Records & Information Management Policy

Author: Sam Pringle

Version: v1.7
Date: 29 Feb 2008
TRIM Ref: DF1/07/185351 – Unrestricted

SIB
strategicinvestmentboard

Contents

Version History

Table 1: Version History

Version Number	Version Date	Summary of Changes
1.0	6-Nov-07	Initial draft created.
1.0	8-Nov-07	Version approved by Chief Operating Officer and Information Manager. (Note that Appendix 3 "*Archiving Old Paper Files*" is incomplete until procedures have been agreed with FileStores).
1.5	20-Dec-07	Amended to include text from DF1/07/198555 "*Records Management Policy v1.1 Draft 070302*"; this was last updated 2-Mar-07. The additional text has been added as a new Section 9, "*The Statutory Duty of SIB and its Staff*" on page 7; an expansion of Section 11, "*Responsibilities and Policy Review*" on page 9 and additional appendix sections A2.4.2 "*Records Managed Outside SIB*" and A2.4.3 "*Contracts Let Directly by SIB*" on page 23. The policy has been renamed "Records & Information Management Policy". (Note that Appendix 3 "Archiving Old Paper Files" is incomplete until procedures have been agreed with FileStores).
1.6	21-Jan-08	Appendix 3 added (following procedures being agreed between DFP and FileStores).
1.7	Feb-07-08	Amended to include policy sections on "*Information Security*" (Section 12) and "*Information Stored on Portable Devices*" (Section 13). Management Summary (Section 1) amended to include a responsibility for information security, "Take personal responsibility for the effective management *and security* of SIB's records and information." The words, "…*and for ensuring that it is kept securely*" added to the End User role in Table 2.

1 Management Summary

This document defines an Information Management Policy for SIB. It outlines its scope and provides eight information management principles to ensure that staff:

- Treat SIB information as a Corporate Resource.
- Make the information they create or capture accessible to those within SIB who need it to fulfil their roles.
- Manage all information in a consistent manner across SIB.
- Record details of key business activities undertaken on behalf of SIB.
- Ensure that SIB's information is accurate and fit for purpose;
- Retain or dispose of information in accordance with legislative requirements or SIB's procedures.
- Take personal responsibility for the effective management and security of SIB's records and information.
- Comply with all statutory and regulatory requirements.

This document also describes the roles and responsibilities of the different types of users particularly in relation to the Electronic Document and Records Management System (EDRMS), which is TRIM. More detailed guidelines for information management within SIB are provided in DF1/07/185398 "*SIB Information Management Procedures*". The key responsibilities of the main roles can be summarised as follows:

Table 2: Information Management Roles in SIB
(Roles in *italic* are outside of SIB)

ROLE	RESPONSIBLE FOR
End User	Creation, capture, storage, dissemination and retrieval of information (including documents and records) and for ensuring that it is kept securely.
SIB Information Manager	Provides records management for SIB, including responsibility for the SIB Corporate File Plan. Also coordinates high level searches for Data Protection and Freedom of Information requests. (Note that the SIB Information Manager is a "power user" in the Northern Ireland Civil Service terminology).
Departmental Records Officer (DRO)	Although SIB is a Non-departmental Public Body (NDPD), it has "Departmental" responsibilities derived from the Public Record Acts, including annual release of records to public record offices. The Departmental Records Officer has strategic oversight of records and information management policy and is also responsible for the provision of advice on compliance with legislative requirements such as Freedom of Information and Data Protection. The Chief Operating Officer (COO) is the Departmental Records Officer.
DFP IMU	*The Department of Finance and Personnel Information Management Unit (DFP IMU) provide technical support and assistance for TRIM, primarily via the SIB Information Manager.*

ROLE	RESPONSIBLE FOR
Systems Administrator	*The Northern Ireland Civil Service Information Management Unit is the system administrator responsible for systems configuration and management.*

Finally this document lists related documents which are subsidiary to this Policy and which facilitate effective information management using the electronic systems used by SIB.

2 Purpose

This document provides an information management policy for the effective and efficient management of SIB's *documents* and *records* (i.e. recorded information).

3 Introduction

SIB depends totally on information and so information is one of the SIB's most important assets. Although much of this information is irreplaceable if destroyed, it is often managed inconsistently and ineffectively.

Effective management of information is essential to improve the efficiency and effectiveness of SIB. The right people must have access to the right information when they need it and the functionality of the Electronic Document and Records Management System (EDRMS) helps to achieve this. However, the full benefits can only be realised if staff comply with this strategic information management policy and the more detailed working procedures.

To do this, SIB needs to:

- Find information about a particular activity or transaction as quickly as possible.
- Identify quickly those people within SIB (or more widely) who can help with a particular issue.
- Find and re-use information, methods and practices which have been successful.

This Information Management Policy seeks to achieve the three objectives above. The following sections provide more detail.

4 Scope

This policy assumes information boundaries within SIB as shown in Figure 1.

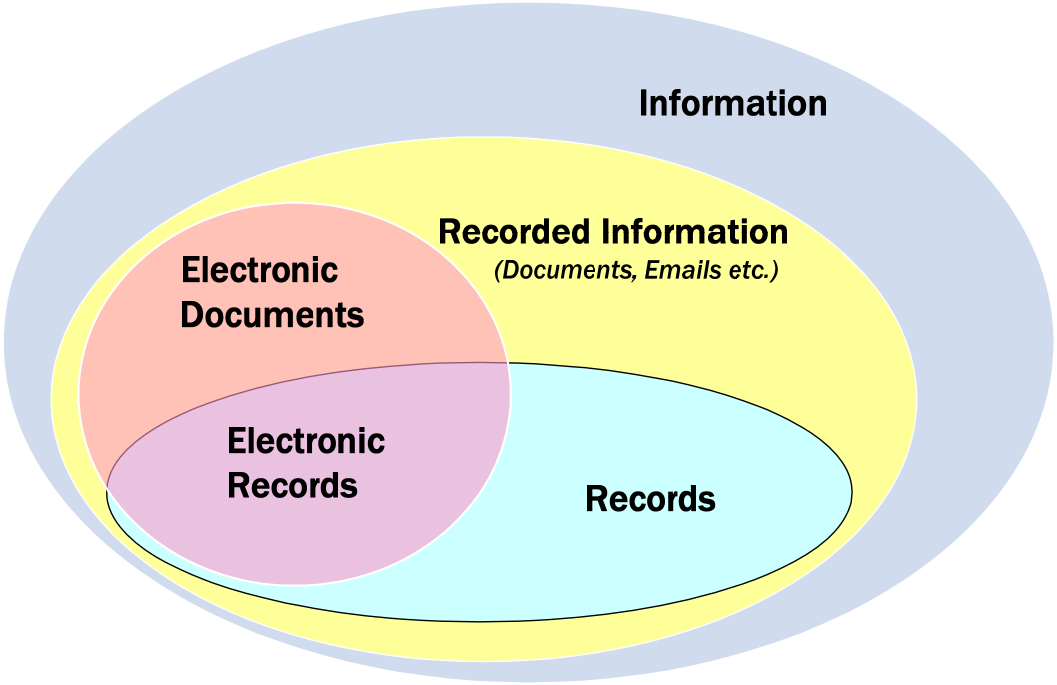

Figure 1: Information Boundaries Within SIB

This Policy covers all recorded information.

