes, information governance and oversight where appropriate.
- Ensuring the full and effective implementation of this Policy, and satisfying Trust Board of the same.
- Ensuring there are suitable arrangements in place for the review and audit of this Policy document to ensure that it remains fit for purpose and that full compliance is achieved.

3.2 The Director of Planning, Performance & Corporate Services is responsible for:

- Providing the Chief Executive and Trust Board with information and assurance pertaining to the governance and management of surveillance camera systems within the Trust.
- Ensuring that NIAS has a robust system and structure in place for surveillance.
- Ensuring all employees are made aware of this Policy and the requirement for their professional conduct at all times during employment.

3.3 Directors & Assistant Directors are responsible for:

- Implementing this Policy and any associated guidance.
- Ensuring arrangements are in place for monitoring and compliance with this Policy.
- Ensuring that there are suitable resources available for the implementation of this Policy.

- Informing the Risk Management Team where there is a significant change in corporate structure or operational practices.
- Appointing data controllers within their area of responsibility for all of the Trust's surveillance camera systems.

3.4 The Risk Management Team is responsible for:

- The development of suitable policies and procedures compliant with legislation relating to the use of CCTV and surveillance equipment.
- Consultation with any other agency or Trade Union representatives on the content of this Policy.
- Regularly monitoring and reviewing this Policy to ensure it remains compliant with legislation and is relevant to the Trusts practices and procedures.
- Assisting managers in the relevant training in regards to surveillance camera systems and record training as per Trust procedures.
- Investigating any issues pertaining to images and information captured on CCTV installations and devices.

3.5 The Data Protection Officer (DPO) is responsible for:

- Ensuring that the ICO is informed of NIAS CCTV and surveillance equipment.
- Privacy notices are accurate and available.
- Ensuring that each individual system is managed by a named member of staff with the appropriate level of authority.
- Ensure adequate arrangements are in place with regards to Information Asset Owners.
- Advising staff on all Data Protection / information governance issues relating to surveillance systems.
- Providing advice and guidance on appropriate use of CCTV images and systems.
- Providing a point of contact between NIAS and external parties such as HSENI and PSNI.
- Redacting and handing over any information as required to the PSNI or HSENI.
- Liaison with the Trusts Caldicott Guardian as necessary.
- Providing assistance and advice on the legitimate use of CCTV images following incidents.
- Taking part in the planning and authorisation process for all new CCTV systems.
- Commissioning periodic audits of CCTV systems to ensure that they remain DPA compliant.
- Investigating any breach of information security in relation to the Trust's surveillance camera system and ensure appropriate governance
- Oversight of arrangements for the nomination and authorisation of suitable contractors.
- Considering on a case by case basis retrieval requests which have a legal basis, i.e. Subject Access Requests, or an applicable warrant.
- Overseeing a DPIA for new systems where necessary.

3.6 The Fire & Security Advisor (FSA) is responsible for:

- Carrying out security assessments and providing an operational requirement for new site surveillance systems in-line with Home Office Guidance.
- Providing an operational requirement for all existing site CCTV systems where all upgrades or modifications are carried out.

- Ensuring that impact assessments are carried out for all site CCTV installations, both current and new.
- Regularly reviewing the data protection impact assessments and ongoing requirements for use of site CCTV installations.
- Measuring progress against the operational requirement on all new site works and upgrades.
- Routine inspection of site CCTV systems / installations to ensure they are compliant as well as fit for purpose.
- Ongoing review to ensure that adequate signage is in place indicating use of site CCTV installations.
- The development of procedures supporting operational use of site based surveillance systems including downloading, reviewing, secure storage and secure disclosure of recorded material to include arrangements for authorised staff only to access.
- Supporting the Information Team with periodic audits of CCTV systems to ensure that they remain compliant.

3.7 The Fleet Manager is responsible for:

- Assessment, procurement and installation and proper functioning of vehicle based surveillance systems including data protection by design of vehicle based systems.
- Erection of signage for vehicle based systems.
- The development of procedures supporting the operational use of vehicle based systems including downloading, reviewing, secure storage and secure disclosure of recorded material to include arrangements for authorised staff only to access.
- Ensuring vehicle based systems are appropriately inspected, serviced and maintained with any faults and repair work conducted in line with this Policy.
- Ensuring the physical security of the system installed, external hardware and internal software storage units are maintained.
- Supporting the Information Team with regards to the collection of and release of information.
- Ensuring that suitable contractors are nominated and do not have access to recorded material without authorisation from the Data Protection Officer.

