Records and Information Management Policy

Author:	Sam Pringle
Version:	V3.6a
Date:	29 Nov 2019
HPE Records Manager Ref:	DF1/12/113567 – Unrestricted

The Strategic Investment Board

Contents

Version History **1**

Summary **3**

1 Introduction **5**

2 Scope **5**

3 Definitions **6**

4 Electronic and Non-electronic Documents and Records **7**

5 Eight Information Management Principles **7**

6 Information Management Guidelines **8**

7 Statutory Duty of SIB and its Staff **8**

8 Roles and Responsibilities **9**

8.1 End Users 9

8.2 Information Asset Owner (IAO) 9

8.3 Data Protection Officer (DPO) 9

8.4 Records Manager 10

8.5 Freedom of Information (FOI) Officer 10

8.6 Departmental Records Officer (DRO) 10

8.7 DoF IMU 11

8.8 Systems Administrators 11

9 Responsibilities and Policy Review **11**

10 Information Security **12**

11 Information Stored on Portable Devices **12**

11.1 Laptops 13

11.2 Smartphones and other Smart Devices 13

11.3 USB Sticks and Other Portable Memory Devices 13

12 Official Information on or in Non-official Systems **14**

12.1 Associate Advisers 14

12.2 Business Records 14

12.3 ICO Guidance 15

Appendix 1 Staff Using Their Own Equipment **17**

A1.1 The Risks 17

A1.2 The Extension to Policy 17

Appendix 2 Information Management Guidelines **21**

A2.1 Creation and Capture/Receipt of Information 21

A2.1.1 Responsibility to Create Records 21

A2.1.2 Record Types in SIB 22

A2.1.3 Context and Metadata 22
A2.1.4 Intellectual Property of Others (Copyright) 22
A2.2 Storage and Retrieval of Information 22
A2.2.1 Security 23
A2.3 Dissemination of Information 24
A2.4 Retention and Disposal of Information 24
A2.4.1 Emails 24
A2.4.2 Private Email Accounts and Other Data Stores 25
A2.4.3 Records Managed Outside SIB 25
A2.4.4 Contracts Let Directly by SIB 25
A2.4.5 Archiving 26
A2.5 Compliance with Statutory and Regulatory Requirements 26
A2.5.1 Data Protection 26
A2.5.2 Freedom of Information Act 2000 27
A2.6 Redacted or Annotated Records 27
Appendix 3 Archiving Old Paper Files 29
Appendix 4 SIB Record Types 31
Appendix 5 Data Protection 33
Appendix 6 External References 35
A6.1 UK Legislation 35
A6.2 Relevant Standards Documents 36
Appendix 7 Glossary of Terms 39

Version History

Table 1: Version History

VERSION NUMBER	VERSION DATE	SUMMARY OF CHANGES
2.0	31-Mar-12	• Policy reviewed, updated and reissued. [Previous version is at DF1/07/185351] • Appendix 3 "*Archiving Old Paper Files*" deleted and rewritten to reference the procedures and records stored in HP Records Manager. • Some of the direct National Archives document links in Appendix A6.2 removed as they no-longer work.
3.0	20-Feb-13	• Policy reviewed and updated as a new revision. • Changes in regard to corporate and information governance procedures – see DF1/13/82970 "*Letter from Noel Lavery to Brett Hannam re Corporate and Information Governance procedures - 22 January 2013*". • References checked and updated as necessary. • Reviewed against the latest "*DoF Records Management Staff Handbook*" (draft). • Numerous minor changes in wording. • "Glossary of Terms" moved to end at Appendix 7 on page 39.
3.1	8-Jul-13	• Review and update • Changes to cover records in social media and private emails in light of ICO guidance issued – see particularly Section 12 "*Official Information on or in Non-official Systems*" on page 14.
3.2	2-Mar-15	Review and update as needed. Mostly minor updates and changes to wording to reflect changes in technology.
3.5	28-Jun-16	Review and update as needed. • Changes to reflect TRIM being renamed as HP Records Manager. • Changes to accommodate the different employment models used by SIB • Added Appendix 1 "*Staff Using Their Own Equipment*".
3.6	1-Aug-18	Review and update as needed. Changes made to reflect GDPR and DPA 2018.
3.6a	29-Nov-19	Review and update as needed.

Summary

This document defines an Information Management Policy for SIB. It outlines its scope and sets out eight information management principles. Everyone in SIB must:

- 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. This means using the information and records m management system – HPE Records Manager (HPERM, previously called HPRM, and before that TRIM) –either within SIB or within the organisation where staff are embedded.
- Manage information in a cons
- istent manner across SIB.
- Record in SIB systems 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 the data protection legislation – see DF1/09/287091 "*SIB GDPR and Data Protection Policy and Procedures*" – and all other, relevant statutory and regulatory requirements relating to information.

This document also:

- Describes the roles and responsibilities of staff who are responsible for managing SIB records and other information assets.
- Provides a framework for information governance and assurance.

More detailed guidelines for information management within SIB are provided in DF1/07/185398 "*SIB Information Management Procedures*".

Key responsibilities are summarised Table 2 below.