- Whatever the medium: e.g. electronic or paper.
- Whether it originates from within SIB or from outside.

The Policy excludes information such as telephone conversations, meetings or physical objects unless these or references to them are recorded as documents (e.g. a “note of meeting”).

This Policy covers information held in discrete computer applications and databases (e.g. financial systems, compensation claim systems and human resources systems). The management of such systems should follow the eight information management principles. The Policy provides a framework for developing specific procedures and guidance. Policies for all other information management products used by SIB derive from this Policy.

Ultimately all (or at least the majority) of records in SIB are expected to be stored electronically.

5 Definitions

Certain words in this Policy have specific meanings and these are explained in the glossary at Appendix 1 on page 13. However, two terms are fundamental to this Policy and are defined as follows.

5.1 Document

A ‘*document*’ can be defined as:

> *“Information that is stored as a single entity on some medium (e.g. on paper, a computer drive etc.)”*

The term also covers information in what might seem non-documentary formats: e.g. computer applications and databases.

5.2 Record

A '*record*' can be defined as:

> *"A document which has content, context and structure and which provides evidence of a business transaction or contains information needed to carry on SIB's business."*

A '*record*' can either be created in SIB or outside. It may be created to fulfil a legal requirement and may be required as legal evidence or to satisfy public accountability or assembly/parliamentary scrutiny.

As records derive from documents, all records will be documents but not all documents will be records. For example, a publication in a library provides information and so it is a document, but it is not a record because it does not provide evidence of an SIB activity.

6 Electronic and Non-electronic Documents and Records

There is an important distinction between electronic and non-electronic *documents* and *records* as they may be processed in different ways. However, ultimately all SIB information should be stored within the Electronic Documents and Records Management System, which is called *TRIM*. Clearly, retrospective management of some paper documents using the EDRMS will only be completed as required. All documents created after 1 April 2007 should be managed using the EDRMS and normally these will be stored electronically.

If electronic storage is not possible or inappropriate, documents and records should still be managed using the EDRMS. This can be done by creating an electronic record that corresponds to the paper record so that the electronic version can be used to track and locate the paper version.

7 Eight Information Management Principles

The success of SIB depends on effective use of its information. It has therefore adopted the following eight information management principles.

The primary principle is:

1 SIB Information is a Corporate Resource. All Information (including emails) belongs to SIB and not to any individual or group.

Therefore, information needs to be:

Available:

2 Staff will limit colleagues' access to information they create or capture only if its sensitivity requires it.

3 Staff will manage information consistently, including the use of approved naming conventions and file structures.

Appropriate:

4 Staff will record details of appropriate Business Activities.

5 Staff will ensure that information is accurate and fit for purpose.

6 Staff will retain or dispose of information appropriately.

Accountable:

7 Staff will accept responsibility for the information they personally manage. Every member of staff is personally responsible for the effective management of the information they create, capture or use.

8 Staff will manage information in compliance with Statutory and Regulatory Requirements. In managing information, staff will comply with the relevant statutory, regulatory and protective marking requirements – including the requirement not to destroy information where there is a legal obligation to retain it.

SIB has the responsibility to train staff so that they can follow these principles.

8 Information Management Guidelines

All staff are under a statutory obligation to create accurate *records* of their activities and to manage and maintain such documentation within the EDRMS. Specific guidelines for managing information are provided in Appendix 2 on page 19. These underpin the eight information management principles and are structured under the following headings:

- Creation and Capture/Receipt of Information – on page 19
- Storage and Retrieval of Information –on page 20
- Dissemination of Information – on page 21
- Retention & Disposal of Information – on page 21
- Compliance with Statutory and Regulatory Requirements – on page 23.
- Redacted or Annotated Records – on page 24.

9 The Statutory Duty of SIB and its Staff

To enable compliance with a wide range of statutory duties and responsibilities, the SIB has a duty to keep a permanent record of all significant documents. Any important or significant document or email must be created and filed. A record must be created where the document contains material which:

- Records decisions, the rationale for decisions or provides authority for action.
- Might be needed to prove whether an activity or transaction took place.

- Might be needed for administrative, accounting, audit, research or historical purposes.
- Will be needed to maintain business continuity.
- Provides the only evidence of the origin of and/or date of receipt of an attached document which needs to be retained.
- Could be requested under the Data Protection or Freedom of Information provisions.

Staff should bear in mind the need to write in clear, unambiguous English; avoiding clichés and unnecessary jargon.

10 Roles and Responsibilities

Three roles are needed within SIB to manage information using TRIM. These are described below.

- End User
- SIB Information Manager
- Departmental Records Officer (DRO)

. Other records management activities are carried out on SIB's behalf by:

- DFP IMU
- Systems Administrator

These are also described below.

10.1 End User

End users are responsible for all processing of information within their areas of work. They have an obligation under legislation to declare records that demonstrate actions taken by them on behalf of SIB.

10.2 SIB Information Manager

The SIB Information Manager is also the Records Manager. The Information Manager is responsible for the SIB Corporate File Plan structure. She also provides and updates disposal schedules for all types of information and archives and disposes of SIB information in accordance with these schedules. There is an SIB code of conduct for records management, DF1/07/174788 "*Code of Conduct for SIB Records Management*".

The Information Manager is responsible for Freedom of Information or Data Protection and may undertake necessary searches needed to fulfil her statutory duties.

The Information Manager receives her delegated authority through the Departmental Records Officer (DRO).

10.3 Departmental Records Officer (DRO)

Although SIB is a Non-departmental Public Body (NDPD), it has "Departmental" responsibilities derived from the Public Record Acts, including annual release of

records to public record offices. The Departmental Records Officer has strategic oversight of records and information management policy and is also responsible for the provision of advice on compliance with legislative requirements such as Freedom of Information and Data Protection. The Chief Operating Officer (COO) is the Departmental Records Officer.