3.8 The Head of Estates is responsible for:

- Liaising with the Fire & Security Advisor on proposed new site installations.
- Procurement, installation and proper functioning of site based surveillance systems including data protection by design of site based surveillance systems.
- Erection of appropriate signage for new site installations.
- Ensuring site based surveillance systems are appropriately inspected, serviced and maintained with any faults and repair work conducted in line with this Policy.
- Ensuring adequate records are retained in line with the Trusts retention Policy.
- Liaising with contractors with regards to the loan of equipment in the event of system breakdown.
- Ensuring the physical security of the system installed, external hardware and internal software storage units is maintained.
- Ensuring that suitable contractors are nominated and do not have access to recorded material without authorisation from the Data Protection Officer.
- Ensuring that recorded material is deleted upon disposal / decommissioning.

3.9 The Information & Communications Technology Department (ICT) are responsible for:

- Facilitate the network infrastructure.
- Maintenance and upkeep of associated network connections.

3.10 Line Managers are responsible for:

- Implementation of this Policy, ensuring and monitoring compliance.
- Ensuring any faults are reported immediately.
- Appointing a deputy to ensure that any systems continue to be managed in the absence of the local manager.
- Ensuring written local procedures are available for each system. These include details of those authorised to export data from the system, a plan of all camera locations with camera numbers, manufactures user guides for digital recording devices, and fault reporting procedures.
- Receiving and actioning requests from the Information Team – the responsible manager will document the date of removal of the recorded material from the site system's HDD, the name of the person removing the recorded material and the date it was delivered to the Information Team.
- Ensuring recording devices are secure and only accessible to those authorised to access the data stored on the device.
- Where necessary ensuring a supply of write-only DVDs are available with every recording device.
- Ensuring system monitors are secure and only visible to those authorised to view images (advice should be sought from the Fire & Security Advisor with regards to monitors in public areas).
- Escalating any concerns to the Fire & Security Advisor.

3.11 All Staff are responsible for:

- Ensuring that effective measures are taken to ensure that the Trust premises and property are maintained in a secure condition and any shortfalls reported.
- Taking steps to safeguard against loss of the Trust property and the property of individuals as far as reasonable practicable.
- Ensure that they act in a professional manner at all times and take personal responsibility for their actions.
- Taking reasonable steps to ensure security of their own personal possessions – the Trust takes no responsibility for personal possessions except in specific circumstances where personal property is handed to staff for safekeeping.
- Reporting of any incidents or suspicious behaviour.
- Complying with Trust surveillance and information security policies and procedures. Recorded data must not be used for any purpose other than that which is legitimate under the relevant policies and procedures.
- Breaches of this Policy by Trust staff will be dealt under normal disciplinary arrangements.
- Complying with the UK GDPR and Data Protection Act requirements.

3.12 The Information Assurance Group (IAG) is responsible for:

- Oversight of this Policy and its impact within the organisation.
- Ensuring the contents of this Policy do not directly affect or have a conflict of interests with any other policy or procedure within the Trust.
- Oversight of the information assurance arrangements of this policy and receiving / agreeing the necessary assurance framework.
- Ensuring adherence to data protection and privacy requirements.
- Receiving and reviewing statistics and information access requests.
- Ensuring any necessary improvements are made.
- Escalating any matters to Audit and Risk Assurance Committee (ARAC) and Trust Board as necessary.

3.12 The Facilities Management Group is responsible for:

- Oversight and approval of surveillance camera / CCTV installations (suitable arrangements for procurement, approved installers, fit for purpose etc. in line with this Policy). See section 4.3 for further information on installation, siting etc.

4.0 KEY PRINCIPLES:

4.1 Planning of New Surveillance Systems:

Surveillance systems can be intrusive and the decision to install surveillance must be informed by a thorough assessment of the issues the system is intended to address. All schemes will be assessed for the impact upon privacy. This impact assessment process will include the Data Protection Officer (or their representative), the Estates Manager, the Risk Manager and the Fire and Security Advisor (FSA), who should collectively consider the following issues:

- The person responsible for the system and images under the Data Protection Act.
- The purpose of the system, and what issues it is going to address.
- Benefits is to be gained from its use.
- If the technology realistically deliver these benefits.
- If less privacy-intrusive solutions, such as improved lighting, signage or other environmental solutions achieve the same objective.
- Is there a need for images of identifiable individuals, or could the scheme use other images not capable of identifying the individual.
- If the system will deliver the desired benefits now, and remain suitable in the future.
- What future demands may arise for wider use of images, and how will these be addressed.
- What is required to minimise intrusion for those who may be monitored.
- If justification is clear for the new system, the FSA must produce a statement of overall security need. The FSA should carry out this work with input from other appropriate staff, and may use the resources of appropriate installation contractors under agreed HSC procurement arrangements.
- Once a system is agreed, it must be authorised by the Facilities Support Group.
- Key stakeholders should work with the FSA to ensure that the system is procured and installed in accordance with the operational requirement.

