



<b>1.0 Title:</b>	<b>RECORDS MANAGEMENT POLICY</b>		
<b>2.0 Author(s)</b>	Alison Vitty, Corporate Manager		
<b>3.0 Ownership:</b>	Finance and ICT Directorate		
<b>4.0 Date of SEMT Approval:</b>		<b>5.0 Date of Trust Board Approval:</b>	June 2009
<b>6.0 Operational Date:</b>	16/03/2016	<b>7.0 Review Date:</b>	February 2018
<b>Version No:</b>	NIAS/TW/IG/3 Version 0.3	<b>Supersedes:</b>	June 2009 v1 March 2012 v 3
<b>8.0 Key words:</b>	Information Governance		
<b>9.0 Other Relevant Policies:</b>	<ul style="list-style-type: none"> <li>- Records Management Strategy 2015 – 2020</li> <li>- Retention and Disposal Schedule</li> <li>- Information Governance Strategy 2015-2018</li> <li>- Information Risk Policy</li> <li>- Freedom of Information Act 2000 and Environmental Information Regulations 2004</li> <li>- Data Protection Act 1998 Policy</li> <li>- Code of Practice on Confidentiality of Service User Information</li> </ul>		

<b>Version Control for Drafts:</b>			
<b>Date</b>	<b>Version</b>	<b>Author</b>	<b>Comments</b>
June 2009	v0.1	AV	No previous document to supersede. Due for review in June 2011. Reviewed in March 2012.
March 2012	v0.2	AV	Reviewed – no updates required. Trust has adopted Part 1 and Part 2 of DHSSPS Good Records, Good Management
February 2016	v.0.3	AV	Records Management Strategy 2015-2020 developed. Updates provided to reflect new IG policies roles ie SIRO/IAOs etc. 16/03/2016 – IGSG reviewed changes. Noted. For release on intranet

## 1.0 **RECORDS MANAGEMENT POLICY**

### 1.1 **Introduction**

The Northern Ireland Ambulance Service (NIAS) recognises that the efficient management of its records is necessary to support its core functions, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust. This document provides the policy framework through which this effective management can be achieved and audited.

The Trust faces pressure to demonstrate legal compliance and high standards of corporate governance.

An effective Records Management Programme is the foundation on which NIAS can build its responses to these growing demands. The Data Protection Act 1998 and the Freedom of Information Act 2000 require that NIAS can identify, locate or account for the disposal of documents in relation to data subject access and Freedom of Information enquiries. Both Acts require that NIAS should publish and implement policies in relation to the disposal of records, while efficient management and best use of resources mean that NIAS should be able to fulfil these requirements quickly and economically.

The NIAS recognises that records are an important corporate asset as they are a key resource for effective operation and accountability. They therefore require proper management throughout their life from creation to disposal and with due regard to legal obligations, professional practice and the Trust's business needs. All public authorities must ensure that records management policies and procedures are fully compliant with legislation and recognised good practice on the management of information. These are:

- Access to Health Records (NI) Order 1993
- Adoption Order (NI) 1987
- Audit Commission Report (NIAO) Compensation Payments for Clinical Negligence 2002
- The Caldicott Report (England)
- The Children's Order (NI) 1995
- Controls Assurance Standards
- Data Protection Act 1998
- Freedom of Information Act 2000 and Environmental Information Regulations (2005)
- Good Management, Good Records – HPSS
- Human Rights Act 2000

- Information Regulations 2005
- Information for Health
- Mental Health Order (NI) 1986
- Public Records Act (NI) 1923
- Regulation of Investigatory Powers Act 2000

A brief description of the legislation requirements are outlined in Appendix 1 of this policy.

This policy gives the basis for good records managements and also forms the foundation of the Trust's Record's Management Strategy.

## 1.2 **Policy Statement**

It is the policy of the Trust, that authentic, reliable and reusable records are created which are capable of supporting business functions and activities for as long as they are required. Adherence to this policy will ensure consistency and conformity of approach. This policy applies to all records of the Trust, and will be achieved by creating a procedural framework, which will ensure that:

- Records are made accessible to enable well-informed and proper judgements to be made;
- Records are kept securely and protected from accidental loss, destruction and unauthorised access;
- Records are kept no longer than is necessary, in accordance with legal and professional obligations and with due regard to the Trust's Records Retention and Disposal Schedule;
- Members and employees are made aware of and trained in management of records within their sphere of work or responsibility.