10.4 DFP IMU

The Department of Finance and Personnel Information Management Unit (DFP IMU) provide technical support and assistance for TRIM, primarily via the SIB Information Manager.

10.5 Systems Administrator

The Northern Ireland Civil Service Information Management Unit is the system administrator responsible for systems configuration and management.

11 Responsibilities and Policy Review

The Departmental Records Officer is responsible for the review and updating of this Information Management Policy. As a minimum, this Policy should be reviewed annually and updated as required.

The Chief Executive Officer is responsible for directing the production of the company records management policy.

The Chief Operating Officer, as Departmental Records Officer, is responsible for:

- The production of the company's records management policy.
- Ensuring that this policy is consistent with the statutory and other regulations applicable to the company and its shareholder.
- Overseeing the implementation of the strategy.
- Ensuring that company records are created and maintained in accordance with the policy.
- Managing all records management risks.
- Ensuring that sufficient resources are devoted to these tasks.
- Ensuring that all staff are aware of their responsibilities and have sufficient training to ensure they can be met.

SIB staff are responsible for creating and maintaining records and other information in accordance with this policy and all policies and procedures derived from it.

12 Information Security

SIB Staff should adopt a common sense approach to information security. They are responsible for information that they create or store – see Principles 7 and 8 in the "*Eight Information Management Principles*", Section 7 on page 6.

Particular care should be exercised with information that may be commercially sensitive (e.g. relating to project plans or bid tenders), information supplied by

government departments that is security marked (e.g. “Restricted”, “Confidential”, “Secret”, etc.)[1] or information covered by legislative restrictions. For example, the storage and use of personal data is specifically covered by the Data Protection Act – see Section A2.5 “*Compliance with Statutory and Regulatory Requirements*” in Appendix 2.

13 Information Stored on Portable Devices

SIB staff use laptop PCs, enabling information to be physically removed from the secure environment of the Department of Finance and Personnel (DFP) IT network and Clare House. Similarly, network information may be stored on other portable devices such as Blackberries (e.g. for email), mobile phones or personal digital assistants – PDAs – (e.g. personal contact information), and USB pen drives (flash memory).

There is therefore a significant risk that information may be seen by third parties if such a device is lost or stolen. The primary concern with the loss of a device is the data contained on it. In particular, staff must be vigilant that personal data (as defined in the Data Protection Act 1998) is **not** stored unencrypted on laptops or other memory devices that may be taken out of the office.

Staff should use their discretion over what is stored on portable devices, including their laptops. As with personal data, commercially sensitive data should not be put at risk. So, for example, information relating to bids for an ongoing tender process must not be stored unencrypted on laptops or other memory devices that may be taken out of the office.

13.1 Laptops

Although the laptops are password protected the information on the hard disks is not encrypted and could be recovered using tools available over the Internet. If you need to encrypt sensitive files, you should speak to the Chief Operating Officer. Sensitive information must not be stored on a laptop hard drive unless it is encrypted. In any case the SIB information policy requires that SIB information is stored in TRIM on the network so that it is both secure and backed up. SIB’s information management policy also requires that personal data (as defined in the Data Protection Act 1998) is **not** stored unencrypted on laptops or other memory devices that may be taken out of the office.

13.2 Blackberries

Data is sent to and from Blackberries in encrypted form from a DFP server that is inside the DFP firewall. Therefore emails sent to or received from someone else in the Civil Service Network do not travel via the Internet. They should be as secure as internal emails sent or received via a laptop.

Blackberries supplied through DFP to SIB are password locked by default and five failed attempted logons with a password will cause the contents of the memory to be wiped. SIB staff must ensure that their Blackberry always has password protection enabled; the password protection facility must not be removed.

[1] SIB should not normally hold security marked government information. Advice should be sought from the Chief Operating Officer if such material is received.

Content protection is enabled on the Blackberries supplied to SIB. This means that the data on them is encrypted. Provided the password is not disclosed the data should therefore remain secure even if a Blackberry is lost or stolen.

13.3 Pen Drives and Other Portable Memory Devices

SIB staff must exercise care and responsibility when using portable memory devices such as, pen drives, portable hard drives, flash memory, CDs or DVDs, mp3 players and the like; any of which can be used to copy information from computers or the network. SIB's information management policy requires that sensitive information or personal data (as defined in the Data Protection Act 1998) must **not** be stored unencrypted on laptops or other memory devices that may be taken out of the office. If you need to encrypt sensitive files, you should speak to the Chief Operating Officer.

Appendix 1 Glossary of Terms

The following glossary is provided in order to clarify terms used in relation to the Electronic Document and Records Management System (EDRMS) or information management and that may have a meaning particular to SIB.

Table 3: Glossary of Terms

TERM	DESCRIPTION
Annotations and Redactions	The *TRIM* "Annotation" function allows users to collaborate on selected documents by adding comments on the electronic document itself. The advantage of this is that the comments can be seen in context of the document image. Only *TIFF* images can be annotated and redacted using TRIM; it is not possible to redact or annotate records in other formats (e.g. text, Word or PDF), which would have to be annotated or redacted using their originating applications. The Annotation functionality is based on the concept of margin notes and sticky notes in the paper world. Redactions are used to conceal sensitive data in documents so that they can be published to a wider audience. Redactions allow the publisher to blank or black out data, such as personal or commercially sensitive data. Both Annotations and Redactions in TRIM itself are restricted to scanned images (*.tif and *.tiff) and exclude Office document formats, where the authoring application is recommended.
Archive	A storage facility for documents or records, usually off-site. Generally the records are no-longer current (or no-longer used) but are not yet due for destruction or disposal under the relevant *disposal schedule*. For example, SIB keeps many of its older, paper files off-site in FileStores – see Appendix 3.
Audit Trail	Data which allows the reconstruction of a previous activity, or which enables attributes of a change (such as date/time, operator) to be stored so that a sequence of events can be reconstructed in their correct chronological sequence.
Class	A class is a subdivision of the overall classification scheme by which the electronic *file plan* is organised. A class may be subdivided into one or more, lower level classes: and this relationship may be repeated down the hierarchy. A class does not itself contain *records*; it is an attribute against which a *folder* is classified.
Classification	A systematic identification of business activities (and thereby *records*) into categories according to logically structured conventions, methods and procedural rules represented in a *classification scheme*.
Classification Scheme	A business classification scheme which is an organised structure within which electronic *folders* are placed. This scheme and the folders that are classified against the scheme, make up the *file plan*.
Container	The TRIM name for a folder – see "*Folder*" on page 15.
Declaration (Declared Final)	See "*Final*" on page 14.
Destruction	The process of eliminating *records* beyond any possible reconstruction.

