



The Northern Ireland Office

**Information Management
Policy**

Version 2.8.1 February 2007

Information Management Policy

Version Information

Status

The current status of this document is: *Draft*

Version History

Number of this Version: 2.8.1

Date of this Version:

This Copy Printed on: 18 December 2008

Owner

The person responsible for this document is the Departmental Records Officer, who is part of the Information Management Centre (Annex A, Dundonald House).

Document Location

The electronic version of this file is located as Record No: 1057079.

Table of Contents

Version Information	2
Status.....	2
Version History	2
Document Location	2
Distribution of this Version.....	Error! Bookmark not defined.
<i>Name</i>	<i>Error! Bookmark not defined.</i>
<i>Role</i>	<i>Error! Bookmark not defined.</i>
<i>Responsibility</i>	<i>Error! Bookmark not defined.</i>
Management Summary	5
Purpose	6
Introduction	6
Scope	7
Definitions	8
Document	8
Record.....	8
Electronic and Non-electronic Documents/Records	8
Eight Information Management Principles.....	9
Information Management Guidelines.....	10
Roles & Responsibilities	10
End Users	10
Local Information Managers (LIMs).....	10
NIONet Editors	11
Record Managers.....	11
Reviewers.....	11
System Administrators.....	11
EDRMS Functionality	11
Intranet Content Management System Functionality	11
Related Documents	12
Policy Review	12
Appendix A: Glossary of Terms.....	13
Appendix B: Information Management Guidelines	18
Creation and Capture/Receipt of Information.....	18
<i>Responsibility to Create Records</i>	<i>18</i>
<i>Record Types in the Department</i>	<i>19</i>
<i>Context and Metadata.....</i>	<i>19</i>
<i>Intellectual Property of Others (Copyright).....</i>	<i>19</i>

Storage and Retrieval of Information	19
<i>Security</i>	20
Dissemination of Information	20
Retention & Disposal of Information	20
<i>Emails</i>	21
<i>Archiving</i>	21
Compliance with Statutory and Regulatory Requirements.....	21
<i>Data Protection Act 1998</i>	22
<i>Freedom of Information Act 2000</i>	22
APPENDIX C: EDRMS – TRIM Context Permissions by User Role	23
Appendix D: Intranet Content Management System (Obtree) Access Levels and Roles	26
Obtree Access Levels.....	26
Obtree Roles	26
Appendix E – Departmental Record Types	27
Appendix F – Data Protection.....	28
The Eight Data Protection Principles	28
Appendix G – External References	29
UK Legislation	29
Relevant Standards Documents.....	29

Management Summary

Where ‘Department’ is used in this document it refers to ‘NIO, its agencies and dependent bodies’.

This document defines a high-level Information Management Policy for the Department. It outlines its scope and provides [eight information management principles](#) to ensure that staff:

Treat Departmental information as a Corporate Resource;

Make the information they create or capture accessible to those within the Department who need it to fulfil their duties;

Manage all information in a consistent manner across the Department;

Record details of key business activities undertaken on behalf of the Department;

Ensure that Departmental information is accurate and fit for purpose;

Retain or dispose of information in accordance with legislative requirements or departmental procedure;

Take personal responsibility for the effective management of Departmental information; and

Comply with all Statutory and Regulatory requirements.

This document also describes the roles and responsibilities of the different types of users of OASIS3 particularly in relation to the Electronic Document and Records Management System (EDRMS) and Intranet (NIONet). More detailed guidelines for information management within the Department are provided in the [Information Management Procedures](#) on NIONet.¹ The key responsibilities of the main roles can be summarised as follows:

ROLE	RESPONSIBLE FOR:
End User	Creation, capture, storage, dissemination and retrieval of information
EDRM LIM (Electronic Document and Records Management Local Information Manager)	Delegated records management functions at Business Unit ² level to facilitate local adherence to this and subsidiary policies. Most EDRM LIMs are also Intranet LIMs.
Intranet LIM	Delegated Intranet content management functions at business unit level. Most Intranet LIMs are also EDRM LIMs.
Record Manager	Providing records management for the Department including responsibility for the Corporate File Plan. Also co-ordinating high level searches for Data Protection and Freedom of Information requests.

¹ [564687 “Information Management Procedures”](#)

² For the purposes of this document a “Business Unit” is defined as “the lowest organisational unit level within the Department with a unique, and self contained, strategic objective e.g. normally branch or division”.

