
# Records Management Policy

# CHANGE LOG

| Version | Date | Author |
|---|---|---|
| 0.1 | 10 August 2012 | Sharon Beattie – Director of Operations |
| 0.2 | 01 October 2012 | Sharon Beattie – Director of Operations |
| 1.0 | 17 October 2012 | Sharon Beattie – Director of Operations |
| 2.0 | 6 February 2012 | Sharon Beattie – Director of Operations |

# CONTENTS

## 1 Introduction

Records Management is the foundation on which the Safeguarding Board for Northern Ireland (SBNI) can build its responses to growing demands for governance and operational effectiveness in relation to information. The Data Protection Act 1998 and the Freedom of Information Act 2000 require that the SBNI processes Subject Access and Freedom of Information Requests within the timeframes set out in law, while there is also an imperative to do so economically to ensure best use of resources. Furthermore, both Acts require that the SBNI publishes and implements policies in relation to the management of records.

The SBNI therefore recognises that records are an important corporate asset requiring proper management throughout their lifecycle; with due regard taken to legal obligations, professional practice and the SBNI's business needs. All public authorities must ensure that records management policies and procedures are fully compliant with legislation and are a good fit with recognised good practice regarding the management of information.

This strategy should be read in conjunction with the DHSSPS Guidance Document 'Good Management, Good Records' which has been adopted as the SBNI's Retention and Disposal Schedule.

## 2 Why do we need a strategy?

A records management strategy is essential to signal a clear direction to all concerned as to how the governance responsibilities and records/information management issues are to be managed by the SBNI over what will inevitably be a medium-long term timeframe.

## 3 Purpose of Strategy

The purpose of this strategy is to provide a framework for planning, developing and implementing records management policies and procedures which are consistent with legislation and the business requirements of the SBNI.

## 4 Scope of Strategy

This strategy relates to all corporate and operational records held in any format by the SBNI as detailed in the Departments of Health's publication 'Good Management, Good Records (GMGR November 2011)'. The Policy provides for:

- The requirements that must be met for the records of the SBNI to be considered a proper record of the activity of the SBNI;
- The requirements for systems and process that deal with records;
- The quality and reliability which must be maintained to provide a valuable information and knowledge resource for the SBNI;
- Review of the policy and checking the quality of implementation;
- An overall statement of records management policy which is supplemented by detailed procedures.

## 5 What is a Record?

A record refers to anything that contains information that has been gathered or created as evidence of any activity, such as emails, Board Minutes, Committee Agendas and Case Management Review (CMR) Reports. The information can be in any format, paper, electronic, digital or voice recording.

Records management is the methodical and consistent control of all records held by an organisation. The records are given appropriate filenames and are grouped together according to classification. The SBNI operates both a manual and electronic filing system.

Records are a corporate asset and the records of the SBNI are important sources of information. These records are vital in the creation and future work of the SBNI for the purposes of accountability and awareness and include areas such as administration, financial, legal and historical information.

The SBNI will create, use, manage and destroy or preserve its records in accordance with all statutory requirements, Accurate records management is

essential to the SBNI's effectiveness and efficiency. Effective record management ensures that;

- The record is present and correct - The record is present and filed in correct location with appropriate security and data protection in place. The document may be needed to form a reconstruction of activities or events that have taken place.
- The record can be accessed - It is possible to locate and access the information from internal filing / archiving systems, electronic and / or manual systems that are in place.
- The record is clear and can be interpreted - The context of the record can be established;
  - who created the record
  - which business activity / process does it relate to
  - does it relate to any other records
- The record can be trusted - The authenticity and integrity of the record must be kept intact as the record must actually be what was created and used by the SBNI. For example, redacted records released under the Freedom of Information Act must be kept to show exactly what was released and the original record kept showing what was withheld.
- The record can be maintained through time - The quality of accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed. Change of format should not compromise the maintenance of the record.

## 6 Responsibilities for Records

All records created by the SBNI are public records as defined in the Public Records Act (Northern Ireland) 1923.

### Statutory Responsibility

'Good Management, Good Records' states that the Permanent Secretary, Departmental Information Manager, Chief Executives and senior managers are personally accountable for records management within their organisation and

have a duty to make arrangements for the safe keeping and eventual disposal of those records under the overall supervision of the Deputy Keeper of Public Records at PRONI.

**Roles and responsibilities within the SBNI**

The formal roles and responsibilities relating to records management within the SBNI are set out in section 3 of 'Good Management, Good Records' and are reproduced in this policy.