TERM	DESCRIPTION
Disposal Schedule	A set of instructions allocated to a *folder* to determine the length of time for which the folder should be retained by the organisation for business purposes, and the eventual fate of the folder on completion of this period of time.
Document	Information that is stored as a single entity on some medium (e.g. on paper, a computer drive etc.).
EDRMS	Electronic Document and Records Management System.
EIR – Environmental Information Regulations	Statutory instrument under the European Communities Act 1972[1] giving a statutory right of access to information about the environment (subject to certain exemptions).
Export	The process of passing copies of a *record* or group of records with their *metadata* from one system to another system, either within the organisation or elsewhere. Export (rather than *transfer*) does not necessarily mean removing them from the first system.
Extract/Redaction	This is a copy of a *record*, from which some material has been removed or permanently masked. An *extract* is made when the full record cannot be released to a requester, for example under freedom of information, but part of the record can. An *extract* of a whole record is made by removing the parts that can be released from the whole. *Redaction* is the opposite of extraction in that a copy of the whole record/folder is released with the excluded parts redacted or removed. (See also *Annotations and Redactions on page 13*).
File Plan	The full set of *classes*, and the *folders* which are allocated to them, together make up a file plan. The file plan is a full representation of the business of the organisation, within a structure which is best suited to support the conduct of that business and meet records management needs.
Final	The process of defining that a *document's* contents (and some of its *metadata* attributes) are frozen as it formally passes into corporate control and is thereby declared as a *record*. This is done in TRIM using the "Final" function. Documents can be declared "Final" or "Final and remove any previous Revisions", which makes only the final version of the document the record.

[1] www.opsi.gov.uk/acts/acts1972/19720068.htm

TERM	DESCRIPTION
Folder (Container)	Folders (referred to as "containers" in TRIM) are created only at the lowest level class in any single part of the *classification scheme*. They can usually be one of three types; a folder that only contains electronic documents; a physical folder that only contains physical paper documents; or a folder that contains both electronic documents and references to physical paper documents, commonly known as a hybrid folder.[1] An electronic folder is a (virtual) container for records (which may be segmented by *part*). Folders are allocated to a class. A folder is the primary unit of management, and is constituted of *metadata*. Some of this metadata may be inherited from the class to which the folder belongs; and some may be inherited by the records which the folder itself contains. Where this term is used in isolation, it refers to both electronic folders and paper folders (as the latter are represented in the system). Otherwise, it is used only when qualified, e.g. *electronic folder*, *physical folder* to refer to that specific type of folder.
Hybrid Folder	A set of related electronic and non-electronic *records*, some stored in an electronic *folder* within the system and some in a non-electronic *folder* (typically, a *physical folder*) outside the system. A hybrid folder may have several *hybrid part*s. Both electronic and non-electronic elements of the hybrid folder must be managed as one.
Information	Knowledge of some fact, opinion, advice, instruction or occurrence, which is communicated and relates directly or indirectly to the functions of SIB. **Note:** In this Policy the word "information" relates to the term "recorded information": i.e. documentary information.
Inheritance	Principle by which an object can take on a *metadata* attribute of its 'parent' entity, either by ***Inheritance on creation*** where the subordinate (or 'child') object takes the value of that attribute when it is created; or by ***Retrospective inheritance*** where either the attribute of the parent object is changed or the parent object is altered (e.g. by moving a *folder* in the *file plan* so that it has a new parent object).
IMU	Information Management Unit of the Department of Finance and Personnel (DFP), which provides network and other IT services to SIB.
Marker	*Metadata* which describes attributes of a *record* that is stored externally to the system (for example, large paper documents such as building plans, a database held outside the EDRM system, a record on a CD-ROM).
Metadata	Additional data about a *record* or *document* within the EDRMS that is linked to that document, record or other object (literally – Data about Data).
Migration	The process of moving records from one technological platform to another, to refresh software or media formats, while maintaining their authenticity, integrity, reliability and usability.

[1] Note that in the NICS TRIM setup it is not possible to create a folder that is a container for other folders (i.e. nested folders are not allowed).

TERM	DESCRIPTION
OCR	Optical Character Recognition. The process by which any readable text on a scanned image is recognised. This results in an image and text version of a scanned image. Often EDRM systems store these separately but allow searching to return the image using the OCR text. Another alternative used by some EDRM systems is to store the image as a text-on-image PDF file.[1]
Part	A part is a segment of a *folder*; it has no existence independent of the folder. A folder will always contain at least one part which, until and unless a second part is created, is co-extensive with the whole folder. The concept of parts allows the contents of folders which would otherwise be closed to be disposed of in a regular and orderly manner.
Permanent Preservation	The process by which *records* are preserved in perpetuity in a *public record office*, in an accessible and reliable form and which maintains them as authentic records, reflecting their business context and use.
Physical Paper File	A paper file that exists in a filing cabinet or other storage system in an office environment. An EDRMS commonly holds a representation of these as a special type of *folder* which allows management of their location and properties.
Pointer	Method of controlling instances of electronic *records* *classified* against more than one folder, without physical duplication of the document. More than one pointer can be created within the *file plan* to reference a single database object, but each must be logically managed as though separate records for disposal. You create a pointer in *TRIM* with the "Make Reference" function – see *TRIM Reference (.tr5 file)* on page 18.
PRO	The Public Record Office[2] (now called *The National Archives*).
PRONI	The Public Record Office of Northern Ireland[3].
Protective Marking	Designations applied to a *record* to show the degree of security that it should be afforded. One of several words and/or phrases taken from controlled lists, which indicate the access controls applicable to a record.

[1] Adobe's Portable Data Format (PDF) is a de-facto industry standard format for electronic documents and is designed as 'electronic paper' for platform and application independent electronic record access and usage.
[2] www.nationalarchives.gov.uk/
[3] www.proni.gov.uk/