ROLE	RESPONSIBLE FOR:
NIONet Editor	NIONet editors are members of the Central Intranet Team and are responsible for making content “live” (active) and maintaining the integrity of the Intranet. They are the <u>NIONet Editor</u> .
Reviewer	Review and decide if appropriate disposal of Department records should be actioned (record managers would undertake the actual destruction). Allocation of retention/disposal schedules and conducting security and sensitivity review of Departmental records before public release.
Systems Administrator	Systems configuration and management.
Departmental Record Officer (DRO)	Departmental responsibilities derived from the Public Record Acts, including annual release of records to public record offices. Strategic oversight of records and information management policy. Provision of advice on Departmental compliance with legislative requirements such as Freedom of Information and Data Protection.

Finally this document lists related documents which are subsidiary to this Policy and which facilitate effective information management using OASIS3.

Purpose

This document provides an information management policy for the effective and efficient management of the Department’s [documents](#) and [records](#) (i.e. recorded information).

Introduction

The Department’s work depends totally on information and so information is one of the Department’s most important assets.¹ Although much of this information is irreplaceable if destroyed, it is often managed inconsistently and ineffectively.

¹ The Flax Programme upgraded OASIS within the Northern Ireland Office, The Northern Ireland Prison Service, Forensic Science Northern Ireland, The Youth Justice Agency and The Compensation Agency.

In addition, OASIS3 is provided to a small number of additional users located within other organisations including but not limited to: The Civil Service Commissioners for Northern Ireland, The Sentence Review Commission, Life Sentence Review Commissioners, the Board of Visitors at Maghaberry and Magilligan, the Visiting Committee at Hydebank Wood, The Northern Ireland Departments, The Home Office, The Ministry of Defence, The Criminal Injuries Compensation Appeals Panel for Northern Ireland, the Prisoner Ombudsman’s Office and the Police Service of Northern Ireland.

For the purposes of this document, where reference is made to the Department or its staff, such references should be taken to refer to the staff who use OASIS3 in all the above organisations, with the exception of The Northern Ireland Prison Service (Note: This is because NIPS has its own EDRMS dataset and records management team).

Effective management of information is essential to improve the efficiency and effectiveness of the Department. The right people must have access to the right information when they need it and the functionality of OASIS3 incorporating the Electronic Document and Records Management System (EDRMS) and intranet helps to achieve this. However, the full benefits of OASIS3 can only be realised if staff comply with this strategic information management policy and the more detailed working procedures.

To do this, the Department needs to:

- a. Find information about a particular activity or transaction as quickly as possible;
- b. Identify quickly those people within the Department who can help with a particular issue;
- c. Find and re-use information, methods and practices which have been successful.

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

Scope

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

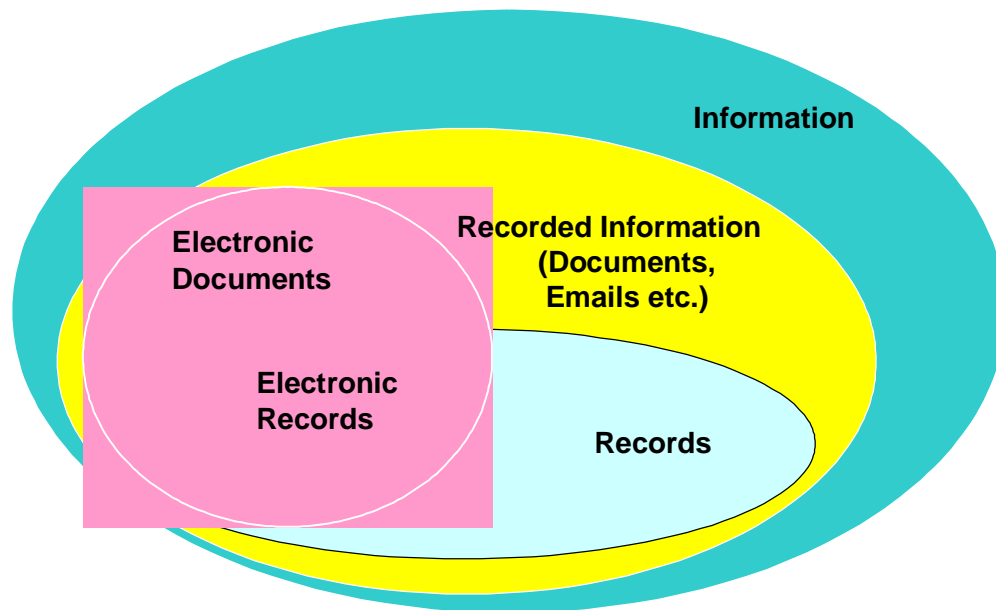


Figure 1: Information boundaries within the Department

This Policy covers all recorded information.

Whatever the medium: e.g. electronic or paper.

Whether it originates from within the Department 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](#).¹

¹ Therefore use of the word information in this Policy relates to the term “recorded information”.