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

ROLE	RESPONSIBLE FOR	INFORMATION ASSET RESPONSIBILITIES
End Users (Everyone in SIB)	Creation, capture, storage, dissemination and retrieval of information as records that are stored in HPERM. Ensuring complete business records are maintained of their activities.	Where embedded with other organisations they must ensure adequate records are maintained both for SIB and the host organisation.
Information Asset Owner	Some users may also have ownership of or responsibility for particular information assets	IAOs should understand what information is held, what is added and

ROLE	RESPONSIBLE FOR	INFORMATION ASSET RESPONSIBILITIES
(IAO)	within SIB.[1] The CEO is the overall IAO for SIB.	what is removed, how information is moved, and who has access and why.
Data Protection Officer (DPO)	Compliance with the General Data Protection Regulation (GDPR) and data protection legislation.	This is a formal appointment under GDPR. Within SIB the same person, Sam Pringle, is Data Protection Officer (DPO), Records Manager and Freedom of Information (FOI) Officer.
Records Manager[2]	Providing information and records management for SIB, including responsibility for the SIB Corporate File Plan. Coordinating high level searches for Data Protection, Freedom of Information and other legislative information requests.[3]	May also be an Information Asset Owner and should advise the other IAOs, in particular the CEO. Maintains the Information Asset Register and accreditation of SIB Information Systems.
Freedom of Information (FOI) Officer	Managing Freedom of Information Requests.	None.
Departmental Records Officer (DRO)	The CEO is the Departmental Records Officer. Although SIB is an Arm's Length Body (ALB), 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.	Senior Information Risk Owner (SIRO) who has overall responsibility for the organisational function of records management.
DoF IMU	*The Department of Finance Information Management Unit (DoF IMU) provide technical support and assistance for HPERM, primarily via the SIB Records Manager.*	*Integrity of SIB HPERM.*
Systems Administrators	*The Department of Finance Information Management Unit (DoF IMU) is the system administrator responsible for HPERM.*	*Integrity of SIB HPERM.*

This document also cross references other documents relevant to records and Information Management.

[1] See DF1/12/465023 "*SIB Information Asset Register*", which lists key information assets and identifies their IAO, and FI1/18/114386 "*SIB GDPR Documentation as a Data Controller*", which identifies information assets containing personal data.

[2] The Information and Compliance Manager is the Records Manager for SIB.

[3] The Records Manager is a "power user" in the Northern Ireland Civil Service terminology.

1 Introduction

This document provides an information management policy for the effective and efficient management of SIB's *documents* and *records* (i.e. recorded information) and its *information assets*.[1]

SIB depends totally on information, making information one of the SIB's most important assets. Much of this information is irreplaceable if destroyed so it must be managed consistently and effectively, which is essential to the efficiency and effectiveness of SIB. The right people must have access to the right information when they need it: *HPE Records Manager* (HPERM) helps to achieve this. However, the full benefits can only be realised if staff comply with the information management policy and procedures.

SIB is obliged to maintain adequate business records to support all its transactions and business decisions. These records must be sufficiently robust to support SIB in any legal actions that may involve the company and to satisfy SIB's auditors.

Information Assurance is a potential risk both for SIB and its sponsor Department, The Executive Office (TEO). This risk is relevant not only in terms of the fines that could be imposed if guidelines were breached but also because of the risk of reputational damage to SIB and TEO, if information assurance breaches were identified.

To satisfy these requirements, 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.
- Provide an overarching framework for information governance and assurance.

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

2 Scope

This Policy covers **all** recorded information and the systems used to manage or store it. Collectively these are referred to as "information assets". The policy applies whatever the medium used for storage: e.g. electronic or paper, tape recordings or transcripts; and whether information originates within SIB or from outside.

The Policy excludes information such as telephone conversations, on-line "chat" applications (e.g. Cisco Jabber), meetings, video conferences, 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

[1] Blue/underlined hyperlinks are terms defined in the "Glossary of Terms" in Appendix 7.

principles and, where appropriate, the systems should be managed as SIB Information Assets. 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.

All records in SIB are stored electronically in HPERM, except where other records management systems are appropriate and sanctioned for this purpose by the CEO: e.g. the Finance or HR systems.

Note that all official information is still held on behalf of SIB (and therefore subject to a Freedom of Information Request) even if held in an individual's private email account or on their personal computer, data store, etc. (see Section 12 on page 14).[1] This is particularly the case for Associate staff who may be using their own IT equipment to carry out assignments.

3 Definitions

Certain words in this Policy have specific meanings and these are explained in the "Glossary of Terms" in Appendix 7 on page 39. However, two terms are fundamental to records and information management; "document" and "record".

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.

A business ***record*** can be defined as:

A document that has content, context and structure and that 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 come from 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 or business decision.

[1] See also the ICO guidance on "*Official information held in private email accounts*".

4 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 *HPE Records Manager*.[1]

Where storage in HPERM is not possible or inappropriate, documents and records should still be managed using HPERM. 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.

Some electronic information may be stored in or managed by approved archives other than HPERM. For example, Finance records in Pegasus Opera or HR records in the Hallmark HR system. However, unapproved archives such as Outlook "PST" files or laptop hard disks must not be used to store SIB records.

5 Eight Information Management Principles

SIB has adopted the following eight information management principles to facilitate effective use of its information.

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:

[1] Retrospective management of older paper documents using HPERM have only been completed as required. All documents created after 1 April 2007 should be managed by and stored electronically in-HPERM.

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 any relevant statutory, regulatory and protective marking requirements – including the requirement not to destroy information where there is a legal obligation to retain it.

6 Information Management Guidelines

All staff have a statutory obligation to create accurate *records* of their business activities and to manage and maintain such documentation within HPERM. Specific guidelines for managing information are provided in Appendix 1 on page 17. These underpin the eight information management principles and are structured under the following headings:

- Creation and Capture/Receipt of Information – on page 21
- Storage and Retrieval of Information – on page 22
- Dissemination of Information – on page 24
- Retention and Disposal of Information – on page 24
- Compliance with Statutory and Regulatory Requirements – on page 26.
- Redacted or Annotated Records – on page 27.

7 Statutory Duty of SIB and its Staff

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

- Records decisions, the rationale for decisions or provides authority for action – evidential information.
- 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 that needs to be retained.
- Is legally required to be kept by any legislative provisions.