- **Accounting Officer –** The Chief Executive Officer of the Public Health Agency will act as Accounting Officer for ensuring that SBNI complies with its statutory obligations in relation to management of records related to the discharge of its SBNI's corporate host functions. The Chair of the SBNI will account to the DHSSPS, through its Sponsor Branch for the management of records related to the discharge of SBNI's statutory objectives and functions.

- **Director of Operations** will perform the role of Senior Information Risk Owner (SIRO) and will take overall ownership of the information risk within SBNI, act as champion for information risk to the Board and provide written advice to the Board, Chair and Accounting Officer on the content of the SBNI's Internal Control in relation to information risk.

- **Office Manager –** the Office Manager is operationally responsible for the day to day implementation of all aspects of Information Governance including records management. They also hold the responsibility for coordinating and overseeing implementation of records management within the SBNI Office. He / She will also provide support and guidance to the Safeguarding Panel Administration staff.

- **Responsibility of SBNI Members**
  SBNI will routinely handle sensitive personal information and there will be safeguards in place within the SBNI to ensure that such information is protected, handled appropriately and explanation and assurances will be

provided to the person / agency from whom information is being sought. Organisations (e.g. those within Justice) who use the Government Marking Scheme should handle any 'confidential' information sent to them by the SBNI in accordance with the handling of 'restricted' documentation.

Similarly SBNI will be sharing information with SBNI Member Agencies and will expect the relevant agencies to ensure that such information is protected and handled appropriately by them accordingly to their own Information Governance policies and procedures.

- **SBNI Officers (including Laypersons and Independent Chairs)**
  All staff of the SBNI who create, use, manage or dispose of records have a duty to protect them and to ensure that any information that they add to the record is necessary, accurate and complete. The confidentiality of the record will always be a priority of the SBNI and all staff involved in managing records will receive the necessary training and must acknowledge their duty of care in relation to Data Protection and ensure that the correct level of security is applied and confidentiality is not breached.

  All records need to be managed in accordance with the terms of the Data Protection Act 1998 and the Freedom of Information Act 2000 and must be suitably robust to meet the requirements of both internal and external audits.

- **Responsibility of Safeguarding Panel Administration Team**

  Administrative staff for the Safeguarding Panels who create or use records of the SBNI have a duty to protect them and to ensure that any information they add to the record is necessary, accurate and complete. The administrative team need to adhere to the records registration process of the SBNI and assure the SBNI that the record is protected and handled appropriately by them accordingly to their own Information Governance policies and procedures.

## 7 Security of Records

All information held by the SBNI must be kept securely, irrespective of the format in which it is held. Records are stored in designated areas under the management of the Office Manager. The security of records that have been removed from the designated storage area is the responsibility of the borrower. The following provisions are put in place to protect SBNI records:

- Office doors, cabinets and desk drawers are locked as appropriate when not in the office
- Access to keys are controlled
- Minor exits and entrances are not left open
- Exits are locked and windows are closed at the end of the working day
- All records are stored in a secure location
- All confidentiality records are stored in a fire-proof safe, kept in a secure office under the management of the Office Manager.
- All work completed by the SBNI is recorded and held in master files. These files constitute the records of the organisation. Each master file is contained within the SBNI corporate File Cover and are managed in accordance with this Policy. All confidential material, e.g. confidential section of Board meetings are held within a master file marked confidential and stored within the fire-proof safe.

## 8 Transporting Records

Movement of records outside of the facility where they are normally used may be required for a variety of reasons. It is the responsibility of the SBNI Operations Manager to make sure that records are transported safely and appropriately.

In particular, where there is a need for records, files and other media containing personal information to be removed from their designated storage area, it is vital that the personal information is kept securely and the following guidelines are to be followed:

- The information must be kept in a secure container, for example a brief case or bag that zips;
- The information must be kept out of sight;

- The information must not be left unattended, without appropriate security;
- Where it is necessary to take personal information home, it must be locked in a fire-proof safe, away where it cannot be accessed by family members or visitors;
- SBNI view the home environment as an extension of the workplace and will provide approved home-workers with encrypted lap-tops (refer to IT Security Policy) and fire-proof safes. All confidential, sensitive, personal material must be kept in these safes;
- Laptops and other software must be kept securely, with documents containing personal information password protected. The lap-top must be kept separate from the confidential, sensitive, personal material. Staff, Independent Chairs and Laypersons must also make sure that they are aware of and in compliance with other guidance and policies in respect of ICT security (applicable to those using an SBNI encrypted laptop);
- SBNI Case Management Review Chairs contracted to undertake work on behalf of SBNI will be required to have appropriate Indemnity Insurance and to provide assurance to the SBNI that appropriate safeguards are in place for the security of documentation;
- All employees or persons contracted to engage in SBNI work should be required to provide a written assurance that they will adhere to SBNI security policy regarding the handling of sensitive personal information. This written assurance will take the form of a declaration signed by the relevant individuals;
- SBNI Members and Members of the SBNI Committees should adhere to this policy section when transporting SBNI records.