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](#). However, such computer applications and databases themselves are outside the scope of the intrinsic functionality of OASIS3. The Policy provides a framework for developing specific procedures and guidance. All other information management products in the Department derive from this Policy.

Definitions

Certain words in this Policy have specific meanings and these are explained in the [Glossary](#) at [Appendix A](#). However, two terms are fundamental to this Policy and are defined as follows.

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.

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 Departmental business.”

A '[record](#)' can either be created in the Department or externally. It may be created to fulfil a legal requirement and may be required as legal evidence or to satisfy public accountability or 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 Department activity.

Electronic and Non-electronic Documents/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 Department's information should be stored within the EDRMS. Clearly, retrospective management of some paper documents using the EDRMS will only be completed as required. All new documents will be managed using the EDRMS and normally these will be stored electronically. If that is not appropriate, they will still be managed using the EDRMS. Information, including documents that should be widely accessible to all staff throughout the Department, should be published via the intranet – NIONet.

Eight Information Management Principles

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

The primary one is:

Principle 1. Information is a Corporate Resource. All Information (including e-mail) belongs to the Department and not to any individual or group.

Therefore, information needs to be:

Available:

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

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

Appropriate:

Principle 4. Staff will record details of appropriate Business Activities.

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

Principle 6. Staff will retain or dispose of information appropriately.¹

Accountable:

Principle 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.

Principle 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.

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

¹ Information that is of ongoing business value must be retained or sent to the Records Management & Review Team (RMRT) for historical archive; and redundant information must be destroyed inline with the Departmental Disposal Schedules

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 B](#). These underpin the [eight information management principles](#) and are structured under the following headings:

Creation and Capture/Receipt of Information

Storage and Retrieval of Information

Dissemination of Information

Retention and Disposal of Information

Compliance with Statutory and Regulatory Requirements

Roles & Responsibilities

The following roles are needed to manage information using OASIS3:

End User

Local Information Manager

NIONet Editor

Record Manager

Reviewer

Systems Administrator

The responsibilities for each of these roles are described below.

End Users

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 the department.

Local Information Managers (LIMs)

Local information managers have delegated authority to manage information within their areas to ensure consistency. This involves specific records management functions. They are also responsible for ensuring that staff within their areas are aware of and adhere to this and other subsidiary policies. LIMs receive their delegated authority through record managers and will receive appropriate training. Most LIMs have responsibility for publishing the content approved by their business area on the intranet (although some LIMs are responsible only for Intranet content).

NIONet Editors

NIONet editors are members of the Central Intranet Team and are responsible for making content “live” (active) and maintaining the integrity of the Intranet.¹

Record Managers

Record managers are responsible for the top levels of the [corporate file structure](#). They also provide and update disposal schedules for all types of information and archive and dispose of Departmental information in accordance with these schedules. Senior record managers may authorise systems administrators to carry out certain functions on their behalf. The NIO has a “[Code of Conduct for Record Managers – May 05](#)” (541162) with which all records managers must comply.

Record managers responsible for Freedom of Information or Data Protection may undertake necessary searches needed to fulfil their statutory duties. They may not necessarily have access to the contents of the records and documents they identify.

Record managers receive their delegated authority through the Departmental Records Officer (DRO).

Reviewers

Reviewers are responsible for reviewing records and recommending an appropriate means of disposal, in accordance with disposal schedules. They also advise what needs to be withheld from release for security and sensitivity reasons via appropriate consultation.

Reviewers receive their delegated authority through the DRO.

System Administrators

System administrators are responsible for the creation of new user roles on the EDRMS, system configuration, and system management including, if necessary, disaster recovery. System administrators will also be responsible for carrying out various systems functionality tasks. These will include conducting statistical analysis and producing audit reports either as part of the management of the technical infrastructure or at the request of senior record managers or security officials.

EDRMS Functionality

The main functionality and permissions associated with each of these roles in relation to the EDRMS is shown at [Appendix C](#). This is not intended to be definitive or complete and will evolve as the EDRMS develops to meet the Departments needs.

Intranet Content Management System Functionality

The main access levels and roles associated with LIMs and the NIONet Editors in relation to the Intranet Content Management System (Obtree) are described at [Appendix D](#).

¹ Responsibility for making items live in certain sections of NIONet may be delegated to appropriate persons. For example, Press Office publishes and makes live the press cuttings, and OSB publishes news items and job vacancies.

Related Documents

The key related NIO documents to this Policy are as follows:

DOCUMENT TITLE	TRIM REFERENCE
“Updated NIO Document Scanning Policy V2_6”	550149 “Updated NIO Document Scanning Policy V2_6”
NIO Disposal Schedules	<p>Generic disposal schedules for paper records “Generic disposal schedules for paper records” are stored in container 470-05.</p> <p>The disposal schedules for electronic documents and records are embedded within the EDRMS.</p>

A list of external references is provided at [Appendix G](#).