Information of an ephemeral or inconsequential nature, or purely personal information, does not need to be captured as a record. Staff should also bear in mind the need to write in clear, unambiguous English; avoiding clichés and unnecessary jargon.

8 Roles and Responsibilities

There are various roles within SIB relating to the management of information. These are summarised in Table 2 on page 3 and covered in more detail below.

8.1 End Users

All SIB staff are end users who are responsible for all processing of information within their areas of work, including:

- Creation, capture, storage, dissemination and retrieval of information as documents and records that are stored in HPERM.
- Ensuring complete business records are maintained of their activities.
- Ensuring compliance with legislation: e.g. the data protection legislation that applies to personal information.

They have an obligation under legislation to declare records that demonstrate actions taken by them on behalf of SIB.

SIB staff may be embedded in other organisations even though they remain SIB employees. In such cases, they must ensure adequate records are maintained both for SIB and the host organisation. This means that only records pertinent to SIB – that record SIB business – are stored in SIB's systems. In many cases the project that embedded staff are working on belongs to the host organisation (e.g. an NICS Department) and it is appropriate that the project records are stored in that organisation's records management systems. However, some records may relate additionally to SIB in which case they should be copied also to SIB's HPERM where necessary.

8.2 Information Asset Owner (IAO)

Some users may also have ownership of or responsibility for particular *information assets* within SIB. For example, the Finance Manager has ownership of the financial information and data that are stored in Pegasus Opera (the SIB Accounting System). These "information assets" should all be identified and recorded in the "*SIB Information Asset Register*" (DF1/12/465023). Personal data assets have additional record keeping required under GDPR – see Section 8.3 below.

For each Information Asset, the IAO should understand what information is held, what is added and what is removed, how information is moved, and who has access and why. Where appropriate they should seek advice from the Information and Compliance Manager.

8.3 Data Protection Officer (DPO)

The DPO is an official appointment under GDPR, which imposes certain legal responsibilities. Amongst these are ensuring that records are kept of information assets containing personal data – see FI1/18/114386 "*SIB GDPR Documentation as a Data Controller*".

The DPO's minimum tasks are defined in GDPR Article 39, to:

- Inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- Be the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc.).

Within SIB the same person, Sam Pringle (the Information and Compliance Manager), is Data Protection Officer (DPO), Records Manager, and Freedom of Information (FOI) Officer.

8.4 Records Manager

The SIB Information and Compliance Manager is also the SIB Records Manager. The Records Manager is responsible for the SIB Corporate File Plan structure. He also provides and updates retention and disposal schedules for all types of information and archives, and manages the disposal of SIB information in accordance with these schedules.

The Records Manager may be an Information Asset Owner in his own right but primarily he manages and advises the other IAOs. He maintains the Information Asset Register and the accreditation of SIB Information Systems (such as Pegasus Opera). Information Assets and accreditation are recorded in the "*SIB Information Asset Register*" (DF1/12/465023).

There is an SIB code of conduct for records management, DF1/07/174788 "*Code of Conduct for SIB Records Management*".

The Records Manager receives his delegated authority through the Departmental Records Officer (DRO) – the CEO.

8.5 Freedom of Information (FOI) Officer

The Records Manager (reporting to the Chief Executive Officer) is responsible for Freedom of Information requests made to SIB and may undertake necessary searches needed to fulfil SIB's statutory duties. More guidance can be found in DF1/09/253908 "*Managing Freedom of Information (FOI) Requests: Procedures for SIB*".

8.6 Departmental Records Officer (DRO)

Although SIB is an arm's length body (ALB), 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 CEO is the Departmental Records Officer.

The CEO is also the Senior Information Risk Owner (SIRO) for SIB who has overall responsibility for the organisational function of records management. In practice he delegates much of the day-to-day management of records to the Records Manager.

8.7 DoF IMU

The Department of Finance Information Management Unit (DoF IMU) provide technical support and assistance for HPERM, primarily via the SIB Information and Compliance Manager. IMU's primary responsibility from SIB's perspective is maintaining the integrity and security of SIB HPERM records system. (SIB uses part of the DoF HPERM dataset for records management).

8.8 Systems Administrators

DoF IMU staff are HPERM system administrators for SIB. ITAssist is responsible for the technical support for HPERM. ITAssist maintains the network within which many of SIB's information assets reside. For example the Pegasus Opera accounts system is held on network servers and accessed using laptops supplied and maintained by ITAssist.

9 Responsibilities and Policy Review

As Departmental Records Officer, the SIB CEO is responsible for the review and updating of this Information Management Policy, which he delegates to the Information and Compliance Manager as necessary. This Policy should be kept under review and updated as required.

The CEO is responsible for directing the production of the company records and information management policy. Amongst other things, he is overall responsible for:

- This policy document.
- Ensuring the policy is consistent with the statutory and other regulations applicable to SIB.
- Overseeing the implementation of the policy.
- Ensuring that corporate records are created and maintained in accordance with the policy.
- Managing records management risks
- Information governance and assurance.
- 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.

In practice, the CEO delegates day-to-day responsibility for records and information management to the Information and Compliance Manager.

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.

10 Information Security

The "*SIB Security Policy and Procedures*" can be found at DF1/09/287618 and the "*SIB Procedures on Loss or Theft of Data or ICT Devices*" can be found at DF1/12/458202. The "*SIB Business Continuity Plan"* (updated annually under the HPERM classification FI21/8/3 "…*Emergency Plans*") also references procedures to follow if a laptop or other device is lost or stolen as well as actions to take where there is a threat of data loss or a lost access to information.