4.2 Selection of Surveillance Systems:

- It is important that the images produced by the equipment are as clear as possible so they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified; for example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose. In most cases the system selected must be capable of producing images that may be of use in the event of criminal behaviour.
- Any procurement / section must be carried out under agreed HSC procurement arrangements.
- Only companies approved by organisations such as the National Security Inspectorate (NSI) and the Security Systems and Alarms Inspectorate Board (SSAIB) will be used to supply and install CCTV / surveillance systems (examples of approving bodies, but not limited to).
- The system must have the capability of storing captured images / information for a minimum of 31 days to ensure that there is adequate time for securing information captured.
- The system must not store images / information for longer than is / would normally be necessary.
- All CCTV installations / surveillance systems must comply with the appropriate BS standards at the time of installation.

4.3 Installation & Siting of CCTV Systems / Surveillance Cameras:

- The location of the equipment will be carefully considered. The way in which images are captured will comply with data protection requirements.
- Cameras will be sited in positions which are clearly visible to service users, visitors and staff.
- To ensure privacy, cameras will operate so that they only capture images relevant to the purpose for which that particular scheme has been established and approved.
- Appropriate signs will be prominently displayed on sites and vehicles to ensure that visitors are aware that they are subject to surveillance. Signs will be clearly visible and readable, contain details of the organisation, the purpose of the system, and who to contact about the scheme (telephone number etc.).
- As far as is reasonably practicable; all cameras should be sited in positions, which will minimise their susceptibility to criminal damage.
- Except for wide angle or long distance observation, views into NIAS office accommodation shall be excluded from the field of vision of all cameras.
- Cameras will not capture any images of residential property under any circumstances

4.4 Site & Vehicle Signage – Wording:

On the outside of vehicles, the following sign is displayed:

For the safety of our staff and service users, this vehicle is fitted with CCTV. Images and audio will be recorded for health and safety and crime prevention purposes. This scheme is controlled by the Northern Ireland Ambulance Service. For further information contact 028 9040 0999

On the inside of vehicles the following sign is displayed:

For the safety of our staff and service users, this vehicle is fitted with CCTV. Images and audio will be recorded for health and safety and crime prevention purposes. This scheme is controlled by the Northern Ireland Ambulance Service. For further information contact 028 9040 0999.

Vehicles have a small LED underneath the saloon camera dome and signage advising that when the LED is illuminated, the vehicle system is recording.

The following signs are displayed at sites:

Images are being recorded and monitored for the purposes of health and safety and crime prevention. This scheme is controlled by the Northern Ireland Ambulance Service. For further information contact 028 9040 0999.

4.5 Management / Use of Surveillance Installations & Schemes:

- All faults must be reported immediately.
- A deputy should be appointed to ensure that the system continues to be managed in the absence of the local manager.
- Written local procedures must be available for each system. These include details of those authorised to export data from the system, a plan of all camera locations with camera numbers, manufacturers user guides for digital recording devices, and fault reporting procedures;
- Digital and analogue systems will have a recording device which is connected to all cameras by cable or wireless. This recording device must be secure and only accessible to those authorised to access the data stored on the device.
- A retention time of 31 days is accepted to be a reasonable period to retain data. Digital systems will overwrite data based upon the settings programmed into the recorder. In some instances, for claims or incidents the information may require being kept for longer than the 31 day accepted period. If this is the case, a full written report on the reasons for extended retention must be provided by the Data Protection Officer or their representative as soon as reasonably practicable.
- Recording devices will have an appropriate media drive to enable the exporting of images to portable media such as DVD/USB drive. A supply of write-only DVDs should be available with every recording device.
- System monitors must be secured and only visible to those authorised to view images. Where the images relate to public areas which are generally accessible and the images merely mirror what can be seen by individuals present in that area there is unlikely to be a problem if a monitor showing these images can be seen by those using the site; however, images from restricted areas must not be visible to the public.
- New and established CCTV schemes must only be modified following a thorough review and planning process. This will ensure that the scheme remains DPA compliant.