## 9 Sending Records

Records created by the SBNI should not, under normal circumstances leave the SBNI. However, it is accepted that there may be circumstances where this is unavoidable, for example records required by the Court. Where records are required by another organisation, the SBNI must retain the original record and provide a quality copy of the relevant sections only of a file.

The following should be followed when personal or confidential business information is being sent through internal or external mailing systems.

- Address the mail correctly and fully, i.e. the name, title and full address of the individual to whom it is being sent, and seal it securely
- Mark envelopes appropriately, e.g. 'Private and Confidential', 'For the Attention of', 'Only to be Opened By', etc.
- Include the message, 'If undelivered, please return to' and followed by details of the sender on the back of the envelope (this can be conveniently achieved by using pre-prepared labels)
- Seek acknowledgement of receipt of information, where appropriate

## 10 Sending Sensitive / Personal Information by E-Mail

At present there is not a requirement to apply encryption to sensitive information transferred across the HSC network to other HSC organisations within Northern Ireland. Information transferred between the SBNI, Trusts and DHSS&PS is not sent across the internet. If you are transferring information to any address that does not end in one of those listed below, it is essential that electronic measures to secure the data in transit, are employed, and it is advised that encryption is therefore applied at all times to transfers of sensitive / personal information.

List of email addresses **within the Northern Ireland private network:**

- **'.hscni.net',**
- **'n-i.nhs.uk'**
- **'ni.gov.uk' or**
- **'.ni.gov.net'**

**No sensitive or patient data** must be emailed to an address other than those listed above unless they have been protected by encryption mechanisms that have been approved by the BSO-ITS.

It is important to remember that although there is a degree of protection afforded to email traffic that contains sensitive information when transmitting within the Northern Ireland HSC network, that it is important that the information is sent to

the correct recipient. With the amalgamation of many email systems, the chances of a name being the same or similar to the intended recipient has increased. It is therefore recommended that the following simple mechanism is employed when transmitting information to a new contact or to an officer you haven't emailed previously.

- **Step 1**. Contact the recipient and ask for their email address
- **Step 2**. Send a test email to the address provided to ensure that you have inserted the correct email address
- **Step 3**. Ask the recipient on receiving the test email to reply confirming receipt.
- **Step 4**. Attach the information to be sent with a subject line 'Private and Confidential, Addressee Only' to the confirmation receipt email and send.

More information on the secure transmission of sensitive information can be sought from the BSO ICT Security Manager.

Examples of sensitive and personal information include but are not limited to:-

- commercially sensitive information;
- contracts under consideration;
- budgets;
- restricted and confidential information;
- appointments – actual or potential not yet announced;
- disciplinary or criminal investigations.

Personal data is further defined by the Data Protection Act (1998).

## 11 Records Registration and Filing

Records registration ensures a link between the record and its administrative roots. The registration of records will follow best practice in records management and allow users to identify and retrieve records efficiently. The SBNI Master File and Confidential covers will be used for all manual files.

Master file covers will be labelled with the following information:

- File title and Reference
- Date of first paper / date file opened

File referencing is the practice of placing a number on record in a file, so that records are easily identifiable from each other. SBNI will create a filing system that is based on good records management practice. Files will be arranged in a logical sequence, known as a 'Filing System', to enable them to be managed, stored and retrieved efficiently and effectively. The use of a 'Filing System' will ensure that the SBNI has an inventory of all its business / corporate files.

The following process will also be followed in relation to the 'Filing System'.