Where personal data is lost or stolen, that may need to be reported to the Information Commissioner's Office (ICO) – see FI1/18/711216 "*SIB Personal Data Breach Management Plan*".

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 5 on page 7.

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 has protective security markings[1] or information covered by legislative restrictions.

11 Information Stored on Portable Devices

The majority of SIB staff use encrypted laptop PCs, enabling information to be physically removed from the secure environment of the NICS IT network and Government buildings. Similarly, network information may be stored on other encrypted portable devices such as smart phones or tablets.

There is a 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 is **not** stored unencrypted on laptops or other storage devices (e.g. CDs, DVDs, USB sticks, etc.) that may be taken out of the office.

Staff **must not** transfer or store SIB personal data, any sensitive commercial information or any Government security marked data to non-NICS personal devices such as home computers, phones or PDAs; except with the permission of the information owner (e.g. a Government Department). Facilities exist to use office laptops to work remotely should this be necessary. For example staff must not auto-forward emails or other documents containing such data to personal or other non-business email accounts or to online data stores. Particular care should be taken with personal computers or other devices that automatically synchronise or back up data to the "Cloud" or similar on-line storage.

IT Security policy is set to minimise or prevent loss of unencrypted data. Only authorised, encrypted official USB drives can be connected to network laptops and CD/DVD

[1] SIB should not normally hold security marked government information, however all Northern Ireland Civil Service are by default OFFICIAL, even if they do not bear a marking. Advice should be sought from the CEO or the Information and Compliance Manager if protectively marked material is received.

drives have write access disabled. The hard drives of all SIB laptops are encrypted using a bit-locker key that is personal to the user.

Even so, 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 should not normally be stored on laptops or other memory devices that may be taken out of the office.

11.1 Laptops

All SIB laptops are encrypted using a key that is personal to the user.

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 HPERM 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.

The contents of laptop hard drives are not backed up on the network. Therefore they must not be used to store records. (Staff can temporarily save documents on hard drives to work on them off-line or so they are accessible off-line, subject to the guidance and restrictions imposed in this policy).

11.2 Smartphones and other Smart Devices

Data is sent to and from official smart devices in encrypted form from an NICS server that is inside the NICS 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.

Smartphones supplied through ITAssist 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 smartphone always has password protection enabled; the password protection facility must not be removed.

Content protection is enabled on the smartphones supplied to SIB. This means that the data on them is encrypted. Provided the password(s) is not disclosed the data should therefore remain secure even if a smartphone is lost or stolen. However, if a smart device is lost or stolen this must be reported as soon as possible to ITAssist and to the SIB Chief Executive Officer. The user should follow the procedures in "*SIB Procedures on Loss or Theft of Data or ICT Devices*" (DF1/12/458202) and the current "*SIB Business Continuity Plan*".

If staff use other mobile devices for official work (or non-SIB smart devices) they must follow this policy in safeguarding information.

11.3 USB Sticks and Other Portable Memory Devices

IT Security policy should prevent copying information to unauthorised devices. However, SIB staff must exercise care and responsibility when using portable memory devices

such as USB sticks, 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 **must not** be stored unencrypted on laptops or other memory devices that may be taken out of the office and nor should it be sent by insecure means (e.g. by email over the Internet).

12 Official Information on or in Non-official Systems

As a general rule official (i.e. SIB) information should not be stored in non-official systems. Staff may temporarily work on SIB documents on non-official Systems provided that they adhere to this policy and the "*SIB Security Policy and Procedures*" (DF1/09/287618). For example, it may be acceptable to work on a copy of a non-sensitive document on a home PC (provided that the original was stored in HPERM and that the copy is secured). It would not be acceptable to transfer a protectively marked document to a home PC to work on it without the permission of the information owner (e.g. an NICS Department).

See Appendix 1 "*Staff Using Their Own Equipment*" on page 17 for more guidance.

12.1 Associate Advisers

Some staff – e.g. Associate Advisers – will predominantly be using their own computing equipment to do work for SIB (or its clients). However, they should still follow the security principles set-out in this and other SIB policies (with appropriate modifications as necessary). Associate Advisers in the SIB Strategic Support Unit (SSU) or the Council Support Unit (CSU) should review with their line manager the security risks for each work package they take on. Where necessary only officially supplied IT equipment may have to be used for a particular piece of work rather than the Associate's own IT equipment.

Associate Advisers using their own IT Equipment must still meet IT security requirements set by SIB for this purpose. These requirements are set out in Appendix 1 "*Staff Using Their Own Equipment*" on page 17.

12.2 Business Records

SIB policy is that all its business records must be saved in HPERM. This means, for example, that business emails should be saved in HPERM and not left in Outlook (see Appendix A2.4.1 on page 24). **Any *business records* in any non-business system must be saved in HPERM** (unless they are already stored in another approved SIB records system: e.g. Finance records are stored in Pegasus Opera). Laptop hard drives, SIB-supplied USB sticks, and the like are not approved SIB records systems. Nor for that matter is Outlook or any other email program.

Associate Staff or staff embedded with other public authorities who may not have access to HPERM should agree arrangements with their line manager(s) to ensure that SIB business records are properly filed. Staff embedded with other public authorities may in practice be saving business records in the host organisation's records management systems because they are records for the host's business and not SIB.

If staff use non-SIB email accounts (e.g. private email accounts) for business purposes they must save copies of any business-related emails to HPERM. As a general rule, staff should not use private email accounts for SIB business purposes. The only exceptions to this are staff such as Associates who are required by their contract to provide their own business equipment or where it has been agreed with the CEO for a particular reason.

If staff use social media for business purposes (e.g. Twitter or Facebook), they should save to HPERM copies of any business-related messages, etc. that constitute a record.