We will seek to comply with all relevant legislation and aim to achieve standards of best practice.

## 1.3 **Why do we need a Policy?**

The Lord Chancellor's Code of Practice on the management of records, which can be found under Section 46 of the Freedom of Information Act, requires the Trust to have in place a policy statement endorsed by Senior Management and made readily available to staff at all level in the Trust on how it manages its paper and electronic records.

## 1.4 **Purpose and Scope of the Policy**

The purpose of this Policy is to ensure that records are managed effectively throughout NIAS and with due regard to specified legislation, professional principles and guidelines.

This policy applies to all records created, received or maintained by staff in the Trust in course of carrying out their duties.

Compliance with this policy will ensure that the Trust can provide evidence of performance and demonstrate accountability, as well as providing information about its decisions and activities.

In the context of this Policy a record is any recorded information that contains information, electronic or in paper, in any media which is created, collected, processed, used, stored and/or disposed of by NIAS employees, as well as those acting as its agents in the course of NIAS business. The Policy applies to health and social services records as well as corporate records.

This policy applies to all members, Directors and employees of Northern Ireland Ambulance Service HSC Trust. Non-compliance with this policy may result in disciplinary action by the Trust or legal action by others.

### 1.4.1 **What does this Policy apply to?**

This Policy and the standards that go with it, apply to the management of records, in all technical or physical formats or media, created or received by NIAS while carrying out its business activities.

Although not an exhaustive list, examples of items that can be records include:

- Documents (including written and typed documents, databases, spreadsheets and presentations);
- Paper based files;
- Computer files (including word processed documents, databases, spreadsheets and presentations);
- Electronic mail messages;
- Diaries;
- Faxes;
- Brochures and reports;

- Internet and intranet pages;
  
- Forms;
- Maps and plans;
- Photographs.

## 2.0 **RESPONSIBILITY FOR TRUST RECORDS**

This Policy and associated standards that go with it, apply to all permanent and temporary employees, contractors, consultants and secondees who have access to NIAS records, wherever these records are and whatever form they are in.

### 2.1 **Managerial Responsibility**

#### 2.1.1 **Trust Board**

The role of the Trust Board is to oversee the effective records management by Officers of the Trust.

#### 2.1.2 **The Chief Executive and Directors**

The Chief Executive and Directors are personally accountable for the quality of records management within the Trust and have a duty to make arrangements for the safekeeping and eventual disposal of those records under the overall supervision of the Deputy Keeper of Public Records, Northern Ireland.

#### 2.1.3 **Senior Information Risk Owner (Finance and ICT Director)**

The SIRO is responsible for ensuring that there is a managerial focus for records of all types, in all formats, including electronic records, throughout their life-cycle from planning and creating through to disposal.

#### 2.1.4 **Caldicott Guardian**

The Caldicott Guardian has a particular responsibility for safeguarding patients' interests regarding the use of personal identifiable information.

The Trust's Caldicott Guardian is the Medical Director

### 2.1.5 **Corporate Manager**

The Corporate Manager is accountable to the Director of Finance and IT for the co-ordination and management of records held within the Trust and is the lead Officer for records management on a day to day basis. Responsibilities include:

- Co-ordinating, publicising and monitoring implementation of the records management strategy and reporting on a regular basis to the Senior Management Team.
- Determining the type of system appropriate to allow effective and efficient discharge of functions while meeting the statutory duty of records management;
- Ensuring that the systems in place for records management are monitored and reviewed by the Senior Management Team and the Board at least annually in order to make improvements to the system;
- Promotion of and overseeing of records management strategy;
- Ensuring that records management functions are supported in their work in terms of commitment and resources;
- Providing advice and support of the records management strategy, policy, framework and processes;
- Providing training in Records Management, Freedom of Information, Data Protection and Environmental Information;
- Providing advice on appropriate low cost storage for Departmental records;
- Developing procedures for the permanent preservation of selected records with the Public Records Office, Northern Ireland;
- Co-ordinating requests for information in compliance with Data Protection and Freedom of Information legislation;
- Undertaking information audits to develop appropriate retention schedules and classification schemes;
- Providing the Trust, in accordance with the Governance framework, details of records management process to enable internal controls to be monitored.

### 2.1.6 **Information Asset Owners (IAOs)/Senior Managers**

The role of Information Asset Owners/Senior Managers is to ensure that records are managed effectively in each Directorate area in accordance with the Trust's Records Management Policy (this document).