- Date of last paper / date file closed and be clearly marked 'closed'.
- Accurate file titling is essential for an efficient filing system. The title of every file should:
  - Accurately reflect its contents.
  - Be as specific as possible – meaningless titles, such as 'miscellaneous' are to be avoided.
  - Indicate both the information content and the types of document, e.g. Safeguarding Board – 'agenda and minutes' rather than just Safeguarding Board.
- Correspondence should be filed in correct files at all times. All papers for filing should bear the appropriate file reference in which the record is to be filed.
- All papers should be filed at the right hand side of the file.
- All papers should be in date order with most recent paper at the top.
- Where possible paper clips / bull dog clips and staples should be removed from papers before filing as these will damage the paper, and when rusted can be a health hazard. This is particularly important where records are to be retained for long periods or permanently.
- Files should not contain either adhesive tabs or post-its. Paper card dividers may be used where necessary.
- Files must not contain any loose papers.
- Plastic treasury tags should be used instead of metal tags.

- Before filing, staff must check for duplication of correspondence when filing and make sure any action or comments are completed before putting file away.
- Files should not contain documents in 'Poly Pockets'
- Bulky items such as publications should be cross referenced within the file and stored in the reference library.
- Depth of paper contained within a file should not be thicker than 2.5 cm. A continuation file, if required, should be open and cross-referenced, for example Volume 1, Volume 2.
- Filing should be completed on a regular basis to avoid backlog and ensure files are up-to-date.
- Files will be reviewed for disposal in accordance with the DHSSPS Guidance Document 'Good Management, Good Records'.

## 12 Version Control

SBNI will use version control to identify where changes have been made to a document and to make sure that everyone is using the most recent version of a document. This is particularly important when a document is being produced or reviewed collaboratively.

The content of a document under version control is never overwritten. However, each time modifications are made to a document a new version is created, which then becomes the current version. Every version number for a given document will be unique.

Each version of a document shall be given an issue number, in the format of 'Version 0.1'. This should appear in the bottom right corner of the document within the footer.

### Initial Draft of a Document

When a document is initially produced, prior to approval, it shall be versioned as 'Version 0.1 Draft'. Subsequent versions of the initial document shall be described

as ‘Version 0.2 Draft’, Version 0.3 Draft’ etc. Where documents are in draft, a ‘DRAFT’ watermark should be incorporated into the document.

**First Approval of a Document**

When a document has been formally approved, it shall be issued as ‘Version 1.0’.

**Initial Review of an Approved Document**

Good practice suggests that documents should be reviewed regularly to ensure that they are up-to-date, relevant and not obsolete. During the review of the formally approved document ‘Version 1.0’, if an amendment is required a new version of the document should be created incorporating the amendment. This will be versioned as ‘Version 1.0 Draft 1’. Subsequent changes during the review of document ‘Version 1.0’ will be versioned as ‘Version 1.0 Draft 2’, ‘Version 1.0 Draft 3’, etc.

If the changes are considered to be minor e.g. spelling, grammar, 1 line change, then the document will be issued as ‘Version 1.1’

If the changes are consider to be major e.g. addition/removal of a section, legislative changes, change in processes, then the document will be issued as ‘Version 2.0’

**Subsequent Reviews of a Document**

If further changes are to be made to document ‘Version 1.1’, the draft version will be described as ‘Version 1.1 Draft 1’, ‘Version 1.1 Draft 2’, Version 1.1 Draft 3’, etc.

If further changes are to be made to document ‘Version 2.0, then draft version will be described as ‘Version 2.0 Draft 1, ‘Version 2.0 Draft 2’, ‘Version 2.0 Draft 3’, etc.

### Change Log

A Change Log will be used to assist with identifying where modifications have been made within each version of a document. In such cases, an entry should include details of the following:

- The version number;
- The date the version was assigned; and
- The author of the changes;

## 13 File Retention, Closure and Disposal

Guidance for the retention, closure and disposal of records within the SBNI is based on the DHSSPS Guidance Document 'Good Management, Good Records' and applies to all business / corporate files.

### Record Closure

All files will be closed when:

- Directed by the SBNI Retention and Disposal Schedule.
- The subject matter is finished. Files will, where appropriate, be time-bound to calendar or financial years. Files in this scenario should be closed at the end of each calendar / financial year and a new file opened if necessary for the next year.
- The depth of paper contained within the file reaches 2.5 cm. a continuation file, if required, should be opened and cross-referenced, for example Volume 1, Volume 2.
- No new papers have been added to the file for two years. A new file can be opened, if it becomes necessary or appropriate.
- It has been open for five years. The maximum time for which a file can remain open is 5 years. If it has not been closed prior to this, it must be closed when it is 5 years old.
- Once a file has been closed, no further papers should be added.
- File covers should be clearly marked 'CLOSED', along with the closure date.