If staff send an SMS message (e.g. from their official smartphone) and this is a business record, it should be saved in HPERM. (The easiest way to do this is to forward the SMS message to an email account and then save the received email in HPERM).

12.3 ICO Guidance

The Information Commissioner has made clear that official information is still held on behalf of a public authority (and therefore subject to a Freedom of Information Request) even if it is held in an individual's private email account or on their personal computer, data store, etc. The ICO has issued guidance on "*Official information held in private email accounts*" and this guidance has wider application to all official information or records held in private or unofficial systems.

"The definition of information under FOIA is provided at section 84 and states that ""information" … means information recorded in any form". Therefore, official information recorded on mobile devices, including text messages on mobile phones, or in any other media, may also be considered to be held on behalf of the public authority in the circumstances outlined in this guidance." [ICO guidance note, "*Official information held in private email accounts*"]

The definition of information for the purposes of official or business records for SIB includes social media and the like. SIB staff must capture and store in HPERM all official records from such "data stores". This will ensure that the information can be made available in response to a Freedom of Information request (but that is not the only reason for saving business records).

SIB staff should be aware that deleting or concealing information with the intention of preventing its disclosure following receipt of an information request is a criminal offence under section 77 of the Freedom of Information Act. For example, where information that is covered by a request is knowingly treated as not held because it is held in a private email account, this may count as concealment intended to prevent the disclosure of information, with the person concealing the information being liable to prosecution.

Appendix 1 Staff Using Their Own Equipment

This section extends the Records and Information and Management Policy where non-SIB-provided IT equipment or facilities are used. Although primarily for Associate Strategic Advisers (staff on variable-hours contracts who provide their own IT equipment) it applies equally – with appropriate adjustments – to other staff who may use non-SIB IT equipment.

A1.1 The Risks

There are information security risks to SIB in all its work (i.e. not just that carried out by Associates). These include:

- Security breaches/leaks of politically sensitive material or information (e.g. to the media).
- Similarly for material or information that is commercially sensitive.
- Reputational risks to SIB were a data/information breach or similar incident to occur.
- SIB Business records not being saved in HPERM.

The potential consequences of a data breach incident could range through reputational, embarrassment at information revealed, to commercial costs if, say, a tender process was compromised and had to be rerun. The biggest risk of a data breach arises not where emails are sent via non-governmental email addresses (e.g. Gmail) – since by and large these are encrypted in transmission – but rather from where the information may be stored: e.g. on portable and non-encrypted devices that are easily stolen or lost. This is particularly so for devices that are not under SIB's control and management. SIB would have to be able to demonstrate that appropriate and reasonable precautions had been taken.

Note in particular that GDPR imposes legislative requirements with regard to the security of personal data.

The Associate contract model requires that Associates supply their own IT kit. Furthermore, the risk is exacerbated for Associates because they vary in their IT knowledge, they may not be security trained or aware and, as many of them are sole or small practitioners, they may not have access to secure back-up facilities, adequate patching of software, etc.

A1.2 The Extension to Policy

After internal review by SIB, the following extension to the Records and Information Management Policy were approved. The aim is to take proportionate action that varies according to the risks identified for each piece of work and to minimise or mitigate the risks of data breaches happening with the consequential reputational or commercial risk.

1. **A risk analysis** (recorded in HPERM) is included for each piece of work to be assigned. Prior to the assignment this should record whether the potential risk warrants requiring the work to be carried out on an SIB-supplied laptop or As-

sociate-owned IT kit. The risk should give suitable weight to impact over likelihood when considering the possibility of a data/information breach.[1]

2. For **substantial pieces of work or work deemed to be high risk**, an Associate may be required to use only an SIB laptop. Work deemed to be high risk should include:
    a. Commercially, or politically sensitive work as identified in the risk analysis (1 above).
    b. Any work involving personal data.
    c. The definition of substantial or high risk is flexible and at the discretion of the head of the Strategic Support Unit (or the line manager) in discussion with the advisor and any other interested parties.
3. Associates must meet or exceed **minimum information security standards** as follows:
    a. That their PC uses whole disk encryption – or an equivalent software encrypted partition to be used.
    b. The operating system(s) and all software is patched and kept up-to-date automatically (e.g. Microsoft update).
    c. Any mobile devices – e.g. smartphones, tablets, etc. – are similarly encrypted.
    d. Their data and work for SIB are backed up on a separate secure encrypted hard disk or on a secure on-line "cloud" using secure, encrypted communication. (Subject to 1and 2 above, Microsoft Onedrive or iCloud are accepted as secure for this purpose).
    e. Data/work for SIB must not be stored on unencrypted devices – e.g. USB sticks, CD-ROMs, etc.
    f. Anti-virus is both up-to-date and set to automatically update.
    g. Software and hardware firewalls are used. As examples, Windows Defender would be acceptable software and most home routers incorporate a hardware firewall.
    h. That the Associate warrants that all the above have been addressed competently or that they have paid a qualified security professional or security company to ensure that it has been done.
4. That only **encrypted email** services are used.
5. SIB business records must be saved in HPERM and this should be done through the heads of SSU or CSU or the line manager if the member of staff does not have access to HPERM.

[1] Note that legislation may require risk assessments – e.g. a Data Protection Impact Assessment (DPIA) where personal data is being processed.

Any substantial variations or exceptions to this policy must be sanctioned by the CEO (who is the Information Asset Owner for SIB). So, for example, an Associate using their own network/IT system that meets or exceeds the minimum standards would be allowed to use this for all work at the discretion of the CEO recorded in writing.

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 5 on page 7. The Appendix is structured under the following headings:

- Creation and Capture/Receipt of Information – below
- Storage and Retrieval of Information –on page 22
- Dissemination of Information – on page 24
- Retention and Disposal of Information – on page 24
- Compliance with Statutory and Regulatory Requirements – on page 26.
- Redacted or Annotated Records – on page 27.