IAOs and Senior Managers are responsible for ensuring staff are aware of the appropriate records management policies and procedures and that they have been trained in the operational procedures required by the Trust.

Responsibilities include:

- Ensuring that appropriate employees are designated to assist with the implementation of records management procedures within the Directorate;
- Ensuring that employees are supported in terms of training and development in their adherence to the Records Management Policy and procedures;
- Ensuring the personal information (eg about a patient/member of staff) is not kept longer than necessary. Information about individual patients may not be passed onto others without the individuals consent except as permitted under Schedule 2 and 3 of the Data Protection Act 1998.
- Ensuring that an inventory of corporate records is maintained which shows the nature and types of records within Directorate function and is accessible to users and indicates the specific retention periods for those records;
- Ensuring that anyone who records, handles, stores or otherwise comes across patient information is aware that they may have a common law duty of confidence to patients. Such a duty will continue even after the death of a patient.

### **2.1.7 Individual Responsibility**

All Trust employees, whether operational, control or administrative based are responsible for any records which they create or use in the performance of their duties. They are responsible for documenting their actions and decisions in the records and for maintaining the records in accordance with good records management practice and professional guidelines.

This responsibility is established at, and defined by the Law eg Public Records Act, Data Protection Act 1998 and other professional guidelines covering the handling for public records. Therefore everyone working for or with the Trust who records, handles, stores or otherwise comes across patient information (eg Patient Report Form, C3 records, Human Resource records), has a personal common law duty of confidence to patients and to NIAS.



The duty of confidence continues, even after the death of the patient or after an employee or contractor has left the Trust or HSC body.

Individuals need to ensure that:

- The record can be assessed;
- The record can be interpreted;
- It is possible to establish who created the document, during which operational process and how it relates to other records;
- The record can be trusted;
- The record can be maintained through time;
- The record is accessible and meaningful, in the right format, to those who need to use it;
- There is no unnecessary duplication between the paper and electronic record collections;
- A file management system is also used for electronic records;
- There is no distinction made between the electronic documents that are printed, printed records that reside in manual record systems and other original documents that are retained as records.

### 3.0 **DEVELOPMENT AND MANGEMENT OF RECORDS WITHIN THE TRUST**

#### 3.1 **Record Keeping**

Records of all types are valuable because of the information they contain and that information is only useful if it is:

- Correctly and legibly recorded in the first place;
- Is kept up to date;
- Is easily accessible when needed.

To ensure quality and continuity of services all records should be accurate and kept up to date. Procedures should be developed to ensure and maintain data quality for both manual and electronic records. These procedures should be passed on to staff who are responsible for producing such information. It is also essential that these procedures are reviewed and updated regularly.

## 3.2 **Creation of Records**

Records are created so that information is available in the Trust to:

- Deliver the services offered by the Trust to the community of Northern Ireland;
- Ensure that appropriate records are kept of the operation of the Trust business and are correctly identified and managed;
- Support day to day business, which underpins decision-making and the delivery and continuity of care;
- Support evidence based practice;
- Meet legal requirements including requests under the Data Protection Act 1998, Access to Health Records (NI) Order 1992, requests for information under the Freedom of Information Act 2000 and Environmental Information (Amendment) Regulations 1998;
- Support in the auditing process;
- Support improvement in clinical effectiveness through research and also to support archival function by taking account of the historical importance of material and the need for future research;
- Ensure whenever, and wherever there is justified need for records to be created for use in the Trust, community and wider public it is done effectively and in line with appropriate legal requirements and recognised good practice;
- Assist the staff in defending any legal claims against it or its staff.

### 3.2.1 **Records Standards**

A record should correctly reflect what was communicated or decided or what action was taken. It should also be able to support the needs of (have a useful purpose in) the business to which it relates and be used for accountability purposes. For example, minutes should provide an accurate record of the decisions taken at a meeting.

Records management procedures and practices should result in records which have authenticity, integrity and usability.

Emails are often regarded as an informal or short lived form of communication. This misconception about how email can be used could result in legal action being taken against NIAS or individual staff. You should treat emails in the same way as you would treat any other form of communication that can be recorded. You should type or write them as if someone else was looking over your shoulder.

The importance of this is emphasised by the fact that emails are subject to Data Protection and Freedom of Information legislation and can also form part of the corporate record. Staff should be aware that emails could be used as evidence in legal proceedings and may be released to the public in response to a FOI request.