Policy Review

The DRO 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.



Appendix A: Glossary of Terms

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

TERM	DESCRIPTION
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, along with the folders that are classified against the scheme, make up the file plan .
Container	The TRIM name for a folder – see “ Folder ”.
Declaration (Declared 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 .
Destruction	The process of eliminating records beyond any possible reconstruction.
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).

¹ <http://www.opsi.gov.uk/acts/acts1972/19720068.htm>

TERM	DESCRIPTION
Export	The process of passing copies of a <i>record</i> or group of records with their <i>metadata</i> from one system to another system, either within the organisation or elsewhere. Export (rather than <i>transfer</i>) does not necessarily mean removing them from the first system.
Extract/Redaction	This is a copy of a <i>record</i> , from which some material has been removed or permanently masked. An <i>extract</i> 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 <i>extract</i> of a whole record is made by removing the parts that can be released from the whole. <i>Redaction</i> is the opposite of extraction in that a copy of the whole record/folder is released with the excluded parts redacted or removed.
File Plan	The full set of <i>classes</i> , and the <i>folders</i> 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.
Folder (Container)	<p>Folders (referred to as “containers” in TRIM) are created only at the lowest level class in any single part of the <i>classification scheme</i>. They can usually be one of four types; i) a folder that is a container for other folders; ii) a folder that only contains electronic documents; iii) a physical folder that only contains physical paper documents; or iv) a folder that contains both electronic documents and references to physical paper documents, commonly known as a hybrid folder.</p> <p>An electronic folder is a (virtual) container for records (which may be segmented by <i>part</i>). Folders are allocated to a class. A folder is the primary unit of management, and is constituted of <i>metadata</i>. 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. <i>electronic folder</i>, <i>physical folder</i> to refer to that specific type of folder.</p>
Hybrid Folder	A set of related electronic and non-electronic <i>records</i> , some stored in an electronic <i>folder</i> within the system and some in a non-electronic <i>folder</i> (typically, a <i>physical folder</i>) outside the system. A hybrid folder may have several <i>hybrid parts</i> . Both electronic and non-electronic elements of the hybrid folder must be managed as one.

TERM	DESCRIPTION
Information	Knowledge of some fact, opinion, advice, instruction or occurrence, which is communicated and relates directly or indirectly to the functions of the Department. 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 <i>Inheritance on creation</i> where the subordinate (or ‘child’) object takes the value of that attribute when it is created; or by <i>Retrospective inheritance</i> 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).
ISD	Information Systems Division of the NIO.
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 ¹ file.
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.

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
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) .
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	<p>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 the Department. A record may have been created to comply with a legal requirement and the Department’s records may be required to be produced as evidence in legal proceedings or to satisfy public accountability or parliamentary scrutiny.</p> <p>[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 departmental policy and procedure by an officer authorised to carry out such actions.]</p>
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”. A list of the current record types can be found at Appendix E .
Redact	See “ Extract/Redaction ”.

¹ <http://www.nationalarchives.gov.uk/>

² <http://www.proni.gov.uk/>

TERM	DESCRIPTION
Review	<p>The examination of the disposal status of a <i>folder</i>, or a <i>part</i> 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).</p> <p>[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].</p>
TNA	<p>The National Archives¹ (formerly the Public Record Office).</p>
Transfer	<p>The process of <i>exporting</i> complete electronic <i>folders</i> (usually in groups) and subsequently destroying them within the exporting system, effectively transferring custody of the <i>records</i>. 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.</p>
TRIM Reference (.tr5 file)	<p>Use the “Make a TRIM Reference” function in TRIM to allow the creation of pointers or shortcuts to records held in TRIM Context. 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 Context.</p> <p>The reference object, when double-clicked, will invoke TRIM Context and display the selected records. You can transport the reference object by any means you choose (for example, including it in an e-mail message, etc). Mailing a TRIM Context 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.</p> <p>The TRIM Context object will appear as a TRIM Context icon with the record title. The “.tr5” extension stands for TRIM Reference.</p> <p>Double clicking a TRIM Reference will start a TRIM Context session; however it will use a current session if it is running. If you do have a session of TRIM Context running, simply drag and drop the reference onto it. This action will automatically display the selected records. (See “Pointer”).</p>



¹ <http://www.nationalarchives.gov.uk/>

Appendix B: Information Management Guidelines

This Appendix describes more specific guidelines governing the management of information within the Department. These underpin the [eight information management principles](#) stated in the main document. The Appendix is structured under the following headings:

Creation and Capture/Receipt of Information

Storage and Retrieval of Information

Dissemination of Information

Retention & Disposal of Information

Compliance with Statutory and Regulatory Requirements

Creation and Capture/Receipt of Information

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 the Department 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. The originator of a record has a duty to ensure that the record is titled and stored appropriately in the file plan. The one exception to this is Private Office responses to Divisional submissions which Divisions will be responsible for filing. This is outlined in the PPS to S of S note of 9 October 2006 which states

¹ <http://www.dca.gov.uk/foi/codemanrec.htm>

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

“All e-mails and attachments sent by a Private Secretary to an official on behalf of a Minister or the Secretary of State relating to a decision, request or comment made by a Minister or the Secretary of State, or a note of a Ministerial Meeting, must be filed appropriately by the main recipient. The Private Offices do not keep official records of such e-mails or attachments”.

Record Types in the Department

All information stored within the EDRMS must be assigned to a “*Record Type*”. The default record type for information created in most MS Office applications is “Document”. The DRO will maintain the list of “Record Types” and associated templates – see [Appendix E](#).

Context and Metadata¹

Appropriate *metadata* will be applied to all *documents* and *records* created, captured and kept by the Department. (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 unless its format or other considerations e.g. security classification, prevent this.

Intellectual Property of Others (Copyright)

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

Staff responsible for scanning documents² received from outside the Department will comply with departmental scanning policy and procedures drawn up to be compliant with British Standard PD0008 (BIP 0008).³

Storage and Retrieval of Information

Staff have a responsibility to make their information accessible to as wide an audience 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.

Staff should consider the wider business goals of the Department 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 Business Unit. Some examples of the implications of this on the way staff should work are as follows:

¹ A definition of *metadata* is provided in “Appendix A: Glossary of Terms”.

² Further guidance on scanning is provided in the “[NIO Document Scanning Policy](#)”.

³ PD0008 is now called BIP 0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. British Standards Institute – see <http://www.bsi-global.com/ICT/IM/bip0008.xalter> (on-line purchase link). RMRT in Millbank retain a hard-copy of PD0008.

Staff should consider the retrieval needs of others within the Department when storing information. For example, this means using a meaningful document title and adding relevant keywords to enable others within the Department 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 the Department who would have an interest in it.

Staff should structure information in a way that reflects the way the Department works. For example, setting up folder structures that relate to the functions of the Department rather than a narrow "silo" view based on organisational structure.

When staff retrieve a document from one of the Department's repositories 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.

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. Protective markings should be assigned to all documents and records in line with guidance issued by the Departmental Security Officer. As OASIS3 is a Confidential HIGH system, electronic documents and records stored within it should not exceed Confidential. Staff requiring advice about storing information above this protective marking should consult with the Protective Security Division.

Dissemination of Information

Staff who receive information not relevant to their own business function will pass it to someone within the Department 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. Staff should consider whether it is appropriate to make information available by publishing it via the NIO Intranet.

Retention & Disposal of Information

Information is captured stored and maintained because it has a value to the Department and to the Government and public at large. 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 the Department is not under a legal obligation to retain it unless the material is of historical significance. It is routine for records managers to remove duplicate information on behalf of LIMs or the metadata of documents that staff have deleted.

¹ A definition of a [pointer](#) is provided in "Appendix A: Glossary of Terms".

The retention requirements for many forms of information can be determined at the point of creation or capture. As such, Records Management and Review Team (RMRT) is required to develop and maintain retention schedules covering all functional areas of the Department. 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 DRO and record managers will assist with their development and maintenance.

Where there is an applicable Generic Disposal Schedule from The National Archives (TNA), this should be used as the basis for the Modification 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.

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 Department’s EDRMS must 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.

The Department 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 files. Relevant emails should be stored in the EDRMS.

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 [TNA](#), it must be in TNA-approved formats and on TNA-approved media.

Compliance with Statutory and Regulatory Requirements

Compliance with legal requirements will protect the Department 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 the Department from criticism.

Compliance with legislation may operate at several levels within the Department. For example, there will be legislation that applies to the Department as a whole, such as the Data Protection Act, and all staff needs to be aware of their information management responsibilities under such legislation. There are also legal requirements that relate to just one aspect of the Department's operations. For example, business units responsible for letting contracts need to comply with EC procurement legislation and the information management requirements that this imposes (e.g. retention of contract documents for 4 years from contract award date).

There is also an obligation on the Department to identify relevant legislation and to inform staff members accordingly. Staff can only be expected to apply legislation and regulations of which they are aware and consequently training and communication exercises will be necessary.