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 HPERM. The "*Lord Chancellor's Code of Practice on the Management of Records*" 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 HPERM.[1] Staff will also consider whether any information, which they create or receive, should be preserved as a record.

[1] For example: evidential information of SIB business, 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 HPERM 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 when filing a record in HPERM is "DoF Document".

A2.1.3 Context and Metadata

Appropriate *metadata* should 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 HPERM.) The originator or recipient of a record should ensure that it is assigned appropriate metadata in HPERM, and stored in the appropriate information system. By default, the record should be stored in HPERM.

A2.1.4 Intellectual Property of Others (Copyright)

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

Staff responsible for scanning documents received from outside SIB should comply with SIB's scanning policy and procedures.[1]

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, using a meaningful document title and including relevant keywords to enable others within SIB to retrieve the document.
- Staff should place documents within the *Corporate File Plan* (i.e. HPERM) 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. Note that the title for a document can be edited: so, for example, the title of a draft document can be prefixed with "[DRAFT]" until it is ready (at which point the word "[DRAFT]" can be removed.

[1] See DF1/08/47368 "*SIB Scanning Policy*" and 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.
- Revisions or drafts should be saved or destroyed depending on the circumstances. Thus editing a document in HPERM will automatically save drafts as one goes along. However, once a document is "final" – e.g. it may be the final version of a report created for and sent to a client – it should be finalised as a record in HPERM. When making it final consider whether to make it final and remove all previous versions (which is one of the options in HPERM).

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 HPERM through automated procedures and processes meaning that earlier revisions are stored (and accessible if needed).

As HPERM maintains version (or revision) control**, staff should not save multiple copies or revisions of the same document; each of which would have a different HPERM reference!** However, staff should create new copies where appropriate. For example, a register of FOI requests for (say) 2012/13 would be closed at the end of the accounting year and a new register created for 2013/14. Similarly the "*Investment Strategy for Northern Ireland 2008–18*" is a separate document from the "*Investment Strategy for Northern Ireland 2011–21*". However, each of those documents would have multiple revisions all maintained under the same record number in HPERM. The top record is always the latest revision.

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". For example, this policy document is marked "Unrestricted" in the page footer; meaning it could be published if necessary (subject to clearance with the CEO).

SIB does not apply Government protective markings (normally capitalised – e.g. "OFFICIAL") although it does respect them (e.g. in information received).

- The NICS network used by SIB is an OFFICAL level network. That is, documents marked more sensitive than "OFFICIAL" should not be stored in it.[1]
- All SIB containers within HPERM have been restricted at a minimum to "DoF SIB", meaning that HPERM users outside SIB should not be able to access the records within them.
- Some containers are further restricted (e.g. to Finance or HR staff).

[1] So be particularly careful with documents from clients with more secure networks: e.g. DoJ or PSNI.

- Staff can change the access to individual HPERM records themselves either opening access to non-SIB users or further restricting the record within SIB. (Note that any restricted records **must** have "DoF SIB IM Function" included in the access list).
- The Information and Compliance Manager can change the restriction on containers. For example, confidential or commercially sensitive project containers may have increased security applied for a limited period.
- There is a legal requirement under data protection legislation to keep personal information secure.

For more information see DF1/09/287618 "*SIB Security Policy and Procedures*" and FI1/18/11611 "*[DRAFT] A Summary of the General Data Protection Regulation*".

A2.3 Dissemination of Information

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

Where possible, staff should email *HP Records Manager references* to documents rather than emailing attachments to multiple addressees to reduce duplication of information. Emailing the link rather than the document means that accidental or unauthorised recipients cannot access the document.

Department of Finance 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 NICS staff; the Information and Compliance Manager can provide more information about how to do this (and advice on whether it should be done).

Staff should consider whether information ought to be published on the SIB website or ask the Information and Compliance Manager for more guidance.

A2.4 Retention and 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). In particular, the act of finalising a document in HPERM (thereby making it a record) can be used to remove all previous revisions or versions of the document. The audit trail is not affected.

The disposal of records and other information should be carried out in accordance with SIB's policies that have been agreed with the Public Records Office Northern Ireland (PRONI). These can be found at DF1/11/237031 "*SIB Electronic Document Retention and Disposal Policy*" and DF1/11/161984 "*SIB Document Retention and Disposal Policy for Paper Records*".

Note in particular that GDPR requires that personal data should be retained no longer than is necessary.

A2.4.1 Emails

If an email 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 HPERM may be deleted from inboxes or other storage immediately they have successfully been added to the official record.[1] Personal, ephemeral and other emails not added to the official record keeping system may be deleted as soon as they have ceased to be of use. Individual members of staff are responsible for doing this.

Be careful that emails are not "lost" under the email retention policies before they have been files as records in HPERM. The default for Outlook is that emails older than three months are automatically deleted both locally and on the email servers.

Emails should not be archived from Microsoft Outlook to ".pst" Outlook archive files. Instead, relevant emails should be stored in HPERM.

A2.4.2 Private Email Accounts and Other Data Stores

See Section 12 "*Official Information on or in Non-official Systems*" on page 14.

A2.4.3 Records Managed Outside SIB

SIB provides strategic advice on projects to Government Departments and other public sector organisations. 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.

To assist SIB's auditors, Strategic Advisors should ideally:

- Include a clause in all operational partnering agreements (OPAs) 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.

Where primary records for a project are maintained elsewhere than SIB the Strategic Adviser should confirm this by email to the Information and Compliance Manager. The email should be filed in the appropriate project container as a record.