- A ‘Closure Sheet’ must be inserted into every file closed. This is to remind staff that no further papers can be added. At this stage the date of the earliest and latest papers should be recorded and;
  - The date of the first review;
  - The date the file is due to be destroyed; or
  - The date the file should be transferred to the Public Records Office Northern Ireland (PRONI), whichever is appropriate, should be recorded on the file cover.
- Once a file has been closed it should be held for the minimum retention period. Once reviewed a decision should be made to place the file into archive/offsite storage or schedule the file for destruction. Only Master Files and Confidential Files should be transferred to archive/storage.

**Record Disposal**

Once records have been closed and held for the minimum retention period, a decision must be taken in relation to their disposal. There are four options for ‘disposal’ of records:

- File to be held for review at a future stage;
- File to be permanently retained within the SBNI;
- File to be transferred to the PRONI for permanent preservation or
- File destruction.

Where records / information are disposed of via destruction, an auditable trail must be retained detailing the records disposed of and the date of disposal. The disposal of any SBNI record must have the approval of the Operations Manager, who will be required to sign and authorise the disposal for the records.

Duplicate, unimportant, material ‘for information’, rough drafts and ephemeral material can be disposed of via destruction, as part of routine administrative practice.

## 14 Management of Handwritten Notes / File Notes

The following guidelines, which are based on good records management practice, apply to all business/corporate files.

### Handwritten or shorthand notes of meetings

The recording of handwritten or shorthand notes is a common occurrence at meetings. An official minute taker should be identified for each meeting. This may be a member of administrative staff, a health or social care professional or a senior manager. Minutes taken should be recorded in a bound notebook, where possible.

Such notes should be retained by the official minute taker until the final minutes are formally approved at the next meeting. The notes can then be disposed of, as appropriate.

It is the responsibility of the chair of the meeting to take responsibility for ensuring the minutes are accurate and formally approved at the following meeting.

Staff members present at meetings, other than the official minute taker, may have handwritten personal notes relating to the meeting. For example, a record of actions they have agreed or been nominated to undertake. These notes should be destroyed once they reach the end of their current use as they are duplicate information contained in the formally approved minutes.

### Handwritten records (file notes)

Handwritten file notes are acceptable but must be dated and signed by the author and the author must be clearly identified. The name and designation of the author should be printed against the first file entry or where appropriate, a list should be inserted at the front of the file detailing the name, designation and signature of all staff responsible for making notes in the file in question.

**Notes/corrections in the margins of a page by a commentator or reader**

- Records must be kept up to date and in chronological order or a logical sequence.
- Information should be recorded at the time of the event. If this is not the case, entries should be made as soon as is practically possible, either on the same day or the next working day.
- Any retrospective information which needs to be added into a record (e.g. where a genuine omission has been identified) should be entered into the record as the next chronological entry, using the current date and time. Reference should be made to the event to which it relates.
- Information added into the record should be legible, clear and unambiguous.
- Information added into the record should be concise, comprehensive and accurate. Only important, relevant and complete information should be recorded.
- Record factual information and avoid subjective comments.
- Use of abbreviations and jargon should be avoided. Where these are commonly used, they should conform to an agreed, standardised list.
- Entries into the record should be dated, timed and signed.
- Authors of entries should be easily identifiable. The name of the entry author should be legibly printed against the signature or a list should be held in the record detailing the name and signature of relevant staff members responsible for entering information into the record.
- Remember – if it isn't recorded then it didn't happen.
- Entries in a record should not be tampered with or changed or added to once they have been signed, without highlighting the change.
- Alterations/changes should be made by striking through with a single line. Any changes should be signed and dated followed by the corrected information. No correcting fluid should be used to make alterations.
- Entries should only be amended if the original information was inaccurate, misleading or incomplete.
- Careful consideration should be given as to the need for notes in the margin or whether the information could be recorded elsewhere in the record.

- The addition of such notes in the margin, or annotations, to a record may constitute the creation of a new record.

## 15 Managing Electronic Records including E-mails

The following guidelines, which are based on good records management practice, apply to the management of electronic records including e-mails. These guidelines do not apply to patient/client/staff information systems.