4.6 Training:

- All staff required to monitor, operate or review recorded material will be given appropriate information, instruction and training on operational use and the information governance requirements including the Data Protection Act.

- Contractors / suppliers will provide training as required by the Trust.
- Any training provided will be recorded on individual staff records.

4.7 Availability of Systems:

- Systems will be operational 24 hours a day every day of the year.
- Any fault in the system will be repaired / addressed as soon as possible.

4.8 Operation of Vehicle Based Systems:

4.8.1 Powering up and down

The vehicle system is operated from the vehicle ignition system and automatically powers up on activation of the vehicle ignition system.

While it is powered up, the external vehicle cameras will continuously record within the cameras' field of view. The internal vehicle camera will record once the alarm switches are activated on the cab or saloon switch panels or when the saloon panic strip is activated. The recording will include footage pre activation and will continue to record up to 15 minute of activation, which would not be the case if the camera had to be switched on manually.

All recordings are written to the hard disk drive (HDD) in the Digital Video Recorder (DVR). The DVR is set up to allow up to 31 days maximum (units will have a minimum of 500 GB hard drives) of recorded material to be retained (the Vehicle Retention Period), however this may vary and in some cases retention may be less or more depending upon frequency of use of the vehicle. The vehicle system automatically powers down 1 hour after the vehicle ignition is switched off.

4.8.2 Security of recorded material taken from the systems:

Only the Fleet Manager, Risk Manager, Fire & Security Advisor, Health and Safety Advisors, Investigating Officers, Driving Instructors and subject matter experts approved by the Data Protection Officer are authorised to review recorded material. In addition in relation to road traffic incidents only staff involved with the litigation process are authorised to review recorded material. They must not view or listen to any unrelated recorded material or use historical recorded material unless there is a justifiable reason to do so.

The DVR is installed in a locked cabinet within the vehicle; the cabinet is fitted with a specific security lock to restrict access. Any keys issued to authorised Trust personnel must be kept securely. All data is recorded in a proprietary format and recorded material cannot be viewed without the relevant software. This software is only issued to authorised personnel within the Fleet Department and the Information Team. Records must be kept on removal of the HDD. All HDDs which are not secured within the system must be kept secure under locked conditions.

4.8.3 Road traffic offences and collision activation:

This section covers the operational use of a vehicle's front, nearside and rear-facing surveillance camera recording facility and the surveillance camera / audio recording facility in the vehicle's saloon. Newer vehicles also have an O/S camera.

Please see sections above (system activation by vehicle ignition, recording periods, access to recorded material, DVR and key security and HDD security), which apply to the use of the system in the context of road traffic offences and collisions.

In those vehicles with an Incident Data Recorder (IDR), the IDR and vehicle system will record in tandem in the event of a road traffic offence and / or a serious road traffic collision, i.e. a collision which is outside the IDR's pre-set parameters, thus capturing evidence surrounding the lead up to the incident and ensuring that relevant evidence is preserved for investigation, insurance claims purposes and potentially production in court if required.

4.8.4 Vehicle saloon activation:

This section covers the operational use of the system within the saloon of the vehicle.

Please see sections above on system activation by vehicle ignition, recording periods, access to recorded material, DVR / key security, and HDD security above, which apply equally to the use of the system within the vehicle saloon.

Antibacterial panic strips are located in the vehicle saloon and when pressed will bookmark the recording to help identify quickly footage / audio related to adverse events that have required use of the panic strip.

If an adverse event has taken place in the vehicle saloon, the adverse event must be reported via the Trust's incident reporting system. The Fleet Manager will then take steps to retrieve the recorded material if appropriate (process under review at time of publication).

4.8.5 Process for removal of HDD from vehicles and extraction of recorded material from the removed HDD (process under review at time of publication):

The Information Team will request the HDD electronically via the Fleet Manager.

The Fleet Manager will receive and action that request. The Fleet Manager will document the date of removal of the HDD, the name of the person removing the HDD and the date it was delivered to the Information Team.

The Information Team will document receipt of the HDD, their software search of the HDD for the required recorded material and, if that recorded material is found, that it has been downloaded and saved.

The Information Team will document the date the HDD is returned to the Fleet Manager. If images / audio are extracted from the recorded material for use in legal (including Coronial) proceedings, including prospective legal proceedings, the Data Protection Officer (or their representative), will complete the relevant access and review forms, internal and external.