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 F](#)). The EDRMS will make it easier to apply these principles and enable the Department to fulfil its duties effectively under the Data Protection Act. The DRO will provide advice about Data Protection and procedures for handling subject access requests under the Data Protection Act.

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. e-mail usage policy. To facilitate this, staff are 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 Code of Conduct for Records Managers. When a member of staff leaves the Department, this personal container and all its contents are destroyed in accordance with this Code of Conduct.

Freedom of Information Act 2000²

In the interests of public accountability departmental documents will be placed in the public domain unless there is a reason for not doing so.

The EDRMS will help the Department to carry out its obligations under FOI. This will be coordinated by the Records Management and Review Team, but all business units will be responsible for ensuring compliance. They will devote enough resources to this, including staff, for the Department to fulfil its obligations.



¹ <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>.

² <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm>.

APPENDIX C: EDRMS – TRIM Context Permissions by User Role

This list will evolve as the use of the EDRMS is developed to meet specific Departmental needs.

TRIM PERMISSION	END USER	LOCAL INFORMATION MANAGER	RECORD MANAGER	REVIEWER	SYSTEM ADMINISTRATOR
RECORD UPDATE PERMISSIONS					
- Create records	✓	✓	✓	✓	✓
- Modify records	✓	✓	✓	✓	✓
- Delete records			✓		✓
- Reverse final declaration			✓		
- Create new parts		✓	✓		
- Modify record class			✓		
- Manage requests		✓	✓		
- Record administration			✓		✓
- Record administration (restricted)					
- Record archivist			✓	✓	
- Document update	✓	✓	✓	✓	✓
- Document delete/purge	✓	✓	✓	✓	✓
- Append to existing notes	✓	✓	✓	✓	✓
- Can save record searches	✓	✓	✓	✓	✓
- Add records relationships	✓	✓	✓	✓	✓
- Remove records relationships	✓	✓	✓	✓	✓
- Attach contacts	✓	✓	✓	✓	✓
- Remove contacts	✓	✓	✓	✓	✓
- Set container	✓	✓	✓	✓	✓
- Change container	✓	✓	✓	✓	✓
- Remove from container					
- Modify record security		✓	✓		
- Set record archiving dates		✓	✓	✓	
- Document Assembly Administration					
LOCATION UPDATE PERMISSIONS					
- Can create internal locations			✓		✓

TRIM PERMISSION	END USER	LOCAL INFORMATION MANAGER	RECORD MANAGER	REVIEWER	SYSTEM ADMINISTRATOR
- Can modify internal locations			✓		✓
- Can delete internal locations			✓		
- Can create external locations		✓	✓		✓
- Can modify external locations		✓	✓		✓
- Can delete external locations			✓		
- View user profile details			✓		✓
- Modify logins and user profiles			✓		✓
CONTROL FILE UPDATE PERMISSIONS					
- Record types			✓		
- Lookup sets			✓		
- User defined fields			✓		
- Classifications			✓		
- Schedules			✓		
- Holds			✓		
- Spaces			✓		
- Document stores					✓
- Indexed words			✓		✓
- Postal codes			✓		✓
- Thesaurus terms			✓		
- Saved searches		✓	✓	✓	✓
- Meetings					
WORKFLOW/ACTION TRACKING					
- Workflow administration			✓		✓
- Actions administration			✓		✓
- Attach actions or activities	✓	✓	✓	✓	✓
- Reassign actions or activities		✓	✓		✓
- Reschedule actions		✓	✓		✓
- Complete actions or activities	✓	✓	✓	✓	✓
- Create workflow	✓	✓	✓	✓	✓
- Create workflow without using template			✓		
- Modify workflow			✓		

TRIM PERMISSION	END USER	LOCAL INFORMATIO N MANAGER	RECORD MANAGER	REVIEWER	SYSTEM ADMINISTRAT OR
MISCELLANEOUS					
- Reporter administration			✓		✓
- Run statistics	✓	✓	✓	✓	✓
- Edit business calendar			✓		✓
- Change system settings			✓		
- Use caption editor			✓		
- Security and audit administrator			✓		
- Define barcode scanners			✓		✓
- Define web templates			✓		✓
- Bypass view access controls			✓		
- Bypass all access controls			✓		✓
- Import and export					✓
- Bypass lockdown					
LOCATION USAGE PERMISSIONS					
- Can be record home	✓	✓	✓	✓	✓
- Can be record owner	✓	✓	✓	✓	✓
- Can be record assignee	✓	✓	✓	✓	✓
- Can be record contact	✓	✓	✓	✓	✓
- Can be record requestor	✓	✓	✓	✓	✓
- Can be action/activity assignee	✓	✓	✓	✓	✓
- Can be activity supervisor	✓	✓	✓	✓	✓
- Can be assigned to an access control	✓	✓	✓	✓	✓



Appendix D: Intranet Content Management System (Obtree) Access Levels and Roles

This Appendix describes how access to the Obtree Content Management System for Intranet LIMs is managed by way of **access levels** and assigned **roles**.¹

Obtree Access Levels

Two levels of access are used (although Obtree supports more), **supervisor** and **author**.