TERM	DESCRIPTION
Record	A *document* which provides evidence of a business transaction or contains information needed to carry on Departmental business. A 'Record' can either be created by or received into SIB. A record may have been created to comply with a legal requirement and NIO records may be required to be produced as evidence in legal proceedings or to satisfy public accountability or parliamentary scrutiny. [A record is a document or other object with a primary value – the purpose for which it was created or captured. It may also have secondary value over time (for example required for a public inquiry or retained for permanent preservation). Once *declared final*, a record cannot be altered and can only be deleted or destroyed in accordance with SIB's policies and procedures by a member of staff authorised to carry out such actions.[1]]
Record Type	All electronic *documents* and *records* must be of a specific record type within the EDRMS which specify particular *metadata* attributes that are required to support a record's integrity and its specific behaviour. The default record type for electronic documents and records within the EDRMS is "Document".
Redact	See "*Extract/Redaction*" on page 13 (See also *Annotations and Redactions on page 13*).
Relate	The *TRIM* "Relate" function allows two or more records to be related or connected with each other. Relationships are useful for grouping records with related information together (e.g. relating a *redacted* version with the original record). Establishing relationships between records can assist people with future inquiries.
Review	The examination of the disposal status of a *folder*, or a *part* of a folder, to determine whether its disposal can take place (i.e. that it should be destroyed, sent to an archive, or retained for a further review at a later date). [As it will be possible to determine the disposal status of some folders and/or parts of folders at the time of creation 'Review' will only apply to those folders or parts of folders where disposal status has not been determined at the point of creation].
Revision	*TRIM* includes the functionality to create multiple Revisions of an Electronic Document. A Revision is basically a modified copy of the document. Multiple Revisions of an Electronic Document can be attached to a single *record*. A document being returned (e.g. after editing) will be added to the record, the older revision being saved as a "previous revision".
TIFF	Short for Tagged Image File Format, TIFF is an image file format that does not lose any quality when it is saved and compressed and is a commonly used format in commercial printing. In *TRIM*, images are stored in TIFF format if they are to be *annotated or redacted*.
TNA	The National Archives[2] (formerly the *Public Record Office*). Note that Northern Ireland has its own public records office, the Public Record Office of Northern Ireland.

[1] In practice, the NICS systems administrators may have to carry out some tasks.
[2] www.nationalarchives.gov.uk/

TERM	DESCRIPTION
Transfer	The process of *exporting* complete electronic *folders* (usually in groups) and subsequently destroying them within the exporting system, effectively transferring custody of the *records*. Records may be transferred for the purpose of permanent preservation in the *Public Record Office*, or some other place of deposit; or following structural changes to the machinery of government, which creates, dissolves or merges organisations.
TRIM (or TRIM Context)	TRIM stands for "Tower Records and Information Management", sold by Tower Software[1] and is the EDRMS adopted by the Northern Ireland Civil Service. SIB is able to use TRIM as part of the services provided to it through the Department of Finance and Personnel (DFP).
TRIM Reference (.tr5 file)	Use the "Make a TRIM Reference" function in *TRIM* to allow the creation of pointers or shortcuts to records held in TRIM. The reference object created by this function contains the record(s) shortcut(s) and can be embedded in other applications, allowing users to quickly view the records in TRIM. The reference object, when double-clicked, will invoke TRIM Desktop and display the selected records. You can transport the reference object by any means you choose (for example, including it in an email message, etc.). Mailing a TRIM reference to a number of staff who may be interested in a given set of documents is a far more effective and network "resource-friendly" method of mailing copies of documents. The TRIM Reference object will appear as a TRIM icon with the record title. The ".tr5" extension stands for "TRIM Reference". Double clicking a TRIM Reference will start a TRIM session; however it will use a current session if it is running. (See "*Pointer*" on page 16).

[1] www.towersoft.com

Appendix 2 Information Management Guidelines

This Appendix describes more specific guidelines governing the management of information within SIB. These underpin the ***eight information management principles*** – see Section 7 on page 6. The Appendix is structured under the following headings:

A2.1 Creation and Capture/Receipt of Information

A2.1.1 Responsibility to Create Records

All staff are under a statutory obligation to create accurate *records* of their activities and to manage and maintain such documentation within the EDRMS. The "*Lord Chancellor's Code of Practice on the Management of Records*"[1] states that:

> *"Records of a business activity should be complete and accurate enough to allow employees and their successors to undertake appropriate actions in the context of their responsibilities, to:*
>
> - *Facilitate an audit or examination of the business by anyone so authorised,*
> - *Protect the legal and other rights of the authority, its clients and any other person affected by its actions, and*
> - *Provide authenticity of the records so that the evidence derived from them is shown to be credible and authoritative.*
>
> *"And that:*
>
> *"Records created by the authority should be arranged in a record keeping system that will enable the authority to obtain the maximum benefit from the quick and easy retrieval of information."*

Staff will consider whether any communication which they receive is relevant to the work of SIB and therefore needs to be captured into the EDRMS.[2] Staff will also consider whether any information, which they create or receive, should be preserved as a record.

[1] Lord Chancellor's Code of Practice on the Management of Records Issued under section 46 of the Freedom of Information Act 2000 November 2002 www.dca.gov.uk/foi/reference/imprep/codemanrec.htm.

[2] For example: information that will be needed by anyone in SIB for future reference or is likely to be of historical significance. Information of an ephemeral or inconsequential nature should not be captured.

A2.1.2 Record Types in SIB

All information stored within the EDRMS must be assigned to a "*Record Type*" – see Appendix 4 for a list of the available record types. The default record type for information created in most Microsoft Office applications is "Document" – "DFP Document" in the TRIM set-up used by SIB.

A2.1.3 Context and Metadata[1]

Appropriate *metadata* will be applied to all *documents* and *records* created, captured and kept by SIB staff. (Wherever practical and feasible, metadata should be determined and entered automatically by the EDRMS.) The originator or recipient of a record will ensure that it is assigned appropriate metadata in the EDRMS, and stored in the appropriate information system. By default, the record should be stored in the EDRMS.

A2.1.4 Intellectual Property of Others (Copyright)

A Document shall not incorporate the intellectual property of others unless SIB has the relevant rights. Staff will not enter documentation (including scanning) into an information system unless SIB owns or has obtained the copyright to do so. Material specifically addressed to SIB can be entered into an information management system.

Staff responsible for scanning documents[2] received from outside SIB will comply with SIB's scanning policy and procedures.[3]

A2.2 Storage and Retrieval of Information

SIB staff have a responsibility to make their information accessible to as wide an audience within SIB as possible, as early as possible. A consistent approach is important to preserving the quality and integrity of our information and ensuring that it can be identified and retrieved in a predictable manner.

SIB staff should consider the wider business goals of SIB when managing information. Staff are required to consider the overall information needs of the business rather than just managing information in a way that simply suits their personal interests or those of their particular project area. Some examples of the implications of this on the way SIB staff should work are as follows:

- Staff should consider the retrieval needs of others within SIB when storing information. For example, this means using a meaningful document title and adding relevant keywords to enable others within SIB to retrieve the document.
- Staff should place documents within the *Corporate File Plan* at the earliest opportunity. Waiting until a document is finalised means that the information it contains may be out of date by the time it is accessible to others in SIB who would have an interest in it.