If the HDD needs maintenance, the Fleet Manager will record:

- a. The date and time of maintenance.
- b. The name of the person performing the maintenance.
- c. The reason for the maintenance.
- d. Type of maintenance being carried out.

- e. The outcome of the maintenance.

4.9 Operation of Site Based Systems:

The Trust currently operates surveillance systems at some of its premises (see Appendix 3). This is to protect Trust vehicles and assets and to detect and prevent crime, such as theft and other criminal activity / fraud and terrorism.

Site systems includes 24/7 surveillance cameras which record images only, not audio.

Site surveillance cameras are sited in such a way that they only monitor the areas intended. Monitors are installed and sited so that they are only accessed and viewed by authorised personnel. Staff involved in the operation of site system must only use the equipment for the purpose of maintaining the security of Trust sites and preventing / detecting crime.

Access to site system will be restricted to members of authorised Trust personnel and Trust contractors who need to undertake maintenance or repairs or need to retrieve recorded material.

Recorded material from site systems will be retained for up to a maximum of 31 days (Site Retention Period), unless it needs to be retained after that period in connection with the investigation of an alleged / actual crime or adverse event etc.

If an adverse event is reported, it will be the responsibility of the incident review panel meeting attended by relevant Trade Unions, Data Protection Officer, Risk Management and the relevant Director / Assistant Director to assess whether the site system may have captured the details of the adverse event.

4.9.1 Security of recorded material taken from site systems

Only the Data Protection Officer, the Risk Manager, the Fire & Security Advisor, Health and Safety Advisors, and investigating officers / subject matter experts approved by the Data Protection Officer are authorised to review recorded material. They will not access the recorded material unless there an adverse event is reported or as otherwise required or permitted by law. They must not view or listen to any unrelated recorded material or use historical recorded material unless there is a justifiable reason to do so in accordance with a Trust procedure and as authorised by the Data Protection Officer.

4.9.2 Records to be kept on removal of recorded material from the site system

The Data Protection Officer (or their representative), will request recorded material from the responsible manager.

The responsible manager will receive and action that request. The responsible manager will document the date of removal of the recorded material from the site system's HDD, the name of the person removing the recorded material and the date it was delivered to the Information Team.

The Information Team will document receipt of the recorded material. If images / audio are extracted from recorded material for use in legal (including Coronial) proceedings, including

prospective legal proceedings, the Data Protection Officer (or their representative), will complete the relevant access forms, internal and external.

4.10 Storing / Viewing Data & Information Recorded:

- Recorded material will be stored in a way that maintains the integrity of the information to ensure that the rights of individuals recorded by surveillance systems are protected and that the information can be used as evidence as necessary.
- The information will be stored in a secure location with restricted access and where necessary, encrypted.
- Once the information is no longer required, it will be automatically deleted with exceptions as outlined in this policy
- No information will be unnecessarily stored or kept beyond the 31 day period with exceptions as outlined in this policy
- Information and data will be recorded and stored, in a recognisable and useable format. This will allow ease of transfer if required to other agencies. Such formats will be of digital standard and transfer of information and data will not interrupt the continuous operation of the equipment installed.
- Recorded images will only be viewed following approval from the Head of Informatics, the Data Protection Officer or the Senior Responsible Officer. Authorised staff will view images in a restricted area, such as a designated secure office. Data Protection Officer.
- Editing of recorded material is prohibited other than to capture footage of a specific time frame / period and thereby to edit out unnecessary footage before or after the required time frame / period or pixelate images of third parties / remove third party audio where technically feasible. At no time should recorded material be manipulated or edited in any way that will prevent it from being reviewed in its original captured form. This includes changing colours, the date / time stamp, integrating two images into one, and so on.
- No unauthorised secondary recording of images and data is permitted under any circumstances (phone recording a monitor for example).
- Any person found recording of information or data on a secondary device will subject to investigation under the Trust Disciplinary process.

4.11 Disclosure of Information:

- Disclosure of information from any of the Trusts surveillance systems will be controlled and consistent with the purpose(s) for which the system was established.
- The date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) will be recorded by the Information Team.
- When disclosing surveillance images of individuals, consideration will be given to whether or not obscuring of identifying features is necessary or possible. Whether or not it is necessary to obscure will depend on the nature and context of the footage that is being considered for disclosure.
- Judgements about disclosure will be made by the Information Team. They have discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights. Once the information has been passed to another body, such as PSNI police, they become the data controller for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures by them.

