Northern Ireland Ambulance Service
Health and Social Care Trust

DATA PROTECTION ACT 1998 POLICY STATEMENT

Title:	Data Protection Act 1998 Policy Statement		
Purpose of Policy:	To ensure that Trust staff understand the principles of the Data Protection Act and their responsibilities under the Act.		
Directorate Responsible for Policy:	Finance and IT Directorate		
Name and Title of Author:	Miss Alison Vitty, Corporate Manager		
Staff Side Consultation	YES (via HR Joint Consultative Group 9 April 2009)		
Equality Screened:	YES		
Date Presented to:	ICT Committee	9 February 2009	
	Trust Board	7 May 2009	
	Comments	**APPROVED**	
Publication Date:	June 2009 (v1) March 2012 (v2) March 2016 (v3)	Review:	October 2016
Version:	NIAS/TW/IG/1(v2)		
(01) June 2009	No previous document to supersede.		
(02) March 2012	Updated in line with DHSSPS Guidance – DPA Policy Statement		
(03) March 2016	Reviewed. No updates made at this time. Further review to be carried out later in year.		

Circulation List:

This Policy has been circulated to the following groups for consultation:

- Staffside
- Executive Directors and Senior Managers

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff
- Trust Internet/Intranet Site

Data Protection 1998 Policy

1.0 Policy Statement

1.1 The Northern Ireland Ambulance Service (the Trust) regards the lawful and correct treatment of personal and sensitive data as an integral part of its functions and vital for maintaining confidence between patients, clients and staff whom we process information about and ourselves.

1.2 The Data Protection Act 1998, which became effective from 1 March 2000, gives every living person (or their authorised representative) the right to apply for access to their records, irrespective of when and how they were compiled, i.e. electronic and manual records.

1.3 The Freedom of Information Act 2000 (FOI) extends the release of unstructured information to third party requests, for example e-mails, diaries, notepads etc. However, access to all personal data (under the Data Protection Act 1998) is an absolute exemption under the Freedom of Information Act 2000.

1.4 Applications for access to records of the deceased are made under the Access to Health Records (NI) Order 1993. Records made after 1 November 1991 can be made available to a patient representative, executor or administrator. Claimants for compensation are entitled only to access information specifically relating to the claim.

1.5 Under the Data Protection Act 1998, former patients now living outside the United Kingdom (UK) have the same rights to apply for access to their UK records. A request for access to records will be treated in the same way as a request made from within the UK.

1.6 Informal, voluntary arrangements exist to allow service users either during, or, at the end of their treatment/consultation to have access to what has been recorded about them. These arrangements are at the discretion of the health/social care professional (the Data Processor) principally responsible for their care and support. The above arrangements are subject to the non-disclosure of information that might cause serious harm or, identify a third party.

1.7 This Policy also facilitates the use of a formal process to seek access to such records, allowing that the appropriate health/ social care professional may exercise their professional judgement in determining the extent of their service users' access.

1.8 A Common Law Duty of Confidentiality exists with respect to health care professionals and service users.

2.0 Definitions

2.1 Personal information/data relates to a living individual who can be identified from the information. This includes:

- Factual information;
- Expressions of opinion about the individual;
- Indication of the intentions of the Data Processor e.g. health/social care professionals; or
- Any other person in relation to the individual concerned.

2.2 Sensitive personal information/data attracts additional protection and is further defined in the Act to mean personal data consisting of information such as:

- Racial or ethnic origin of the data subject;
- His/her political opinions;
- His/her religious beliefs or other beliefs of a similar nature;
- Whether he/she is a member of the trade union;
- His/her physical or mental health or condition;
- His/her sexual life;
- The commission or alleged commission by him/her of any offence; or;
- Any proceeding for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings and the sentence of court in such proceedings.

Sensitive personal data must not be processed other than in limited circumstances that are described in the Data Protection principles; "personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) At least one of the conditions in Schedule 2 is met, and
(b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

(Refer to definition in glossary for conditions attached to processing personal and sensitive personal information – Schedules 2 and 3).

2.3 A record can be in computerised and/or manual form. It may include such documentation as:

- Hand written notes;
- Letters to and from other health/social care professionals;
- Patient Report Forms;
- C3 Electronic records;
- Printouts;
- Photographs;
- Videos and tape recordings.