- Electronic documents should be structured into files, folders and sub-folders, in the same way as paper files are organised.
- If there is a hybrid system (i.e. parallel use of electronic and paper files) the folder system should use the same file titles/index terms as the paper filing system.
- A standard Naming Convention should be used for naming electronic documents. They should have file titles which are easily understood by all members of staff. Only use commonly understood abbreviations.
- Responsibility for the storage, security and disposal of an electronic record rests with the person who created it.
- Templates* (based on the corporate templates) should be developed and used for common forms of documents e.g. memos, standard letters, reports etc.
- Electronic records should be version controlled by either marked with a 'Draft' or a 'Version Number'. (Refer Section 11 – Version Control.)
- E-mails which form part of a record should be managed appropriately by either printing to the paper file or saving to the relevant folder.
- Staff should dispose of electronic files in the same timescale as paper files, in accordance with the PHA's Retention and Disposal Schedule.

## 16 Protective Markings on File Covers

The following guidelines, which are based on good records management practice, apply to all files - business/corporate files and patient/client/staff files.

* Microsoft Office Templates

‘Protective markings’ are applied to file covers so that those handling and receiving them are aware that additional measures may need to be implemented in order to protect the information contained within the files. The SBNI uses only one protective marking on File Covers.

- Files containing personal data will always be classified as ‘confidential’ because of the sensitive personal information contained within the records. These files should be clearly labelled on the back and front with sticky labels as ‘confidential’ and should only be accessed by authorised persons.
- Business/corporate files may need to be classified as ‘confidential’, but this will depend upon the sensitivity of their content. Therefore, if a file contains papers which are confidential, then the file cover needs to be marked confidential. However, it should be noted that the classification can change with time. For example, tender applications may only be confidential until the tendering process has completed and the contract has been awarded.

  Those with a responsibility for files should be careful not to ‘over-classify’ them. Although a protective marking may be in use, it does not automatically exclude any of the information contained in a file from potentially being shared or disclosed under information legislation e.g. Data Protection Act 1998, Freedom of Information Act 2000.

## 17 Equality Screening

Having considered this policy, SBNI are satisfied that there is no scope to promote equality or good relations and no risk of adverse impact on equality. Documentation to evidence the screening has been produced and is publically available.

## Appendix

There are a range of legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

The key legal and professional obligations covering personal and other information listed[1] in this Appendix are as follows:

- The Access to Health Records (Northern Ireland) Order 1993
- The Access to Personal Files and Medical Reports (Northern Ireland) Order 1991
- Administrative Law
- The Adoption Agencies Regulations (Northern Ireland) 1989
- The Blood Safety and Quality Regulations 2005 (as amended)
- The Census (Confidentiality) (Northern Ireland) Order 1991
- The Civil Evidence (Northern Ireland) Order 1997
- The Common Law Duty of Confidentiality
  – Confidentiality: DHSSPS code of practice (PDF 111KB)
- The Computer Misuse Act 1990
- The Congenital Disabilities (Civil Liability) Act 1976
- The Consumer Protection (Northern Ireland) Order 1987
- The Control of Substances Hazardous to Health Regulations (Northern Ireland) 2003
- The Copyright, Designs and Patents Acts 1988
- The Data Protection Act (DPA) 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community Code Relating to Medicinal Products for Human Use

[1] Further information is detailed in the Department of Health's publication Good Records Good Management (GMGR)

- The Electronic Communications Act 2000
- The Environmental Information Regulations 2004
- The Foster Placement (Children) Regulations (Northern Ireland) 1996
- The Freedom of Information Act (FOIA) 2000
- The Gender Recognition Act 2004
- The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) (No. 2) Order 2005
- The Health & Personal Social Services, General Dental Services (Amendment) Regulations (Northern Ireland) 2008
- The Health & Personal Social Services, General Medical Services Contracts Regulations (Northern Ireland) 2004
- The Health and Safety at Work (Northern Ireland) Order 1978
- The Health and Social Services (Reform) Act (Northern Ireland) 2009
- The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology Act 2008
- The Human Rights Act 1998
- The Limitation (Northern Ireland) Order 1989
- Police Act 1997 and the Memorandum to A Code of Practice for Third Party recipients of Criminal Record Information
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Public Health Act (Northern Ireland) 1967
- The Public Interest Disclosure (Northern Ireland) Order 1998
- The Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order (Northern Ireland)1925
- The Radioactive Substances Act 1993
- The High-activity Sealed Radioactive Sources and Orphan Sources Regulations 2005
- The Re-use of Public Sector Information Regulations 2005

- The Sexual Offences (Amendment) Act 1992 (as amended by the Youth Justice and Criminal Evidence Act 1999)

This policy should be read in conjunction with the SBNI's Freedom of Information, Data Protection and Confidentiality Policies and the ICT Security policy.