- PSNI requests must be made using the official Form 81 under DPA stating the purpose of the request, how the material will assist investigation and how a failure to provide the information would prejudice the stated purpose. Under no circumstances should material be released without first receiving the official documentation. Under the Police and Criminal Evidence Act, PSNI may seize equipment / information if they have reasonable grounds to believe it is evidence of an offence (process under review at time of publication).
- The method of disclosing information should be secure to ensure they are only seen by the intended recipient.

4.12 Individual Subject Access Requests:

- Under UK GDPR individuals whose information is recorded have a right to view this information and unless they agree otherwise, to be provided with a copy of that information. This must be provided promptly and within no longer than 1 month of receiving a request.
- Decisions about disclosure will be made by the DPO having regard to the ICO's guidance and any relevant code of practice.
- Those who request access must provide details which allow the Trust to identify them as the subject of the information, and also to locate the information on the system.
- All individual subject requests will be logged and suitable records maintained.
- Only the Information Team are permitted to release this information after carefully considering the circumstances and nature of the request.
- The Information Team has oversight of the process for these including the following:
 - The details required to find the information (photographic evidence or a description of what they were wearing at the time they believe they were caught on the system, to aid identification etc.).
 - Date, time and location.
 - Labelling / identification of the information.
 - The secure method by which the individual will be provided with a copy of the information.
 - There will be no fee for this unless the request is manifestly unfounded, repetitive or further copies are requested.
- If the information or images captured contain third party images that are unrelated to the initial application, staff should consider obscuring the images and identity of those third-party individuals (including NIAS staff) as required by the DPA.
- Where the material requested consists of or contains health data (personal data relating to the physical or mental health of an individual, including the provision of health care services, which reveals information about his or her health status), the health data may not be disclosed in response to an access request. The Trust's Caldicott Guardian will support decision making in this area as necessary.
- Staff should seek advice and guidance from the Data Protection Officer when handling SAR requests for CCTV recordings.

4.13 Freedom of Information:

- All requests for information under the above will be dealt with on a case by case basis by the Information Team.

- If individuals are capable of being identified from the relevant surveillance system, then it is personal information being held about the individual concerned. It is generally unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the information for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the DPA.
- However, consideration can be made of the expectations of the individuals involved, what the information considered for disclosure would reveal and the legitimate public interest in the information when deciding on whether disclosure is appropriate.
- Requestors may ask for information regarding the operation of the systems, the siting of them, or the costs of using and maintaining them.
- Even where footage is exempt from FOIA/FOISA it may be lawful to provide it on a case-by-case basis without breaching the DPA, where the reason for the request is taken into account.

4.14 Handling of Information Captured:

- Any copy recordings will be placed in a sealed envelope which is signed, dated and then stored securely until the investigation is complete. Viewing of images is controlled by the Data Protection Officer or a person nominated to act on their behalf.
- Any request to view recorded data must be made through the Data Protection Officer (or their representative). Images can only be used for the purpose for which the system was intended.
- Most requests from statutory agencies such as PSNI can be dealt with during normal working hours, although there may be occasions where urgent access is sought, particularly when dealing with serious crimes. The Trust will have an emergency procedure to consider such requests.
- PSNI and others legitimately requesting access to images should never be given the original data. Copies should be made onto portable media, such as write-only DVDs and handed over against a signature. Images should not be sent by email or other networked systems (process under review at time of publication).
- There may be very rare occasions when PSNI require the original recording device, or the hard disk drives from the device. This may be necessary to safeguard forensic data following a serious incident. This will be dealt with by the Information Team.
- All media containing CCTV images must be treated as confidential waste if disposal is required.
- Misuse of CCTV equipment and unauthorised processing of data may be criminal offences under the Data Protection Act.

4.15 Retention of Recorded Material:

Recorded material will not be retained for longer than the applicable retention period unless a request has been made for it under DPA or other regime, it is required for evidential purposes in legal (including Coronial) proceedings (including any appeal, and taking into account any applicable limitation period), or it is needed to support any ongoing investigations.

Recorded material that is to be retained for longer than the retention period will be retained securely by the Information Team and clearly marked as to why it is being retained. Regular review of recorded material will be carried out by Data Protection Officer or their

representative to ensure that the recorded material is still relevant / needs to be retained. Recorded material which is no longer required is deleted / disposed of confidentially.