Supervisors can edit live content (“Active”) and make content live.

Authors can create and edit content but only in draft (“At Work”) mode. Once content is live authors can only work on a new version/copy and they have to ask the Central Intranet Team to make content live.

Most Intranet LIMs only have author access. A few have supervisor access to certain areas (e.g. Office Services LIMs have supervisor access to News, Updates and Bulletins so they can make news items live immediately).

Access levels are set in Obtree by changing the settings for a role (e.g. to change access level for a page from author to supervisor).

Obtree Roles

“**Roles**” are used to determine which areas of the Intranet LIMs can edit.

The Central Intranet Team can edit any part of NIONet.

LIMs are assigned to roles which correspond to their Agency/Division. Thus PRSD LIMs can only edit PRSD pages.

Certain roles have wider access, e.g. Personnel Services LIMs can edit personnel pages under the Personnel Home Page and pages under Personnel Help.

Roles can overlap, e.g. OSB LIMs and ISD LIMs can both edit news-like items on the NIONet Home Page.

Membership of an Obtree role is assigned through Active Directory. To make a LIM a member of a role, OASIS Service Desk add the role name to the LIMs AD profile. They do this at the request of the Central Intranet Team. The use of AD means that LIM access to Obtree is managed by the OASIS single log-on.



¹ More information can be found in the restricted TRIM Folder [4021~05](#) “[Obtree Administrator](#)”.

Appendix E – Departmental Record Types¹

Record Type	Main Use
Access to Information Request	To manage Data Protection, Freedom of Information and EIR requests etc. received by the Department
Archive Box	To manage the archiving of physical files from the Department into secondary storage facilities
Document	To manage the creation and storage of electronic “recorded information”. This is the default record type for electronic information created in “standard” MS Office applications
Folder Level 1	To provide a first level container below the classification in which to store folder levels 2 and 3 containers or documents
Folder Level 2	To provide a second level container in which to store folder level 3 containers or documents
Folder Level 3	To provide a third level container in which to store documents
Government Enquiry	To manage the process of responding to and monitoring government enquiries received by the Department
Minister’s Case	To manage the process of responding to and monitoring Minister’s Cases.
Parliamentary Question	To manage the process of responding to and monitoring parliamentary questions received by the Department
Personal Storage Container	Unique to each member of staff and used to store personal documents, for temporary storage, and to store ephemeral documents and notes.
Personnel File	To manage staff personnel information throughout their careers within the Department
Physical File	To manage the existence of physical documents and records within the Department
Physical Object	To manage the existence of physical objects as records within the Department
Scanned Image	To manage the creation of scanned images as records within the Department



¹ N.B. Records Management and Review Team has the capability to add record types as required via the EDRMS.

Appendix F – Data Protection

The eight data protection principles are defined in the [Data Protection Act 1998](#).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 <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>.

Appendix G – External References

UK Legislation

[Public Records Act 1958](#)¹

[Data Protection Act 1998](#)² (See also BIP 0012³)

[Freedom of Information Act 2000](#)⁴

[Environmental Information Regulations 1992](#)⁵ (as amended 1998)

Freedom Of Information, Environmental Protection, The [Environmental Information Regulations 2004](#)⁶

[Information Commissioner's Codes of Practice on Data Protection](#)⁷

- [CCTV](#)
- [The Employment Practices Code](#)
- [The Employment Practices Code: Supplementary Guidance](#)
- [Quick Guide to the Employment Practices Code: Ideal for Small Businesses](#)
- [Code of Practice on Telecommunications Directory Information and Fair Processing](#)

[Lord Chancellor's Code of Practice on the Management of Records Issued under section 46 of the Freedom of Information Act 2000](#)⁸

Relevant Standards Documents

- British Standards Institution BSI DISC PD0008: 1999 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.⁹
- International Standards Organisation ISO 17799 / BS7799 Information Security Management.¹⁰

¹ <http://www.nationalarchives.gov.uk/policy/act/act.htm>

² <http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm>

³ BSI Data Protection Guide BIP 0012 (formerly PD0012 – <http://www.bsi-global.com/ICT/Legal/bip0012.xalter> (on-line purchase link). RMRT in Millbank retain a hard-copy of PD0012.