It is the responsibility of all members of staff to manage their emails appropriately in order to comply with Data Protection and Freedom of Information legislation.

To manage emails appropriately, staff must identify those which are records of their business activities and those which are not.

- Emails that might constitute a record are likely to contain information relating to business transactions that have or going to take place, decisions in relation to the business activity or any discussion that took place in relation to the activity.
- Emails regarded as short lived contain no information relating to business activities eg arranging a date for a meeting, receipt for attendance at a meeting.

It is important that emails are identified as records are moved from personal email boxes eg inbox, sent box or folders created under an inbox and managed in the same way as other records. To prevent loss of valuable information, emails messages must be acted upon and moved to the central filepath as quickly as possible.

Under the Freedom of Information Act 2000 is it a criminal offence for any member of staff to deliberately and knowingly destroy information (including emails) under the Control of the Trust which is required for the purpose of disclosure pursuant to a pending application seeking such information. Destruction of such information under these terms may lead to criminal prosecution of the individual responsible for the destruction of the information.

### 3.2.2 **Health Care Records**

The purpose of the clinical record ie Patient Report Form is to facilitate the care, treatment and support of a particular client.

Patient and client records should be:

- Factual;
- Consistent and accurate;
- Written clearly, legibly and in such a manner that cannot be erased. Erasers, liquid paper or any other obliterating agents should never be used to cancel errors. A single line should be used to cross out and cancel mistakes or errors and this should be signed and dated by the person who has made the amendment.
- Accurately dated, time and signed.
- All handwritten entries will be in permanent ink;
- No inappropriate personal or offensive comments should be included.

Patient records should not include:

- Unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation and offensive subjective statements;
- Personal opinions regarding the patient (restrict to professional judgements on clinical matters).

Relevant staff should also refer to the Trust's Policy and Procedure for Completion of Patient Report Forms for further guidance and information.

### 3.2.3 **Records in Transit**

If records are being delivered to another location they should be enclosed in envelopes and sealed for transfer. Any records that may be damaged in transit should be enclosed in suitable padding or containers.

Each box or envelope should be addressed clearly and marked confidential with the senders name and address on the reverse.

There are various options if records are to be mailed such as recorded delivery, registered mail etc. When considering options staff should consider the following:

- Will the records be protected from damage, unauthorised access or theft?
- Is the level of security offered appropriate to the degree of importance, sensitivity or confidentiality?
- Does the mail provided offer "track and trace" options and is a signature required on the delivery?

The records must not be left unattended in transit at any time. When carried in a car, they must be locked in the boot.

### 3.2.4 **Handing and Transporting Records**

- Staff should avoid eating, drinking or smoking near records.
- Records should be handled carefully when being loaded, transported or unloaded.
- Records should **never** be thrown.
- Records should not be left in unattended vehicles.
- Records of any type should **NOT** be left in vehicles overnight.

## 3.3 **Storing Paper Records**

### 3.3.1 **Current Records**

When a record is in constant or regular use or is likely to be needed quickly, it makes sense to keep it within the area responsible for the related work.

Storage equipment for current records will usually be adjacent to staff ie their desk drawers or nearby filing cabinets to enable information to be filed and managed so that it can be retrieved when it is next required. Records must always be kept securely and when a room containing records is left unattended, it should be locked. A sensible balance should be achieved between the needs for security and accessibility.

There is a wide range of suitable office filing equipment available. The following factors should be taken into account:

- Compliance with Health and Safety Regulations;
- Security (especially for sensitive and confidential material);
- Types of records to be stored, their size and quantities;
- Usage and frequency of retrievals;
- Suitability, space efficiency and cost.

### 3.3.2 **Semi Current Records**

As the need for quick access to particular records reduces, it may be more beneficial to move the less frequent used material out of the work area and into an archive storage area in another part of the building.

When transferred into archive semi-current paper records should be stored on shelves in a way that facilitates retrieval. The records should be boxed, stored off the floor and away from dampness and dust.

The width of aisles and general layout of storage areas must conform to fire, health and safety, and similar regulations.

Large documents such as maps, should be housed in special storage arrangements to ensure that they are not damaged and are easily accessible.

### 3.3.3 **Storing Non-Paper Records**

Photograph and film collections assembled by the staff through their work within the Trust should be regarded as Public Records and subject to this policy. Note that provisions of the Data Protection Act 1998 on registration of records and restriction of disclosure relate to photographs of identifiable individuals as well as to other personal records.