Recorded material that has been stored on the Trust network file storage system may be available on system backups for a period of up to 13 months. Recorded material is only to be retrieved from this location in a disaster recovery, or similar, scenario. All backups are secure, and can only be retrieved by authorised members of the Information Team. Considerations will be made on a case by case basis for retrieval requests which have a legal basis for retrieval, i.e. access requests, or an applicable warrant.

4.16 Complaints:

- Any complaints received will be managed through the Trust's complaints process with assistance from the relevant Director, local managers of the unit and advice from Information Team and Risk Management Team as appropriate.
- Complaints received about processing under the Data Protection Act will be dealt with by the Data Protection Officer (or their representative).
- Where these DPA concerns cannot be resolved by the HoI, the individual has the right to escalate the complaint to the office of the Information Commissioner (ICO).

5.0 IMPLEMENTATION OF POLICY:

5.1 Dissemination:

With regards to dissemination this procedure will be:

- Issued to all Board Members, Chair, Non-Executive Directors, Chief Executive, Directors and Assistant Directors.
- Disseminated to the required staff by Assistant Directors.
- Made available on the Internet and SharePoint so that all employees and members of the public / stakeholders can easily have access.
- Discussed during Corporate Induction.

5.2 Resources:

Information contained within this Policy will be made available to new employees at the commencement of employment, at employee induction programmes, and via information leaflets. Training on the application of this procedure for relevant managers and staff will be facilitated/delivered by the Risk Manager and Information Team as necessary.

5.3 Exceptions:

There are no staff exempt from the operation of this Policy.

6.0 MONITORING:

It is the responsibility of the Facilities Support Group to monitor associated installations and the Information Assurance Group (IAG) to monitor the implementation of and assess the level of compliance with this procedure. The Risk Management Team / Information Governance Team and Internal Audit may carry out random checks / audits (see Appendix 2).

7.0 EVIDENCE BASE/REFERENCES:

- CCTV Code of Practice 2000, Information Commissioner.
- Data Protection Act 2018
- UK General Data Protection Regulation HMSO.
- The Protection of Freedoms Act 2012
- Freedom of Information Act, 2000.
- Maintenance of CCTV surveillance systems – code of practice, 2008 - published by the British Security Industry Association.
- Equality Act 2010.
- Human Rights Act, HMSO.
- Regulation and Investigatory Powers Act 2000.
- Privacy and Electronic Communications Regulations.

8.0 CONSULTATION PROCESS:

This procedure has been developed by the Fire & Security Advisor and the Risk Manager. Consultation took place with Information Governance, Fleet, Planning, Performance and Corporate Services Directorate, Safety, Quality and Improvement Directorate, Medical Directorate, Human Resources Directorate, Emergency Planning, Trade Unions, Senior Managers, Assistant Directors and Directors within the organisation. The final content of the document was agreed at the Information Assurance Group, Senior Management Team and Audit and Risk Assurance Committee (ARAC).

9.0 APPENDICES:

Appendix 1 – Request For Copy Of Recorded Information.

Appendix 2 – CCTV Policy Audit Tool.

Appendix 3 – Full List Of Current CCTV Installations.


10.0 EQUALITY STATEMENT:

10.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise, to ascertain if this Policy should be subject to a full impact assessment, has been carried out.


10.2 The outcome of the equality screening for this procedure undertaken on 5th January 2023 is:

Major impact	<input type="checkbox"/>
Minor impact	<input type="checkbox"/>
No impact.	<input checked="" type="checkbox"/>

11.0 SIGNATORIES:


Lead Author

Date: 30th March 2023


Lead Director

Date: 30th March 2023

APPENDIX 1 – REQUEST FOR DISCLOSURE OF PERSONAL DATA FROM CCTV:

Disclosure Request Details
1.1 Site / location / vehicle from which data is required:
1.2 Timescale within which the information is required: CCTV footage is required between the hours of [enter start time and end time] on the [enter date] from camera(s) located in / at [enter details of the location or specific detail required], [delete 2nd camera details if not required] and the camera covering [enter details of the location or specific detail required] add additional camera locations if required.
1.3 Please provide as much detail as possible as to the specific reason for access (be as specific as you can to enable identification of the correct data):
1.4 How would you like to receive any evidence found: <input type="checkbox"/> View only <input type="checkbox"/> Hard copy / disk of video images of subject and actions <input type="checkbox"/> Single frame of a subject