A2.4.4 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 procurement is maintained by the Chief Executive Officer (CEO).

[1] In any case, IT policy on email accounts is set by default to delete emails within Outlook after three months. It is better not to rely solely on this: i.e. delete emails as soon as they are filed (or no longer needed).

Before a contract in which SIB leads is signed (e.g. for the provision of consultancy), the records relating to that contract must be inspected by the CEO, Legal Director or other responsible officer and certified fit for purpose.

A2.4.5 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.[1]

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 GDPR, 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

All staff are responsible for data protection. The General Data Protection Regulation (GDPR) came into law on the 25th May 2018.[2] The UK has implemented GDPR by way of the Data Protection Act 2018[3] (25-May-18, DPA 2018) that replaces the previous Data Protection Act 1998 and supplements the reforms to data protection laws that are contained in GDPR.

Where a data breach involves personal or sensitive personal data SIB should follow FI1/18/711216 "*SIB Personal Data Breach Management Plan*".

The Data Protection Officer will provide advice about Data Protection and procedures for handling subject access and other requests under the Data Protection Act.[4] See DF1/09/287091 "*SIB GDPR and Data Protection Policy and Procedures*" for more information.

---

[1] See also DF1/11/161984 "*SIB Document Retention and Disposal Policy for Paper Records – 2011*" and DF1/11/237031 "SIB *Electronic Document Retention and Disposal Policy – 2012*".

[2] See FI1/18/11611 "*[DRAFT] A Summary of the General Data Protection Regulation*". The NICS Intranet has a section on GDPR May 2018. The ICO has a Guide to the General Data Protection Regulation (GDPR) on its website. You can find the official PDF of the Regulation (EU) 2016/679 (General Data Protection Regulation) as a neatly arranged website at https://gdpr-info.eu/.

[3] See http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[4] See FI1/18/619917 "*Managing Subject Access Requests (SARs) and Other GDPR Requests - Procedures for SIB*".

All staff are entitled to a degree of privacy within the working environment. This also applies to their use of the information systems providing that they comply with all usage policies (e.g. email usage policy).

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).

HPERM helps SIB to carry out its obligations under Freedom of Information legislation. This will be co-ordinated by the Departmental Records Officer and the Information and Compliance 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 HPERM first **before** the redacted copy is created. The redacted copy can be related to the original record using the "Relate" function in HPERM.

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, unredacted record would be lost if it had simply been added as a new revision.

HPERM 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 Professional 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 HPERM records that are images using HPERM; otherwise the originating application has to be used. For example, Adobe Acrobat Professional has extensive annotation functions and Microsoft Word allows the addition of comments, etc.

[1] http://www.legislation.gov.uk/ukpga/2000/36/contents

Appendix 3 Archiving Old Paper Files

SIB's offsite records are managed by OASIS under the overall contract for the NICS. In general sending files to or retrieving files from offsite storage is dealt with by the Finance Team or the Information and Compliance Manager.

SIB's records and procedures relating to offsite storage can be found in the HPERM container, DF1-07-6542 "…*Records Management - Record Storage and Archiving*".

Appendix 4 SIB Record Types

Table 3 lists the HPERM record types available to SIB (there are others that are only available to be created by (e.g.) system administrators: e.g. DoF Personal Containers. Generally only "DoF Document" appears in the list by default.

Table 3: SIB Record Types

RECORD TYPE	MAIN USE
DoF Container	Containers below the classification that can be created by the SIB Information and Compliance Manager and that are used to store documents and records. End users cannot create containers.[1]
DoF 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.
DoF Paper File	To manage the existence of physical documents and records within SIB. (Note that creation of a DoF Paper File is only available to the SIB Information and Compliance Manager).
DoF Personal Document	To manage the storage of personal documents by staff. However, NICS policy has been to phase these out and they are not automatically available to new staff. These were restricted to a maximum of 30 documents and stored in a staff member's "DoF Personal Container". Documents cannot be moved freely between DoF Containers and DoF Personal Containers (this is an imposed limitation, not a technical limitation). Only the DoF Personal Document record type can be stored in a personal container; similarly a DoF Personal Document type should not be stored in regular DoF Containers.

[1] Other types may be visible to some staff if, say, another Department has given them access to its records.

Appendix 5 Data Protection

The SIB Data Protection Officer (DPO) has overall responsibility for data protection within SIB. The DPO is Sam Pringle, dataprotectionofficer@sibni.org. SIB's Privacy Notice is available on its website.

All SIB staff are responsible for compliance with the General Data Protection Regulation (GDPR), which came into law on the 25th May 2018.[1] The UK has implemented GDPR by way of the Data Protection Act 2018[2] (25-May-18, DPA 2018) that replaces the previous Data Protection Act 1998 and supplements the reforms to data protection laws that are contained in GDPR.

Where a data breach involves personal or sensitive personal data SIB should follow FI1/18/711216 "*SIB Personal Data Breach Management Plan*".

A general SIB guide can be found at FI1/18/11611 "*[DRAFT] A Summary of the General Data Protection Regulation*".

[1] See FI1/18/11611 "*[DRAFT] A Summary of the General Data Protection Regulation*". The NICS Intranet has a section on GDPR May 2018. The ICO has a Guide to the General Data Protection Regulation (GDPR) on its website. You can find the official PDF of the Regulation (EU) 2016/679 (General Data Protection Regulation) as a neatly arranged website at https://gdpr-info.eu/.