### 3.3.4 **Retention of Records**

The length of the retention period depends on the type of record and its importance to the business of the Trust. The destruction of records is an irreversible act, whilst the cost of keeping them can be high and continuing.

The Department of Health, Social Services and Public Safety Guidance – “Good Management, Good Records – Retention and Disposal Schedule” takes account of legal requirements and sets out minimum retention periods for clinical and administrative, both paper and electronic records. The Trust has local discretion to keep material for longer, subject to local needs, affordability and where records contain personal information, ensure the requirements of the Data Protection Act 1998 are met. The Trust has adopted the DHSSPS Good Records, Good Management Part 2 Retention and Disposal Schedule. All staff should refer to <https://www.dhsspsni.gov.uk/articles/records-disposal-schedules>

Records categorised for permanent preservation will need to be initially placed in long term storage with a view to them then being moved to a suitable archive as agreed with the Public Records Office, Northern Ireland.

#### 3.3.4.1 **Disposal of Records**

Most Trust records, even administrative ones contain sensitive or personal information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures their complete illegibility. Normally this will involve shredding, pulping or incineration. This can be done on site or via an approved contractor. A description must be kept of all records which have been destroyed, when and by whom. CD/back-up tapes/audio tapes identifiable information must be destroyed following advice from IT staff.

When records are destroyed by an external service provided, a Certificate of Destruction must be obtained from the Company destructing the records.

#### 3.3.4.2 **Retention and Destruction of Emails and Electronic Documents**

An email constitutes an official record when the document is made or received in connection with the transaction of Trust business. Emails should be retained for the same period of time as the Trust would need to retain such a record if it were in paper format. As previously stated, under the Freedom of Information Act 2000 certain emails and their content may be discoverable and would therefore be liable to disclosure. It is good practice to destroy all emails that do not need to be retained for specific lengths of time. Good housekeeping in emailing is a necessity if the Trust is to comply with the Act.

### 4.0 **Access to Records**

As a public body, the Trust's information is held on a basis of need and where information is not required for performing the business of the Trust it will be destroyed in line with retention and disposal schedules.

Staff will maintain appropriate records of their activity and ensure those records are correctly classified and can be accessed by the appropriate professional or employees of the Trust.

The Trust will provide access to its records in line with the relevant legislative requirements and appropriate professional guidelines. Both Trust staff and associated professionals are required to ensure they maintain the quality and consistency of records they create and ensure they follow the correct local procedures to allow both local and central access as appropriate.

Certain information held by the Trust is exempt from disclosure to the public. Examples of exemptions include information that relates to an individual and information provided in confidence; where appropriate, the Trust is required to publish information in either written or electronic format, on its activities in line with its “Publication Scheme”.

The Trust will publish or provide information to interested applicants under the Freedom of Information Act 2000, the Data Protection Act 1998 and the Environmental Information Regulations 1998, where the application is correctly presented, any prescribed fee has been paid and information requested is not subject to an exemption.

#### 4.1 **Disclosure**

The collecting of minimum appropriate information in order to perform the business the Trust requires the appropriate use of the information collected.

The disclosure of information must be limited to enhancing the delivery of a service, to service users, staff and the corporate aims of the Trust.

Disclosure of information to appropriate organisations and professional bodies should be limited to the information requested and in line with the Law and Trust’s protocols on information sharing.

Disclosure must follow rights under Law, for examples as outlined in the Data Protection Act 1998, Human Rights Act 1998, Freedom of Information Act 2000 and guidelines; and other national, professional and local organisational guidelines and Policy.

The improper disclosure of information may be in breach of the law, organisational guidelines/or Policy such as on confidentiality and other professional guidelines and may result in legal action by others and/or disciplinary action by the Trust.



5.0 **Designated Accountability**

- 5.1 The person accountable for overseeing the implementation of this policy and guidelines is the Corporate Manager.
- 5.2 The Director of Finance and IT will ensure that staff operating in the Trust are made aware of developments in law, HPSS and/or other professional guidelines and recognised good practice.
- 5.3 The Trust's Records Management Policy is required to be reviewed every two years or in line with legislative and good practice requirements.



---

**Liam McIvor**  
**CHIEF EXECUTIVE**

---

## **APPENDIX 1**

### **LEGISLATION AND NATIONAL GUIDELINES**

#### **1.1 Access to Health Records**

Data subjects now have access rights to records irrespective of when they were created, although under Section 30 certain records including health may be constrained or denied.