2.4 Within the Data Protection Act 1998, a "health and social care record" is defined as a record consisting of information about the physical or mental health, or condition of an identifiable individual, made by, or on behalf of, a "health professional", in connection with the care of that individual. This takes the form of a Patient Report Form completed by a Paramedic or Emergency Medical Technician involved in the care of the patient, as well as the electronic record of the clinical details obtained during the emergency call.

3.0 Purpose and Aims

The purpose and aims of this policy are to:

- Provide a framework for the legal, secure and confidential management of information;
- Ensure the utmost protection of information for patients, service users and staff in compliance with current legislation;
- Identity how the Trust executes its duty to keep patient, client and staff information safe and confidential, whilst at the same time not comprising its ability to share information when needed.

On a daily basis, the Trust deals with personal and sensitive information about patients, clients and staff. In order to work effectively, the Trust must establish and maintain a strong relationship of trust between its patients, clients and staff. As shared practice amongst organisations and agencies increases, so does the risk of problem with misrouting, misinterpreting and possibly misusing sensitive information and it is therefore of paramount importance that standards of confidentiality form the core of this relationship of trust.

4.0 Policy Statement

We need to collect and use information about people with whom we work in order to carry out our business and provide our services. These may include members of the public, current, past and prospective employee and suppliers. In addition, we may be required by Law to collect and use information. All personal information, whether in paper, electronic or any other format, must be handled in accordance with DPA.

The main focus of this policy is on providing guidance in relation to the protection, sharing and disclosure of patient/client/staff information, but it is important to stress that maintaining confidentiality and adhering to data protection legislation applies to all staff and departments within the Trust. To this end, the Trust fully endorses and abides by the principles of data protection. In summary, this means personal information must be:

(i) Processed fairly and lawfully;
(ii) Processed for limited purposes and in an appropriate way;
(iii) Relevant and sufficient for the purpose;
(iv) Accurate;

(v) Kept for long as necessary and no longer;
(vi) Processed in line with individuals' rights;
(vii) Secure;
(viii) Only transferred to other countries that have suitable data protection controls.

Therefore the Trust will, through appropriate management, and strict application of criteria and controls:

(a) Observe fully the conditions regarding the fair collection and use of information;
(b) Meet its legal obligations to specify the purposes for which information is used;
(c) Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
(d) Ensure the quality of information used;
(e) Apply strict checks to determine the length of time information is held;
(f) Ensure that the rights of people about whom information is held can be fully exercised under the DPA: and
(g) Ensure staff are appropriately trained.

These "rights" include:

(h) The right to be informed that processing is being undertaken:
(i) The right of access to one's personal information;
(j) The right to prevent processing in certain circumstances;
(k) The right to correct, rectify, block or erase information which is regarded as wrong information;
(l) Take appropriate technical and organisational security measures to safeguard personal information;
(m) Ensure that personal information is not transferred abroad without suitable safeguards.

4.2 In addition, the Trust will ensure that:

(a) There is a member of staff with specific responsibility for data protection in the organisation (the Corporate Manager is accountable to the Director of Finance and IT for the co-ordination and management of DPA);
(b) Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
(c) Everyone managing and handling personal information is appropriately trained to do so;
(d) Everyone managing and handling personal information is appropriately supervised;
(e) Anyone wanting to make enquiries about handling personal information knows what to do;

(f) Queries about the handling of personal information are promptly and courteously dealt with;

(g) Methods of handling personal information are clearly described;
(h) A regular review and audit is made of the way personal information is managed;
(i) Methods of handling personal information are regularly assessed and evaluated;
(j) Regular assessments of Trust compliance with the DPA 1998 will take place.

4.3 Rights of Access by Individuals

(a) Under the Data Protection Act 1998, any living person, who is the subject of personal Information held and processed by the Trust, has a right to apply for access to that information. This is known as a subject access request.

(b) An individual does not have the right to access information recorded about someone else, unless they are an authorised representative.

(c) It is important that the Data Processor (refer to Annex A) ensures that third party information is removed from the record prior to release to the applicant unless the third party has given their consent to the release of the information.

4.4 Denial of Access

Access can be refused if the Trust has previously complied with an identical or similar request in relation to the same individual, unless a reasonable interval has elapsed between compliance with one request and the receipt of another.

There are a number of other instances when the Trust may refuse access.