⁴ <http://www.opsi.gov.uk/ACTS/acts2000/20000036.htm>

⁵ http://www.opsi.gov.uk/si/si1992/Uksi_19923240_en_1.htm

⁶ <http://www.opsi.gov.uk/si/si2004/20043391.htm>

⁷ <http://www.ico.gov.uk/eventual.aspx?id=437>

⁸ <http://www.dca.gov.uk/foi/codemanrec.htm>

⁹ PD0008 is now called BIP 0008 – Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically. British Standards Institute – see <http://www.bsi-global.com/ICT/IM/bip0008.xalter> (on-line purchase link). RMRT in Millbank retain a hard-copy of PD0008.

¹⁰ <http://www.standardsdirect.org/iso17799.htm> (on-line purchase link). RMRT in Millbank retain a hard-copy of ISO 17799 / BS7799.

- International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001.¹
- International Standards Organisation ISO 23950 Information and Documentation: Information retrieval (Z39.50): application service definition and protocol specification.²
- International Standards Organisation ISO 2788 Documentation: Guidelines for the establishment and development of monolingual thesauri.³
- International Standards Organisation ISO 5964 Documentation: Guidelines for the establishment and development of multilingual thesauri.⁴
- [MoREQ: Model requirements for Recordkeeping](#).⁵
- [The National Archives](#)⁶ (formerly the Public Record Office) – Here you can find...
 - A home page for [Records Management](#).⁷
 - [Requirements for Electronic Records Management Systems – 2002 revised requirements](#).⁸ (“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”).
 - [Data Protection Act 1998: A guide for record managers and archivists](#).⁹
 - [Guidelines for management, appraisal and preservation of electronic records](#).¹⁰ (“These two guidance documents were produced under the auspices of the Electronic Records from Office Systems (EROS) programme of The National Archives”).
 - [Manual of guidance on access to public records](#).¹¹ (link to download PDF).
- [Office of the e-Envoy](#).¹² (Note: “This information is being maintained for archive/historical purposes and will not be updated”).

¹ <http://www.bsi-global.com/ICT/Legal/bsiso15489-1.xalter> (on-line purchase link). RMRT in Millbank retain a hard-copy of ISO 15489 parts 1 and 2.

² <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=27446&scopelist=> (on-line purchase link).

³ <http://www.collectionscanada.ca/iso/tc46sc9/standard/2788e.htm> (extracts and a purchase link).

⁴ <http://www.collectionscanada.ca/iso/tc46sc9/standard/5964e.htm> (extracts and a purchase link).

⁵ <http://www.cornwell.co.uk/moreq>

⁶ <http://www.nationalarchives.gov.uk/>

⁷ http://www.nationalarchives.gov.uk/recordsmanagement/?source=ddmenu_services1

⁸ <http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/>

⁹ <http://www.nationalarchives.gov.uk/policy/dp/default.htm>

¹⁰ <http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>

¹¹ <http://www.nationalarchives.gov.uk/recordsmanagement/advice/>

¹² <http://archive.cabinetoffice.gov.uk/e-envoy/index-content.htm>

- [e-Government Interoperability Framework Version 6.1](#) (18/3/2005).¹
- [e-Government Metadata Framework](#) (1/5/2001).²
- [e-Government Metadata Standard Version 3.0](#) (29/4/2004).³
- [e-government category lists](#) [GCL], version 1.1, UK Office of the e-Envoy, May 2002.⁴
- e-government [Framework Policies](#).⁵ (Note: “This information is being maintained for archive/historical purposes and will not be updated”).
- e-government: a Strategic Framework for public services in the information age: Guidelines: [Security Framework v4](#), 2002.⁶ (Note: “This information is being maintained for archive/historical purposes and will not be updated”).
- British Standards Institution BSI DISC PD0025 Effective records management. Practical implementation of BS ISO 15489-1.⁷



¹ http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=949

² http://www.govtalk.gov.uk/schemasstandards/metadata_document.asp?docnum=860

³ http://www.govtalk.gov.uk/schemasstandards/metadata_document.asp?docnum=872

⁴ <http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/pdf/referencefinal.pdf>

⁵ [http://www.e-envoy.gov.uk/frameworks-top/\\$file/frameworksindex.htm](http://www.e-envoy.gov.uk/frameworks-top/$file/frameworksindex.htm)

⁶ [http://www.e-envoy.gov.uk/frameworks-security/\\$file/security.htm](http://www.e-envoy.gov.uk/frameworks-security/$file/security.htm)

⁷ <http://www.bsi-global.com/ICT/KM/bip0025-2.xalter> (on-line purchase link). PD0025 is now called “BIP 0025”. RMRT in Millbank retain a hard-copy of PD0025 parts 1 and 2.