The Data Protection Act supersedes the Access to Health Records apart from the sections dealing with access to information about the deceased. The Access to Health Records Act provides rights of access to the health records of deceased individuals or their personal representatives and others having claim on the deceased's estate. In other circumstances, disclosure of health records relating to the deceased should satisfy common law of confidence requirements.

Patient Report Forms (PRFs) can form records under this legislation base.

#### **1.2 Audit Commission (NIAO) Compensation Payments for Clinical Negligence 2002**

The Northern Ireland Audit Office (NIAO) report on "Compensation Payment for Clinical Negligence" 2002, identified a number of areas that require improvement within the systems and procedures for dealing with clinical negligence and any resulting compensation payments.

#### **1.3 The Caldicott Review (England)**

In March 1996, guidance on the Protection and Use of Patient Information was published by the Department of Health. This guidance required that when the use of patient information was justified, only the minimum necessary information should be used and it should be anonymised wherever possible. In light of that requirement, the Chief Medical Officer established the Caldicott Committee to review the transfer of all patient identifiable information from NHS organisations to other NHS or non-NHS bodies for purpose other than direct care, medical research or where there is a statutory requirement, to ensure that current practice complies with the Departmental guidance.

On completion of the work, the Committee concluded that, whilst there was no significant evidence of unjustified use of patient identifiable information, there was a general lack of awareness throughout the NHS of existing guidance on confidentiality and security, increasing the risk of error or misuse.

The Caldicott Committee's Report, published in December 1997, included sixteen recommendations which related to ensuring best practice in the use of information flows between organisations.

Caldicott Guardians are also appointed in HSC Trusts in Northern Ireland.

#### 1.4 **Controls Assurance**

Information Management is one of the Controls Assurance Standards developed by the HPSS. The standard requires a systematic and planned approach to the management of records to be in place, so that the Trust can ensure, from the moment a record is created until its ultimate disposal, it can control both the quality and quantity of information it generates; can maintain that information in a manner that effectively services its needs and those of its stakeholders; and it can dispose of the information appropriately, when it is no longer required.

#### 1.5 **The Data Protection Act (DPA) 1998**

The DPA 1998 places a statutory responsibility on all HPSS organisations to protect the personal data which they hold. In relation to records management, this means that organisations must implement measures to:

- Maintain the accuracy of records held;
- Protect the security of personal data;
- Control access to personal data;
- Make arrangements for secure disposal once the record is no longer required.

#### 1.6 **Freedom of Information Act 2000** **Environmental Information Regulations 2005**

The Freedom of Information Act and Environmental Information Regulations 2005 gives the public the right to access to information held by public bodies. The Act recognises that members of the public have the right to request from the Trust information such as:

- Our costs?
- What services are being provided?
- How to make a complaint?
- Response times;
- Targets that are being set;

The NIAS HSC Trust Publication Scheme has been produced in line with section 20 of the Freedom of Information Act 2000, under which the Information Commissioner has approved a new model publication scheme for use by all public authorities from 1 January 2009.

Since 1 January 2005, any person who makes a request to the Trust for information, must be informed within 20 days whether the Trust holds that information and if so, it must be supplied. A public interest test may be carried out to determine if the benefit in disclosure outweighs the public interest in non-disclosure.

Freedom of Information relies on good record keeping including the creation of reliable records, which can be located when requested, and which are correctly disposed of, or selected for permanent preservation, at the appropriate time. Freedom of Information requires that there should be an audit trail to track the legal disposal of documents that are no longer required.

#### 1.7 **Good Management Good Records (DHSSPS)**

These guidelines offer an overview of the key issues and solutions and best practice for HPSS staff to follow when preparing a Records Management Strategy. It represents the joint DHSSPS and PRONI view of how records should be administered and sets the standards required of the HPSS.

#### 1.8 **Human Rights Act 1998**

The Trust must observe the right of individuals to respect for their private lives. Information should only be disclosed when the disclosure is authorised by law. In selecting information for disclosure, the Trust should make the least intrusion possible into an individual's private life.

#### 1.9 **The Public Records Act (NI) 1923**

All HPSS records are public records under the terms of the Public Records Act (NI) 1923. Chief Executives and Senior Managers of all HPSS organisations are personally accountable for records management within their organisation. They have a duty to make arrangements for the safe keeping and correct disposal (under the Disposal of Documents Order (NI) 1925) of those records under the overall supervision of the Deputy Keeper of Public Records whose responsibility includes permanent preservation.