4.4.1 Access to all or part of a record will be denied if:-

(a) In the opinion of the relevant health/social care professional the information to be disclosed would be likely to cause serious harm to the physical or mental health of the applicant or any other person.
(b) The obligation to consult does not apply where the data subject has already seen or knows about the information that is the subject of the request, nor in certain limited circumstances where consultation has occurred prior to the request being made.

4.4.2 In addition, the Data Protection (Subject Access Modification) (Health) Order 2000 states that access may be denied in circumstances where:-

(a) The granting of access to a patient representative would disclose information, provided by the patient in the expectation that it would not be disclosed, to the person making the request;

(b) The granting of access would disclose information obtained as a result of any examination or investigation to which the patient consented, in the expectation that the information would not be so disclosed to another individual;
(c) The patient has expressly indicated that such information should not be disclosed to another individual.

4.4.3 Notification of refusal to grant access will be given as soon as possible, in writing. The Trust will record the reason for this decision, and will also fully explain the reason to the applicant.

4.4.4 Even if the Trust is aware that the applicant has received a copy of the information from another source, it must provide a copy of the information if held.

4.5 **Exemptions**

If the release of personal data would reveal information, which related to and identified another person (third party) for example, where a relative has provided certain information, this information will be withheld unless consent from the individual is obtained. (Third party information does not apply to health professionals, however refer below).

If the release of personal data is likely to cause serious harm to the data subject's physical or mental health or of any other person (which may include a health professional), this information will be withheld on the advice of the health professional responsible for care. (Refer to Data Protection (Subject Access Modification) (Health) Order 2000)

Where the request for access is made by a service user/member of the public on behalf of another data subject, such as parent for a child, access can be refused, if the data subject had either provided the information in the expectation that it would not be disclosed to the applicant or had indicated it should not be disclosed, or if the data was obtained as a result of any examination or test to which the data subject consented on the basis that information would not be disclosed.

There is an exemption in the Data Protection Act 1998 that allows personal information to be disclosed for the purposes of preventing or detecting fraud and for attempting to secure the apprehension of offenders (Section 29 – Crime and Taxation), but there are limits on what can be released. The Trust release information to PSNI, the Police Ombudsman and Historical Enquiries under this domain.

5.0 Scope of the Policy

The scope of this policy extends to:

- Corporate and administrative records
- Human Resource records
- Financial Records
- Medical/clinical records e.g Patient Report Forms
- Call detail documents created via C3
- Resource Management Centre
- Health and social care records

5.1 Deceased Patients Health Records

Where the patient has died, access to the health records can be made under the Access to Health Records (NI) Order 1993. The patient's personal representative and any person who may have a claim arising out of the patient's death has the right to apply under this Act.

6.0 Roles and Responsibility

The Trust has a duty to ensure that the requirements of the Data Protection Act 1998 are upheld.

6.1 Responsibility of Chief Executive

The Trust's Chief Executive as "Accountable Officer" has overall responsibility for Data Protection within the Trust.

6.2 Director of Finance and Information Technology

The Chief Executive has nominated the Director of Finance to ensure that the Trust complies with the requirements of the legislation.

6.3 Personal Data Guardian

The Personal Data Guardian has responsibility for safeguarding confidentiality of data flows. The Trust's Personal Data Guardian is the Medical Director.

6.4 Data Protection Officer

The Corporate Manager has been appointed to the post of Data Protection Officer. Responsibilities include:

- Ensuring compliance with legislation principles;
- Progressing the Data Protection Action Plan;
- Ensuring notification of processing of personal data to the Information Commissioner is up to date;
- Providing guidance and advice to staff in relation to compliance with legislative requirements;

- Reporting via the Untoward Incident Reporting process on any breaches of Data Protection legislation.

6.5 **Data Owners/Information Asset Owners**

Directors, Assistant Directors and Seniors Managers are responsible for information held manually and electronically within the Directorate areas and for development of procedures in relation to same. As Data Owners their responsibilities include:

- Informing the Data Protection Co-ordinator of any changes in the processing of personal data;
- Identifying and justifying how sets of data are used;
- Identifying all personal data for which they are responsible and;
- Agreeing who can have access to the data.

6.6 **All Staff**

Maintaining confidentiality and adhering to data protection legislation applies to all staff and Directorates within the Trust. The Trust will take all necessary steps to ensure that everyone managing and processing personal data understands that they are contractually responsible for following good data protection practice and where appropriate, bound by a common law duty of confidence.