[1] A definition of *metadata* is provided in Appendix 1.
[2] Further guidance on scanning is provided in DF1/08/47368 "*SIB Scanning Policy*".
[3] See British Standard PD0008, "*Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. British Standards Institute*".

- Staff should structure information in a way that reflects the way SIB works. For example, creating containers that relate to the functions of SIB rather than a narrow "silo" view based on organisational structure.

When staff retrieve a document it is important to know if they are looking at the most recent version or if the information has been superseded in some way. This means that it is important to apply version control and identify the sequence in which documents were created. This is applied within the EDRMS through automated procedures and processes which are largely invisible to the end user.

A2.2.1 Security

Staff have a duty to protect information for which they are responsible, even though it is to be made as widely accessible as possible. There is an equally important requirement to protect information that is in any way sensitive or confidential. Where appropriate, documents should be protectively marked (e.g. to mark them as “unrestricted”, “restricted” or “commercially sensitive”.

The Department of Finance and Personnel network used by SIB is a restricted level network. That is, documents marked more sensitive than “Restricted” should not be stored on it.

A2.3 Dissemination of Information

Staff who receive information not relevant to their own business area will pass it to someone within SIB who can determine whether it should be a record.

Where possible, *pointers*[1] (or *TRIM references*) to documents should be used rather than emailing attachments to multiple addressees to reduce duplication of information. This will also improve the accuracy of information as the most recent version will be accessible.

Note that Department of Finance and Personnel staff and others outside of SIB do not have access by default to SIB records. It is technically possible to give access to particular documents to named DFP staff; the Information Manager can provide more information about how to do this (and advice on whether it should be done).

Staff should consider whether information should be published on the SIB website – see DF1/07/147638 “*Publication Scheme (2007): Strategic Investment Board Limited (SIB)*” or ask the Information Manager for more guidance.

A2.4 Retention & Disposal of Information

Information is captured stored and maintained because it has a value to the organisation. Information that is inaccurate or out-of-date should not be kept (unless there is a clear historical value to the information). Indeed, keeping inaccurate information can be damaging. Staff should therefore aim to delete information that is no longer needed for business purposes and where there is no legal obligation to retain it.

[1] A definition of a *pointer* is provided in Appendix 1.

In particular, the act of finalising a document in TRIM (thereby making it a record) can be used to remove all previous revisions or versions of the document. The audit trail is not affected.

SIB staff cannot delete documents in TRIM themselves but have to make a request to the SIB Information Manager. (SIB staff can finalise documents.)

The retention requirements for many forms of information can be determined at the point of creation or capture. The Information Manger will develop and maintain retention schedules covering all functional areas of SIB. Such schedules will meet the legal requirements for retaining records in relation to functional areas of business, estimates on the time period of retention required to fulfil business need (based on time periods or event realisation) and potential historical value. These schedules will also determine actions to be taken on information either after a set time period or after a particular event. This will ensure that information can be managed with confidence and either be deleted, archived or reviewed for permanent preservation. All retention schedules will be approved by the Departmental Records Officer.

Where there is an applicable generic disposal schedule from the Public Record Office of Northern Ireland (PRONI)[1] (or The National Archives (TNA)[2]), this should be used as the basis for the Retention and Disposal Policy. Any change to information in an information system must not destroy any record unless the relevant Retention and Disposal Policy explicitly permits this.

A2.4.1 Emails

Applying the above guidelines to emails means that if a message conveyed contributes to full understanding of a policy decision, results in an action being taken, or forms a significant part of the "story" it must be kept. If not, it should be deleted. Those emails not required for business needs or which do not need to be retained "for the record" should be deleted as soon as they have ceased to be of use. Emails that are added to the EDRMS should be deleted from inboxes or other storage areas immediately they have successfully been added to the official record. Personal, ephemeral and other emails not added to the official record keeping system should be deleted as soon as they have ceased to be of use. Individual members of staff are responsible for doing this.

SIB may apply limits on the time that emails may be kept outside the EDRMS before automatic deletion. Emails should not be archived from Microsoft Outlook to ".pst" Outlook archive files. Instead, relevant emails should be stored in the EDRMS.

A2.4.2 Records Managed Outside SIB

SIB provides strategic advice on projects to government departments. Responsibility for maintaining the primary records of these projects lies with the Departments themselves. Where the procurement of consultancy support is managed by the Central Procurement Directorate (CPD), the creation and maintenance of records relating to that procurement is the responsibility of CPD.

[1] www.proni.gov.uk/
[2] www.nationalarchives.gov.uk/

To assist SIB's auditors, Strategic Advisors should:

- Include a clause in all operational partnering agreements explicitly stating who has responsibility for the maintenance of records; and
- Where possible, include in SIB's records a note indicating the location and file reference of the departmental records relating to each project.

A2.4.3 Contracts Let Directly by SIB

Where SIB is solely responsible for the letting of a consultancy contract (e.g. to support its own operations), the company must maintain a complete set of records covering all activities, decisions (and their rationale) and communications relating to the contract. Where activities are carried out by Central Procurement Directorate on behalf of SIB, a note to that effect should be included in SIB's records. A check-list of the documentation that should be recorded in the course of a procurement is maintained by the Chief Operating Officer (COO).

Before a contract in which SIB leads is let (e.g. for the provision of consultancy), the records relating to that contract must be inspected by the COO and certified fit for purpose.

A2.4.4 Archiving

Any selection of information to be archived must faithfully reproduce the relevant records. This output must take into account their nature, the operational circumstances of the information system, and include metadata and other contextual information if this is required for the records to be meaningful. For transfer to PRONI (or the The National Archives), it must be in TNA-approved formats and on TNA-approved media.

A2.5 Compliance with Statutory and Regulatory Requirements

Compliance with legal requirements will protect SIB from challenge in the courts – fighting lawsuits is both costly and diverts staff from performing their normal duties. In addition, compliance with regulations will protect SIB from criticism.

Compliance with legislation may operate at several levels within the SIB. For example, there will be legislation that applies to SIB as a whole, such as the Data Protection Act 1998, and all staff need to be aware of their information management responsibilities under such legislation. There are also legal requirements that relate to particular aspects of SIB's business: e.g. contracts need to comply with EC procurement legislation and the information management requirements that this imposes.

A2.5.1 Data Protection Act 1998

All staff are responsible for applying the eight data protection principles as defined in the Data Protection Act 1998[1] (see Appendix 5 on page 33). The EDRMS will make it easier to apply these principles and enable SIB to fulfil its duties effectively under the Data Protection Act. The Departmental Records Officer and Information Manager will provide advice about Data Protection and procedures for handling subject access requests under the Data Protection Act.

[1] http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm.

All staff are entitled to a degree of privacy within the working environment. This also applies to their use of the information system providing that they comply with all usage policies (e.g. email usage policy). To facilitate this, each member of staff is provided with a personal storage container to which only they and system administrators can access. The latter would only do so with the individual's permission and in accordance with the professional code of conduct. When a member of staff leaves SIB, this personal container and all its contents are destroyed.

A2.5.2 Freedom of Information Act 2000[1]

In the interests of public accountability staff should consider placing SIB documents in the public domain unless there is a reason for not doing so (e.g. commercial sensitivity).[2]

The EDRMS will help SIB to carry out its obligations under Freedom of Information legislation. This will be co-ordinated by the Departmental Records Officer and Information Manager, but staff are responsible for ensuring compliance.

A2.6 Redacted or Annotated Records

If a record is redacted (i.e. a copy of the record is made from which some material has been removed or permanently masked) then the redacted copy must be saved as a new record. It **must not** be stored as a new revision or version of the existing document. If a document to be redacted has not been made "Final" then it should be made final in TRIM first **before** the redacted copy is created. The redacted copy can be related to the original record using the "Relate" function in TRIM.

The reason for this is that when a document is finalised the earlier revisions can be removed – only the final version constitutes the evidential record – so the original, un-redacted record would be lost if it had simply added as a new revision.

TRIM has a redaction function that works internally on a TIFF image record. Other documents can be redacted using their native application. For example, Adobe Acrobat v8 has an electronic redaction function that allows content to be blacked out **and removed** from a PDF document. Staff should be aware that simple deletion or "painting" a black box over items to be redacted does not always remove the information from some applications (e.g. Microsoft Word).

Records may have to be redacted when they are published on the SIB website or otherwise released outside SIB (e.g. some costs in a bid proposal may be redacted because of commercial sensitivities).

Alternatively, an extract of a whole record may be made by removing the parts that can be released from the whole. Similarly the extracted record must be saved as a new record that is related to the original.

Annotations can be added to TRIM records that are images using TRIM; otherwise the originating application has to be used. For example, Adobe Acrobat

[1] http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm.
[2] See DF1/07/147638 "*Publication Scheme (2007): Strategic Investment Board Limited (SIB)*".

has extensive annotation functions and Microsoft Word allows the addition of comments, etc.

Appendix 3 Archiving Old Paper Files

SIB's offsite records are managed by Filestores[1] under the overall contract for Clare House. In general the process for sending files to or retrieving files from offsite storage will be the responsibility of the Information Manager. In her absence, when files need to be retrieved urgently, Finance or the Admin team will take this responsibility. SIB staff, as a rule, should never have to deal with Filestores directly as this will be done through the Clare House contact(s) in Information Security branch (CPD).

The following people are the named contacts when dealing with any records held/to be sent offsite:

SIB:	Information Manager (IM)	
Clare House (IS):	Richard McBride, IS Branch	ext 76426
	Julie Wright, IS Branch	ext 76433

A3.1 Sending Files to Offsite Storage for the First Time

Files to be sent offsite for the first time must have been identified as no longer being 'current' or required to be held onsite for business use or reference. Any file to be sent offsite must have been officially 'closed' by the IM or by Finance. Each file must have an SIB reference number and a title which will be entered into the spreadsheet of SIB files currently held by Filestores[2]. This will be done by the IM. In case of her absence either the files should be kept until her return, or the Admin/Finance team will take responsibility of overseeing this process.

Richard McBride in IS Branch (Clare House, Ground floor – directly below SIB, lough-side) will provide flattened Filestores boxes to be constructed. If a large number is required he will have to be notified in advance. Boxes should be packed so that the lid can fit completely and securely onto the box. Ideally files of the same type/on the same topic should be packed together. Each box should be marked clearly with the list of contents (SIB-related titles/reference numbers) in the space provided.

A list of file names and reference numbers should be provided for Richard's team. This information also needs to be included in the spreadsheet Filestores – Files Sent/Received[3] (Files Sent Offsite sheet). Richard's team should be informed when files are ready for collection. He will arrange for collection and will co-ordinate with Filestores.

Filestores will provide their own reference numbers for each box once they have been barcoded and logged. This will be fed back to the IM via Richard McBride. This information **must** be entered into the 'Filestores – List of Files from SIB'

[1] http://www.filestores.com/index.htm
[2] TRIM ref: DF1/07/194972 - Filestores List of Files from SIB
[3] TRIM ref: DF1/08/16371 - FileStores - Files Sent/Received

spreadsheet.[1] Without this information there is a vastly increased chance of records being 'lost' once they are in the care of Filestores.

A3.1.1 The basic process

1. Identify files to be sent offsite
2. Request boxes from Richard McBride
3. Update spreadsheets DF1/07/194972 and DF1/08/16371 with file name and reference number
4. Pack and label boxes. Provide list of files in each box to Richard from list DF1/08/16371.
5. Contact Richard when boxes are ready to be uplifted
6. Richard will provide reference number for each box from Filestores
7. Update spreadsheet DF1/07/194972 with this reference number.

A3.2 Requesting Files from Offsite Storage

A request must be made to the Information Manager (usually via email) to retrieve files from offsite storage. The required files will be identified by file name and reference number from the list of files already held in offsite storage.[2] The Filestores reference numbers should be supplied to Richard McBride who will request the files from Filestores.

The title and reference number of the files requested should be entered into the spreadsheet DF1/08/16371 along with the date requested and which staff member requested the files. When the files are received this list should be consulted to ensure that all files requested have been received and are delivered to the relevant member of staff. The member of staff who requested the files has responsibility for ensuring they are kept safely and securely until they are returned to the Information Manager to be returned offsite.

If there are additional files in the box that are not required by the member of staff the IM has responsibility for guarding these files in a secure area until they can be sent offsite again at some point in the future.

A3.2.1 The basic process

1. Member of staff emails IM with a request to have files retrieved from Offsite Storage
2. IM identifies files required (in conjunction with member of staff) from list DF1/07/194972
3. IM completes list DF1/08/16371 (sheet 2) with name of staff member requesting files and date request made.

[1] As Footnote 3 above
[2] TRIM ref: DF1/07/194972 - Filestores List of Files from SIB

4. Supply Filestores references and SIB titles of files required to Richard McBride
5. When files arrive check against aforementioned list (DF1/08/16371) that all files have arrived. Enter date received on list DF1/08/16371 (sheet 2).
6. IM gives files to relevant staff member advising them of their responsibilities to keep information secure.

A3.3 Sending Files Back to Offsite Storage.

Ideally files will be sent back to offsite storage in the same box in which they were received. This means that the boxes have already been barcoded by Filestores and reference numbers do not need to be changed. Of course this may not always be possible, e.g. when only certain files are required and need to be retained onsite for a longer period of time than the rest of the box's contents.

The relevant steps under section A3.1 'Sending Files to Offsite Storage for the First Time' must then be taken to ensure that a complete list of what has been sent offsite is retained by SIB.

Appendix 4 SIB Record Types

Table 4 lists the TRIM record types available to SIB (there are others that are only available to be created by (e.g.) system administrators: e.g. DFP Personal Containers.

Table 4: SIB Record Types

RECORD TYPE	MAIN USE
DFP Container	Containers below the classification that can be created by the SIB Information Manager and that are used to store documents and records.
DFP Document	To manage the creation and storage of electronic "recorded information". This is the default record type for electronic information created in the standard Microsoft Office applications.
DFP Paper File	To manage the existence of physical documents and records within SIB. (Note that this is only being tested by DFP (at November 2007) and is only available to the SIB Information Manager).
DFP Personal Document	To manage the storage of personal documents by staff. These are restricted to a maximum of 30 documents and are stored in a staff member's "DFP Personal Container". In the NICS TRIM set-up used by SIB documents cannot be moved freely between DFP Containers and DFP Personal Containers (this is an imposed limitation, not a technical limitation). Only the DFP Personal Document record type can be stored in a personal container; similarly a DFP Personal Document type cannot be stored in regular DFP Containers.

Appendix 5 Data Protection

The following is a very brief extract from the Data Protection Act.

The eight data protection principles are defined in the Data Protection Act 1998.[1]

A5.1 The Eight Data Protection Principles

1. 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.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

[1] www.opsi.gov.uk/ACTS/acts1998/19980029.htm.

Appendix 6 External References

A6.1 UK Legislation

Public Records Act 1958[1] and the Public Records Act (Northern Ireland) 1923.[2]

Data Protection Act 1998[3] (See also BSI Data Protection Guide BIP 0012 (formerly PD0012 [4])

Freedom of Information Act 2000[5]

Environmental Information Regulations 1992[6] (as amended 1998)

Freedom Of Information, Environmental Protection, The Environmental Information Regulations 2004[7]

Information Commissioner's Codes of Practice on Data Protection[8]

The "*Lord Chancellor's Code of Practice on the Management of Records*"[9]

Civil Evidence Act 1995[10]

Civil Evidence (Northern Ireland) Order 1997 SI 1997/2983 (N.I.21)[11]

Copyright, Designs and Patents Act 1988[12]

A6.2 Relevant Standards Documents

- British Standards Institution BIP 0008: 2004 *Code of Practice for Legal Admissibility and evidential weight of information stored electronically*. ISBN 0-580 42774-9
- British Standards Institution BIP 0008-2: 2005 *Code of Practice for Legal Admissibility and evidential weight of information communicated electronically*. ISBN 0-580 45672-2
- British Standards Institution BIP 0008-3: 2005 *Code of Practice for Legal Admissibility and evidential weight of linking electronic identity to documents*. ISBN 0-580 45678-1
- BIP 0009-1:2004 *Legal admissibility and evidential weight of information stored electronically. Compliance Workbook* [for use with BIP 008].

---

[1] www.nationalarchives.gov.uk/policy/act/.
[2] www.hmso.gov.uk/legislation/northernireland/nisr/yeargroups/1921-1929/1923/1923anip/aos/c20.htm and www.proni.gov.uk/NIRMS/1923%20act.pdf.
[3] www.opsi.gov.uk/ACTS/acts1998/19980029.htm
[4] See www.bsi-global.com.
[5] www.opsi.gov.uk/ACTS/acts2000/20000036.htm
[6] www.opsi.gov.uk/si/si1992/Uksi_19923240_en_1.htm
[7] www.opsi.gov.uk/si/si2004/20043391.htm
[8] www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practice.aspx.
[9] Lord Chancellor's Code of Practice on the Management of Records Issued under section 46 of the Freedom of Information Act 2000 November 2002 www.dca.gov.uk/foi/reference/imprep/codemanrec.htm.
[10] www.england-legislation.hmso.gov.uk/acts/acts1995/Ukpga_19950038_en_1
[11] www.opsi.gov.uk/si/si1997/19972983.htm
[12] www.opsi.gov.uk/Acts/acts1988/ukpga_19880048_en_1

- BIP 0009-2:2006 *Code of practice for legal admissibility and evidential weight of information communicated electronically. Compliance Workbook* [for use with BIP 008].
- BIP 0009-3:2006 *Code of practice for legal admissibility and evidential weight of linking electronic identity to documents*. *Compliance Workbook* [for use with BIP 008].
- International Standards Organisation ISO 17799 / BS7799 Information Security Management.
- International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001.
- International Standards Organisation ISO 23950 Information and Documentation: Information retrieval (Z39.50): application service definition and protocol specification.
- International Standards Organisation ISO 2788 Documentation: Guidelines for the establishment and development of monolingual thesauri.
- International Standards Organisation ISO 5964 Documentation: Guidelines for the establishment and development of multilingual thesauri.
- MoREQ: Model requirements for Recordkeeping.[1]
- The National Archives[2] (formerly the Public Record Office) – Here you can find…
  i. A home page for Records Management.[3]
  ii. Requirements for Electronic Records Management Systems – 2002 revised requirements.[4] ("The National Archives updated the functional requirements for electronic records management systems (ERMS) in collaboration with the central government records management community during 2002. The revision takes account of developments in cross-government and international standards since 1999").
  iii. Data Protection Act 1998: A guide for record managers and archivists.[5]
  iv. Guidelines for management, appraisal and preservation of electronic records.[6] ("These two guidance documents were produced under the auspices of the Electronic Records from Office Systems (EROS) programme of The National Archives").

[1] www.cornwell.co.uk/edrm/moreq.asp.
[2] www.nationalarchives.gov.uk/ (see also the Public Record Office of Northern Ireland, www.proni.gov.uk/).
[3] www.nationalarchives.gov.uk/recordsmanagement/?source=ddmenu_services1
[4] www.nationalarchives.gov.uk/electronicrecords/reqs2002/
[5] www.nationalarchives.gov.uk/policy/dp/default.htm
[6] www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm

v. Manual of guidance on access to public records.[1] (link to download PDF).

- British Standards Institution BSI DISC PD0025 *Effective records management. Practical implementation of BS ISO 15489-1*.

[1] www.nationalarchives.gov.uk/recordsmanagement/advice/