[2] See http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

Appendix 6 External References

A6.1 UK Legislation

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

Disposal of Documents Order (S.R & O 1925 No.167)[3]

General Data Protection Regulation (GDPR)

Data Protection Act 2018[4]

Freedom of Information Act 2000[5]

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

Environmental Information Regulations 2004[7]

The "*Lord Chancellor's Code of Practice on the Management of Records*"[8]

Civil Evidence Act 1995[9]

Civil Evidence (Northern Ireland) Order 1997 SI 1997/2983 (N.I.21)[10]

Copyright, Designs and Patents Act 1988[11]

Re-Use of Public Sector Information Regulations 2005[12]

[1] http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51

[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] http://www.proni.gov.uk/1925_disposal_of_documents_order.pdf

[4] See http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[5] http://www.legislation.gov.uk/ukpga/2000/36/contents

[6] http://www.legislation.gov.uk/uksi/1992/3240/contents/made

[7] http://www.legislation.gov.uk/uksi/2004/3391/contents/made

[8] http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf

[9] http://www.legislation.gov.uk/ukpga/1995/38/contents

[10] http://www.legislation.gov.uk/nisi/1997/2983/contents/made

[11] http://www.legislation.gov.uk/ukpga/1988/48/contents

[12] http://www.legislation.gov.uk/uksi/2005/1515/contents/made

A6.2 Relevant Standards Documents

- Northern Ireland Records Management Standard[1]
- British Standards Institution BIP 0008: 2004 *Code of Practice for Legal Admissibility and evidential weight of information stored electronically*. ISBN 0-580 42774-9[2]
- 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].
- 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.[3]
- 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.[4]

[1] http://www.proni.gov.uk/index/professional_information/records_and_information_management.htm

[2] http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030191165

[3] http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030055690

[4] www.cornwell.co.uk/edrm/moreq.asp.

- The National Archives[1] (formerly the Public Record Office) – Here you can find…
  i. A home page for Information and Records Management.[2]
  ii. Data Protection Act 1998: A guide for record managers and archivists.[3]
  iii. The National Archives Guidance and Standards[4]
- British Standards Institution BSI DISC PD0025 *Effective records management. Practical implementation of BS ISO 15489-1*.

[1] www.nationalarchives.gov.uk/ (see also the Public Record Office of Northern Ireland, www.proni.gov.uk/).

[2] www.nationalarchives.gov.uk/recordsmanagement/?source=ddmenu_services1

[3] www.nationalarchives.gov.uk/policy/dp/default.htm

[4] http://www.nationalarchives.gov.uk/information-management/guidance/a.htm

Appendix 7 Glossary of Terms

The following glossary is provided in order to clarify terms used in relation to HPERM or information management and that may have a meaning particular to SIB.

Table 4: Glossary of Terms

TERM	DESCRIPTION
Annotations and Redactions	The *HPE Records Manager* "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 HPERM; 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 HPERM 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 – 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.
Business Record	See *Record*.
Class	A class is a subdivision of the overall classification scheme by which the electronic *file plan* is organised. A class may be sub-divided 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 HPERM name for a folder – see "*Folder*" on page 41.
Declaration (Declared Final)	See "*Final*" on page 40.
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 39*).
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 HPERM 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] http://www.legislation.gov.uk/ukpga/1972/68/contents

TERM	DESCRIPTION
Folder (Container)	Folders (referred to as "containers" in HPERM) 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.
HPE Records Manager	HPERM (previously called HPRM and before that TRIM) is the EDRMS adopted by the Northern Ireland Civil Service. SIB is able to use HPERM as part of the services provided to it through the Department of Finance (DoF).
HPE Records Manager Reference (.tr5 file)	Use the "Make a HP Records Manager Reference" function in *HPE Records Manager* to allow the creation of pointers or shortcuts to records held in HPERM. 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 HPERM. The reference object, when double-clicked, will invoke HPERM 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 HPERM 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 HPERM Reference object will appear as a HPERM icon with the record title. The ".tr5" extension stands for "HPERM Reference". Double clicking a HPERM Reference will start a HPERM session. (See "*Pointer*" on page 43).
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.

[1] Note that in the NICS HPE Records Manager 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
Information Asset	Broadly a system or repository for information. Examples include a records management database like *HPE Records Manager*, databases of mapping data or the delivery tracking system used in the Asset Management Unit (AMU). SIB's Information Assets are recorded in DF1/12/465023 "*SIB Information Asset Register*".
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 (DoF), 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.
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.

[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.

TERM	DESCRIPTION
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. Staff can create a pointer in *HPE Records Manager* with the "Make Reference" function – see *HPE Records Manager Reference (.tr5 file)* on page 41.
PRO	The Public Record Office[1] (now called *The National Archives*).
PRONI	The Public Record Office of Northern Ireland[2].
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.
Record	A *document* which provides evidence of a business transaction or decision, or contains information needed to carry on SIB's business. A 'Record' can either be created by or received into SIB. A record may have been created to comply with a legal requirement. SIB records may be required to be produced as evidence in legal proceedings, to satisfy public accountability or Assembly scrutiny, or in response to a Freedom of Information request. 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.[3] See Section 7 on page 8 for guidance on what to save as "business records".
Record Type	All electronic *documents* and *records* must be of a specific record type within HPERM 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 HPERM is "DoF Document".
Redact	See "*Extract/Redaction*" on page 39 (See also *Annotations and Redactions on page 39*).
Relate	The *HPE Records Manager* "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.

[1] www.nationalarchives.gov.uk/

[2] www.proni.gov.uk/

[3] In practice, the NICS systems administrators may have to carry out some tasks.

TERM	DESCRIPTION
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	*HPE Records Manager* 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 *HPE Records Manager*, images are stored in TIFF format if they are to be *annotated or redacted*.
TNA	The National Archives[1] (formerly the *Public Record Office*). Note that Northern Ireland has its own public records office, the Public Record Office of Northern Ireland.
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.

[1] www.nationalarchives.gov.uk/