Requestor Information – Signature & Counter Signature:	
Signed by Requester:	
Name of Requester:	
Job Title:	
Countersigned by Line Manager:	
Name of Counter Signature:	
Job Title of Counter Signature:	

FORM TO BE RETURNED TO THE INFORMATION GOVERNANCE TEAM
informatics.department@nias.hscni.net

To be completed by the Information Governance Team

Information Governance Team:	
Request Granted	Request Denied (provide reason)
Name:	Name:
Position:	Position:
Date:	Date:

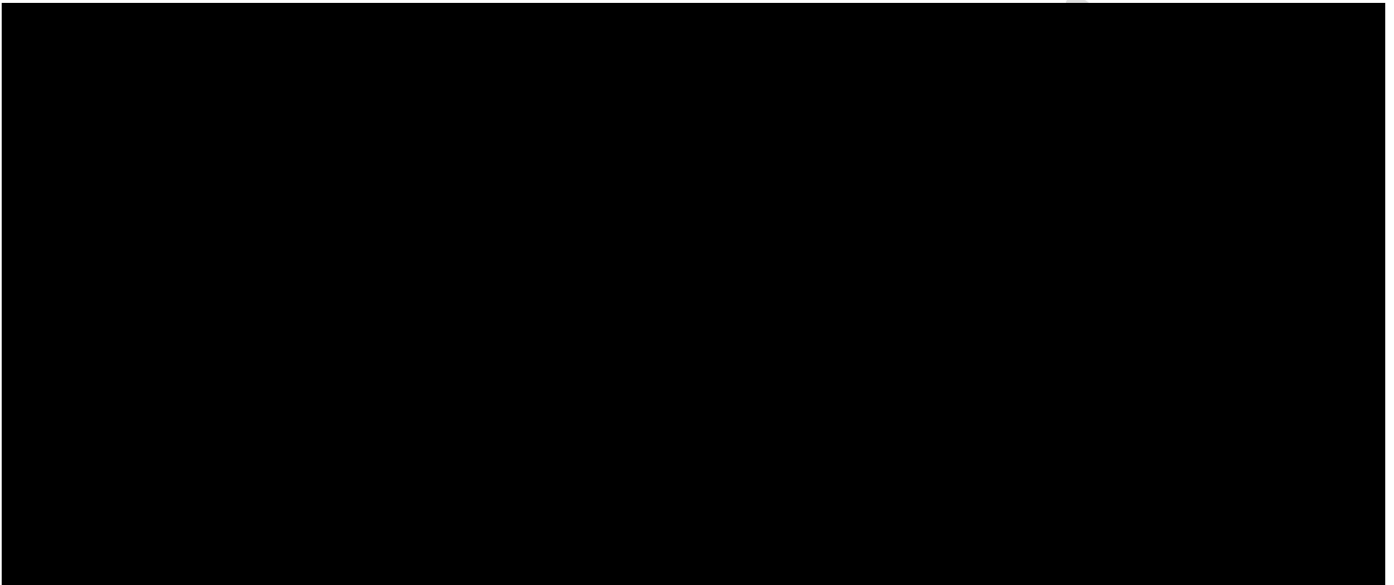
To be completed by the Requestor on receipt of information

Requestor:	
Requester Name:	
Job Title:	
Sign (acknowledge receipt of information):	
Date:	

APPENDIX 2 – CCTV POLICY AUDIT TOOL:

Directorate: Auditor: Address:		Date of Audit:		
		YES	NO	COMMENTS
1	Is access to the CCTV control area restricted to all but authorised personnel?			
2	Is the CCTV Control Room Key Register completed when access is requested to the CCTV control room?			
3	Are the correct procedures followed for persons requesting to view and/or record CCTV images?			
4	Is the CCTV Control Room Access Register completed when persons request to view and/or record CCTV images?			
5	Is all CCTV footage disposed of appropriately?			
6	Are all cameras situated so they can only monitor the intended area of coverage and not positioned anywhere that would be considered private e.g. office or toilet?			
7	Are signs in place showing that CCTV systems are in operation?			
8	Have cameras been positioned to avoid capturing the images of persons not visiting the premises?			
9	Is a procedure in place for operational equipment to be checked regularly and maintained to ensure it is in good working order?			
10	Has a review of incidents involving CCTV systems been reviewed and analyses to identify trends and high risk incidents?			

APPENDIX 3 – LIST OF CURRENT CCTV INSTALLATIONS:



DRAFT intended for future publication