These responsibilities and common law duties apply equally to all transient staff including trainees, secondees and professional advisors.
Further responsibilities include:

- Observing all guidance and codes of conduct in relation to obtaining, using and disclosing personal data;
- Observe all information sharing protocols in relation to the disclosure of information to provide care for individuals;
- Obtaining and processing personal information only for specified purposes;
- Only accessing personal information that is specifically required to carry out their work;
- Recording information correctly in both manual and electronic records;
- Ensuring any personal information that is held is kept secure;
- Ensuring that personal data is not disclosed in any form to any unauthorised third party.

Failure to adhere to any guidance in this policy could result in staff being personally liable under the Data Protection Act 1998 and may also result in disciplinary action.

7.0 Relevant Policies, Procedures and Guidance – Legislative Framework

Staff must comply with relevant legislation, professional standards and guidance and other DHSSPS publications as follows:

- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order (Northern Ireland) 1925
- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records (NI) Order 1993
- Human Rights Act 1998
- Computer Misuse Act 1990
- The Common Law Duty of Confidentiality
- Data Protection (Subject Access Modification) (Health) Order 2000
- Data Protection (Subject Access Modification) (Social Work) Order 2000
- DHSSPS Code of Practice – Confidenality of Service User Information (2012)
- Guidance on Caldicott Principles
- Good Management, Good Records – DHSSPS, 2004
- Northern Ireland Records Management Standard (PRONI)
- Controls Assurance Standard

8.0 Equality and Human Rights Consideration

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998. The Equality Commission for Northern Ireland Guidance states that the purpose of screening is to identify those policies which are likely to have a significant impact on equality of opportunity so that greatest resources can be devote to those.

Following screening, no significant equality implications have been identified. The policy will therefore not be subject to an equality impact assessment.

9.0 Review of Policy

This policy will be reviewed in three years from the date of issue or as required with legislative or good practice recommendations.

_____

Liam McIvor
CHIEF EXECUTIVE

Annex A

DATA PROTECTION – GLOSSARY OF TERMS

Data	Information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose e.g a computer or (b) is recorded as part of a relevant filing system
Personal Data	Data which relates to a living individual who can be identified from the data itself or in conjuction with other data held by the Data Controller. This includes any expression of opinion about the individual and any indication of the intentions of the Data Controller in respect of the individual.
Sensitive Personal Data	Personal data consisting of information as to: - The racial or ethnic origin of the data subject - Political opinions; - Religious beliefs; - Membership of a Trade Union; - Sexual Life; - The commission or alleged commission of any offence - Any proceedings for any offence committed or alleged to have been committed
Data Controller	The person who is responsible for the manner in which any personal data is processed. The Northern Ireland Ambulance Service is the Data Controller. Individual members of staff who process data on behalf of the Trust are data users.
Data Processor	A person or organisation that processes data on behalf of the Data Controller (other than an employee of the Data Controller)
Data Subject	An identifiable individual who is the subject of personal data.
Health and Social Care Professional	Includes a registered medical practitioner, a registered nurse or midwife and professions allied to medicine eg Paramedics, Emergency Medical Technicians
Health Record	Any record which consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health profession in connection with the care of that individual e.g Patient Report Form

Processing	Obtaining, recording or holding the data or carrying out any operation on the data, including – organising, adapting, or alteration of the data, retrieval, consultation or use of the data, disclosure of the data, blocking, erasure, or destruction of the data
Information Commissioner Office	The Information Commissioner's Office is the UK's independent authority set up to promote access to official information and to protect personal information
Information Note	A written request from the Information Commissioner to a Data Controller seeking to determine whether or not a Data Controller has failed to comply with the Data Protection Act. Failure to comply with such a notice is an offence.
Notification	Notification is the process by which a Data Controller's processing details are added to a register. Under the Data Protection Act every Data Controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. The Commissioner maintains a public register of Data Controllers available at www.ico.gov.uk. A register entry only shows what a Data Controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.
Subject Access	Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data. A subject access request must be made in writing and must be accompanied by the appropriate fee. In most cases, the maximum fee will be £10. A request must include enough information to enable the person or organisation to whom the subject is writing to satisfy itself as to their identity and to find the information. A reply must be received within 40 days as long as the necessary fee has been paid. A Data Controller should act promptly in requesting the fee or any further information necessary to fulfil the request. If a Data Controller is not processing personal information of which this individual is the data subject, the data controller must reply saying so.
Relevant Filing System	Any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically, the set is structured either by reference to individuals or reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible