

---

## **Management, appraisal and preservation of electronic records**

Vol 2: Procedures

---

**Management, appraisal and preservation of electronic records**

© Public Record Office

2nd edition 1999

Public Record Office  
Kew, Richmond, Surrey  
*<http://www.pro.gov.uk/recordsmanagement>*

## About the Public Record Office

As the national archives for England, Wales and the United Kingdom, the Public Record Office acts as the nation's memory. It manages the public records system of the United Kingdom under the Public Records Acts of 1958 and 1967 and undertakes four core activities:

- supervising the selection, safekeeping and transfer of public records created by government departments, courts, tribunals and non-governmental public bodies
- keeping the records selected for preservation in the Public Record Office or assigning other suitable places of deposit for them
- providing access to the records and encouraging and promoting their use
- advising government and others on public record issues and related policy matters.

The records held by the Public Record Office (PRO) span one thousand years and fill 167 kilometres of shelving. The PRO also oversees public records held by other bodies such as county record offices. All these records contain information essential for good governance. They provide a sound basis for historical and genealogical research. They help to make government accountable over time. They can be used as legal evidence, and they extend knowledge of past actions and decisions to inform future decision-making. In carrying out its duties, the Public Record Office serves the needs of present and future generations.

The Public Record Office vision for the beginning of the twenty-first century is that readers will be able to access many public records electronically. To meet this aim, the PRO has set the following strategic aim:

*To increase the accessibility of the public records by electronic means, in the Office and around the world.*

One of the key objectives that will help to realise this strategic priority is:

- to decide how best to select, preserve, store and give access to electronic records created by government.

Other longer term priorities are :

- to enhance the quality and efficiency of our public services
- to promote the value and use of public records as a national information and education resource
- to raise the standard of records management in government and to improve the selection of public records
- to improve access and preservation by harnessing developments in copying technology.



# Contents

---

<b>Guidelines on electronic records management</b>	7
Intended audience	

---

<b>1. Introduction</b>	9
1.1 The need for procedures	
1.2 Developing procedures	
1.3 Strategies for improving electronic records management	

---

<b>2 : Creating and capturing records</b>	19
2.1 Types of electronic record	
2.2 Sources of electronic records	
2.3 Record capture	
2.4 Naming conventions	
2.5 Document and record metadata	
2.6 File/folder metadata	

---

<b>3 : Managing and maintaining records</b>	39
3.1 Organisation, access and retrieval mechanisms	
3.2 Access management, accountability and audit	
3.3 Managing e-mail as records	
3.4 Managing records on websites, Intranets and the GSI	
3.5 Review of systems related to electronic records	

---

<b>4 : Inventory, appraisal and disposal</b>	63
4.1 Developing an inventory: knowing what records exist	
4.2 The sample inventory form	
4.3 Developing an inventory in an unmanaged environment	
4.4 Planning for appraisal: developing a selection mechanism	
4.5 Disposal	

---

<b>5 : Preservation of electronic records</b>	83
5.1 Purpose of preservation	
5.2 Developing a preservation strategy	
5.3 Migration of records to new computer systems	
5.4 Selecting and refreshing physical media	
5.5 Back-up of electronic records	
5.6 Preservation of contextual metadata	
5.7 Export of electronic records	
5.8 Environmental storage conditions	
5.9 Documentation and security	

---

<b>6 : Transfer of electronic records</b>	93
6.1 Purpose of transfer	
6.2 Formats used for transfer	
6.3 Formats used for presentation	
6.4 Media and channels for transferring records	
6.5 Transferring the records	

---

<b>7 : Annexes</b>	105
A: Safeguarding records across Year 2000	
B: Outline functional requirements	
C: Relevant standards	

---

<b>8 : Index</b>	118
------------------	-----

# Guidance on electronic records management

This is one of a series of guidance documents on the management, appraisal and preservation of electronic records in government, produced under the auspices of the Electronic Records from Office Systems (EROS) Programme of the Public Record Office.

This guidance document focuses on procedures for best practice in electronic records management, aiming to translate general principles into practice. Volume One describes general principles of electronic records management in more detail. This volume concentrates on:

- best practice in records management procedures for capturing, keeping and making available electronic records
- the development of inventories, and the process of appraisal and disposal of electronic records
- strategies for permanent preservation, and the current requirements for transfer of records in electronic form to the Public Record Office.

The guidance in this series focuses on office documents as electronic records. At the present time, these typically consist of the type of documents – text-based word-processed documents, e-mail messages, spreadsheets, presentations and scanned image documents – which are found in many standard desktop office environments. With the rapid development of information and communications technology in government, however, a wider range of record types will emerge: website (hypertext) documents, multimedia documents, digital audio and video, and dynamically interlinked documents. Many of the developments in desktop information technology will tend to blur the boundaries between types of records, and increase the problems of capturing and retaining all elements of a record.

Best practice in records management is continually evolving. As issues emerge and are addressed, and as further best practice in managing electronic records is defined, this guidance will be developed and updated both by revision and the publication of new material. Guidance on electronic records management, case studies and other material is available in print form, and on the PRO website at <http://www.pro.gov.uk/recordsmanagement/>

---

## Intended audience

The guidelines in this whole series are primarily intended for government business managers, Departmental Record Officers, Heads of IT and Information Systems, strategy and planning managers, project managers and PRO

Client Managers. This volume is intended for the practitioner, and describes what should be done to put the principles of electronic records management into practice. The guidance is intended primarily for those working in central government; but much will also be relevant in local government and throughout the public sector.

This document describes practical procedures of electronic records management, and is intended as a pragmatic overview of the type of management controls which should be implemented in the working environment. It is primarily intended for the practitioner who has responsibility for day-to-day operational management of records, and for those planning for (or influencing) the implementation of corporate electronic records policy in IT systems. Both records management and IT communities need to have a clear understanding of the issues involved. Future publications in this series will offer more detailed guidance on practice and procedures in specific system environments.

Throughout this document the term 'department' should be taken to apply to any public sector organisation, including all departments and agencies across government. The term 'record manager' refers to both Departmental Record Officers (DROs) and other managers who have some operational responsibility for records management.

# 1 : Introduction

1.1 This document is the second volume in the series of guidelines for the *Management, appraisal and preservation of electronic records*, produced by the Electronic Records from Office Systems (EROS) Programme of the Public Record Office. The first volume, entitled *Principles*, concentrates on policies and principles for electronic records management, aiming to identify why this is an important issue for senior managers and strategy planners to engage with, and to recommend some broad approaches towards doing so.

1.2 This document concentrates on the practice of electronic records, recommending the records management controls by which the principles expressed in the first volume can be made concrete and achievable - what needs to be done. The structure of the document broadly follows the natural lifecycle of the record. It addresses five topics:

- the need for procedures and how these can be developed from policy
- creation and capture of electronic documents into record-keeping systems
- keeping and management of electronic records within record-keeping systems
- inventory control, appraisal, selection and disposal of electronic records
- long-term and permanent preservation, and transfer to the Public Record Office.

Organisational issues and systems design issues are covered in the first volume of this guidance.

1.3 A 'record-keeping system' is a general purpose system in which records are maintained for operational access, and to serve as instruments of accountability; it may take one of several different forms in different environments. A specialised electronic records management system is one kind of record-keeping system, and provides well-defined and distinctive facilities within a more constrained technical environment. In this document, the phrase 'record-keeping system' is used to denote a system designed to incorporate aspects of record-keeping appropriate to the use, context and level of information technology in place in the organisation.

1.4 This section deals with:

- the need for procedures to guide the handling of records
- the need to assert intellectual control over records
- the need to design sustainable record-keeping systems

- the formulation of procedures from a broader policy statement
- strategies for improving electronic records management.

### The need for procedures

1.5 Whatever the extent of information technology systems installed in the organisation, there is a need to develop an appropriate level of procedures which can guide and govern their use. These procedures should be developed for use across the whole organisation, and aim to provide a consistent and understandable working environment which is able to support the creation, use, management, disposal and preservation of electronic records over time. Robust procedures can help to:

- support innovation and better ways of working
- avoid duplication and wasted work by standardisation
- make a broader range of information accessible to a wider range of people
- prevent the loss of records
- provide a more flexible response to organisational changes
- assist the organisation in meeting its responsibilities.

Effective electronic records management works hand-in-hand with effective information management to achieve common aims. It does so by creating a closer fit between user behaviour in handling information, record-keeping requirements and organisational development, and in demonstrating the value which electronic records add to the enterprise and to government as a whole. Records management is concerned with gaining control over the recorded information which an institution needs to do business – and is therefore vital to the success of the organisation.

### Asserting intellectual control of electronic records

1.6 Information technology is now pervasive in all government departments and agencies. It is not only to be found in central mainstream information processing systems but it is also diffused to the end user, reaching into all parts of the organisation. Local area and wider networking systems link end users together, enabling a sophisticated flow and exchange of information – electronic records – both within and between departments.

1.7 The primary rationale motivating such a widespread use of technology is to enable a more fluid, responsive and innovative use of information in shaping new ways of working and of organising within departments. From a records management point of view, the inevitable effect will be to extend greater flexibility – and also thereby responsibility – to the end user in ensuring that appropriate records are created and ‘registered’ in the first place. In the electronic environment, the records manager is less concerned with the physical

management of records (which will be partly or wholly undertaken by an IT provider) and more with their intellectual management – ensuring capture of content and context, appropriate organisation for present and future access, and the establishment of systematic controls on retention and disposal. In the electronic environment, however, it is difficult to determine what records exist, since electronic records do not occupy visible space.

1.8 The records manager will be concerned with designing and influencing the environment within which records creators and users operate – establishing organisational standards for record-keeping requirements, requiring that new information systems incorporate easily understandable facilities to support these, providing guidance and direction for operational users, and working to develop an organisational culture of record-keeping. The development of well-understood and robust procedures which can be applied at all stages of the records life cycle and in all parts of the organisation, is an essential activity for successfully gaining control of electronic records.

1.9 Clearly, this will be a long term strategy where tenacity and consistency of purpose will win the day. The records manager should strive to extend control of the current situation whenever opportunity admits, as well as preparing for the future by incorporating a records management perspective in new information systems developments and organisational changes. Even, or especially, where the current policy of the organisation is ‘print to paper’, records managers should, within this transition phase, endeavour to build the necessary infrastructure which will be able to support a high quality of records management in parallel with organisational and technological change as it occurs, rather than simply as a response to unforeseen problems.

1.10 The International Council on Archives recommends that those involved with managing and safeguarding records should:

- ‘be involved in the entire life cycle of electronic systems that create and retain archival records to ensure the creation of electronic records that are authentic, reliable and preservable
- ensure that record creators create and retain records that are authentic, reliable and preservable
- manage the appraisal process and exercise intellectual control over records
- articulate preservation and access requirements to ensure archival records remain available, accessible and understandable.’ (see Annex C for reference).

Designing an environment for sustainable record-keeping

1.11 A record-keeping system is made up of the technology itself, the people who use the technology in their day-to-day work, and the organisational and management controls which determine acceptable activities and business outcomes; procedures are the practical definition of this system. These three elements are interdependent – when one element changes, the others must adjust accordingly – and finely balanced in a system which is well established and working satisfactorily.

1.12 The guidance on procedures in this document is intended as a guide to action for those with a records management responsibility, but does not offer prescriptive formulae which will be effective in all situations. While there are some elements which describe particular requirements of the Public Record Office (for example, in relation to acceptable transfer formats for electronic records), other elements will need to be adapted and evolved to fit the local situation. Recognising that departments and agencies will be at different stages of development and deployment in their use of information technology, the basic requirement is for records managers to ensure that the appropriate records management controls for the level of IT which is in use are developed, and made clear and effective.

1.13 Additionally, wherever possible, there is a need to anticipate new developments and evaluate the implications for electronic records, to ensure the continued relevance and effectiveness of the record-keeping systems and to safeguard records for future business and PRO requirements. Bearing in mind that a print-to-paper policy is not likely to be sustainable in the long term, records managers should already be planning for a fully electronic environment, which may well require an adaptation of current information and records management practices. Experience in many fields shows that as staff, and the organisation as a whole, become familiar with working (primarily or completely) within the electronic environment, there is a tendency to think less about making copies for the paper world. More information is generated electronically – for instance, by the more significant use of e-mail – that should be considered for the record, and less of this material is printed to paper and filed. Although the formal organisational policy remains, the de facto policy tends towards treating the electronic record as the primary copy.

1.14 In this context, an evaluation of appropriate procedures should take account of the existing situation in practice, and develop a transitional strategy which can assist the organisation in making a smoother passage to the fully electronic environment, without the loss of corporate memory or accountability entailed by unmanaged electronic records.

---

**Developing procedures**

1.15 The Public Record Office places importance on the development of formal corporate policies which establish the importance of electronic records and the principles which should guide their management. Such a policy statement, endorsed by senior management, is a strong platform for the systematic development of consistent organisation-wide procedures, and provides backing when seeking compliance in practice. The first volume in these guidelines, which deals with the principles of electronic records management, gives guidance on the development of a corporate policy. Here, this section offers an approach to the development of practical procedures assuming a policy statement which already exists.

**Formulating procedures  
from policy**

1.16 The process of formulating procedures from a more general policy statement involves the identification of specific areas of business activity in which the broad principles can be packaged and expressed as working procedures that are easily related to day-to-day operational activities. These policy packages are a specialisation of general policy principles for electronic records within a particular well-defined area. They are put into the context of specific working practices and records management needs by the development of practical procedures, advice and guidance which embody the principles in action. For example, some key areas in which development of a policy package might have an early initial impact are:

- procedures for the capture and management of e-mail messaging as electronic records
- developing records management practices for electronic documents within an MS Office system
- managing records within an Intranet, or within an Internet website
- exchange of records between departments over the Government Secure Intranet.

1.17 The sequence of activities within a typical cycle for developing a policy package, as part of a wider implementation process, are:

*Detail specific areas*

Identify and prioritise key areas for earlier implementation of the electronic records policy, based on factors such as:

- an identified strategy for developing an aspect of electronic records management
- making a valuable contribution to key departmental objectives
- compliance with legal requirements

- areas which are most feasible, and would take a relatively short time to carry through
- areas which could yield useful and visible results, and confer a high profile and good publicity
- areas which involve manageable numbers of people who are well motivated for success.

*Develop procedures*

Develop the required procedures which will lead to desired practical outcomes, examining the impact on existing systems, determining and allocating roles and clear lines of responsibility. Develop the necessary guidance and training measures needed to support implementation of these procedures.

*Establish testing and monitoring criteria*

Devise performance measures and other mechanisms which can be used to determine the degree of compliance in actual practice.

*Validate and review*

Determine what action can be taken when problems are identified, and potential strategies for tackling them. Carry out the monitoring and review process.

1.18 This general approach to the development of practical procedures will be guided by the development of a strategy for closing the gap between the actual situation as it is embodied in current practice, and the desired situation as expressed in formal policy. While a policy is a statement of general principles, a strategy is a means for putting those principles into action.

---

**Strategies for  
improving electronic  
records management**

1.19 This section is intended to demonstrate examples of how policy issues relating to electronic records can be developed into more concrete statements, that should be widely broadcast in the organisation and incorporated into more detailed procedures and operational plans.

1.20 Each of these areas first states the underlying general principles and follows with the specific strategies to put them into practice. Making such strategies explicit is a useful guide to action for those who are faced with developing and building on electronic records initiatives in a particular departmental context. They can be cascaded down into specific operational situations by developing a more finely-grained focus and detailed procedural guidance. This top-down approach will be helpful in encouraging equivalent

broad outcomes for records management even though the means of achieving these will vary according to the demands of the particular situation.

1.21 The general principles identified here are discussed in the first volume of these guidelines; the later sections of this guidance amplify the strategies in terms of specific procedures for each of the three main sections.

Creating and capturing  
electronic records:  
*Principles*

1.22 For each business process, it must be possible to capture the records that provide evidence of the business activities emerging from that process, where this is conducted by electronic means.

1.23 Records which are captured should be authentic and complete representations of the business activity from which they are derived, and should retain their context of use.

1.24 Record capture mechanisms should capture all necessary metadata needed to access and manage the electronic record throughout the full lifecycle.

1.25 For each record-producing system, responsibility for ensuring record-keeping requirements are met should lie with nominated individuals, and overall with the organisation as a whole.

*Strategies*

1.26 The boundaries of business processes and systems, and the legal and other requirements that affect them, should be well defined and understood to enable the capture of electronic records of the resulting transactions.

1.27 Each business process should be assessed to determine and articulate the record-keeping requirements and records management practices that should be applied to them.

1.28 The limits of corporate, workgroup and individual workspaces, and the rules which apply to documents and records that cross the boundaries between these workspaces, should also be defined.

1.29 Record-keeping requirements should specify which electronic records types should be captured and maintained in electronic format as the primary record, which should be converted to a non-electronic format, apply this consistently across the organisation, and develop mechanisms for assessing compliance.

1.30 Record-keeping requirements should articulate all metadata elements which are necessary for the management of each electronic record type; record-generating information systems should provide the facilities necessary to support capture of this metadata, and its retention with the associated record.

1.31 Users of electronic records management systems should be made aware of their roles and responsibilities, and end user policies and guidelines should be described in appropriate detail and widely disseminated.

Maintaining and managing  
electronic records:

*Principles*

1.32 Record keeping systems should be designed to meet the needs of all stakeholders and necessary system functions, where appropriate including electronic document and image management, electronic records management, and workflow systems, without compromising the integrity of the record.

1.33 Records managers should make comprehensive efforts to become aware of, and make accessible, all electronic records across the organisation, and to support corporate information and knowledge management and new ways of working while ensuring adherence to record-keeping requirements.

1.34 Electronic record-keeping systems should be designed to manage the content, context and structure of records as a whole and to ensure that records remain reliable and authentic.

1.35 Where they are designated as the primary record, electronic records must be maintained in accessible electronic form.

1.36 Record-keeping systems should aim to ensure that all records which should be kept are retained, and that all records which should not be kept are destroyed.

*Strategies*

1.37 Record-keeping requirements which an electronic records management system must satisfy should be identified and described, including operational needs from the business domain, accountability requirements, and wider responsibilities to society and the cultural domain.

1.38 Record-keeping requirements, which may be satisfied by dedicated electronic records management software systems or by designing and implementing record-keeping functionality into systems not primarily designed

for that purpose, should be consistently implemented across the organisation.

1.39 Record-keeping systems should provide an auditing mechanism to quality assure implementation of record keeping requirements.

1.40 Electronic records management systems should provide a mechanism which allows authorised users to discover which records are available for use, and which tracks use of these records to ensure authenticity.

1.41 In enabling access, electronic records management systems should be capable of controlling user access to categories of records, by allocating allowable actions and access rights to an individual user or a user group

1.42 Appraisal should be undertaken during system design if feasible, based on analysis of business processes, or as early as possible in the life of existing records, to mitigate the need for unnecessary continual migration of records and to safeguard continued maintenance.

Preserving accurate and  
accessible electronic  
records:

*Principles*

1.43 Electronic records must be maintained to ensure that the content, context and structure is accessible, comprehensible and managed for as long as recordkeeping requirements determine.

1.44 Electronic records must be maintained for as long as recordkeeping requirements determine, without loss of information, and must be disposed or transferred as appropriate.

1.45 The organisation should provide appropriate electronic access to records irrespective of their location, both within and beyond the boundaries of the organisation.

1.46 The organisation should protect its electronic records from inappropriate access.

*Strategies*

1.47 The records management function should establish standards and procedures to ensure the integrity of its electronic records over time.

1.48 Electronic records of continuing value should be migrated through successive upgrades of hardware and software in such a way as to retain the

context, content and structure and the integrity of the electronic records created in earlier systems, utilising approved technological standards.

1.49 Recordkeeping systems should identify, capture, maintain and migrate the metadata required for electronic records and the systems that create them, including contextual information about the records and the activities that they document, in conjunction with the records themselves.

1.50 The connection between the records and the metadata should be maintained for as long as the records exist, across successive migrations to upgraded hardware and software systems.

1.51 Recordkeeping systems should enable the export of electronic records, without loss of content, context and structure, for transfer to permanent preservation according to PRO standards and guidelines.

## 2 : Creating and capturing records

2.1 This section deals with the capture of records into the record-keeping system. The computer systems in use may be a formal electronic records management system which will provide facilities to actively support capture, or a looser organisation of material across an office network. The collection of management controls and procedures which govern the operation of the software and hardware environment binds all these elements together into the record-keeping system. In either case, procedures will have to be defined to determine:

- the types of electronic record which can be captured by the system
- the kinds of document which should be captured as a record
- the points at which a working document should become a formal record
- the naming conventions by which a record can be titled
- the metadata which should be kept with the record.

---

### Types of electronic record

2.2 Electronic records within the office environment can be generated from a wide variety of different sources, and appear in a wide range of different formats. Unlike the records which are generated by large database systems or datasets, there is rarely a one-to-one correspondence between application system and record collection. In an office systems environment, the same few general office applications will be used to create documents and generate records across the full range of business activity in the department. These may be stored in a file or folder at any point within the corporate filing system. A typical file or folder of electronic records may potentially contain a variety of physical record types. It will obviously be important to consider these physical forms when planning for future maintenance and preservation of access, to ensure that adequate knowledge about the record is captured in the first place.

2.3 The complexity of physical format in electronic records is evolving at a rapid pace. At the present time the majority of electronic records in office systems will be simple text-based records or relatively uncomplicated spreadsheets, currently the main staple of the typical desktop. As software applications become more advanced, the complexity and interactivity of the documents which they generate becomes more sophisticated, adding note and voice annotations to text-based documents, digital sound and video to presentations, 3-D modelling and simulation to analytical documents. A broad categorisation of electronic record format types is:

*Text-based documents*

Although simple text records present significant problems for capture, management and maintenance, more advanced text documents will add new non-text elements, and develop a less clearly defined presentational format. It is common for a single document to be built from the various elements of an integrated office automation suite by embedding components one within another.

*Multi-dimensional documents*

Some forms of electronic record can be represented in more than one way on the screen and on the printed page. A spreadsheet can be represented as either a set of base figures and formulae, or as the result of the calculations – both are part of the record, although it may not always be necessary to retain them. A presentation may consist of a set of prepared slides and speakers notes, which can be displayed and used in different ways.

*Multi-media documents*

Multi-media documents are composed of a number of different elements which interact together to display their full meaning – graphical, moving image, sound and text elements – which may be capable of behaving differently at different times in response to variations in user interaction.

Managing the record as a whole

2.4 There is a clear trend for documents to:

- become more and more multi-media based
- be composed of separate re-usable components
- have a virtual, network-based, rather than physical, disk-based, existence
- to be able to take different presentational forms for different uses.

These changes require that the record is managed as a coherent whole, rather than as individual physical units. This is an essential difference between document management and records management – the ability to capture, keep, and make accessible the integrated record rather than a collection of unrelated document parts. In developing electronic records management, DROs and IT specialists should aim to build procedures and systems which are capable of working at the level of the entire record.

---

Sources of electronic records

2.5 The route through which the record is generated, or received into the organisation, is a helpful way of categorising electronic records in order to develop procedures for their effective capture and subsequent management. Electronic records may be generated internally within an organisation and

distributed via a local area network, be received from outside the organisation through a wide area network, or emerge from material mounted on an Intranet or public Website. In some cases, an electronic record may also be generated from an original in another form – from paper or microfiche, for example.

#### Records from a local network

2.6 A substantial proportion of electronic records in office systems will be generated by the normal range of office applications, such as word processors, spreadsheet programs, or graphics packages. Sturdy procedures and clear guidance are necessary in an open office environment where end users have a substantial degree of autonomous control over the creation and filing of records. The use of standard templates and document property settings can help to produce consistent record metadata. In an enterprise-wide corporate document system, there may be scope for integrating record-generating applications directly with the record-keeping system to ensure capture at the time of initially saving the document.

2.7 Internally generated e-mail messages are now widely used to convey formal information and may attach or comment upon significant documents; as such it is an important source of electronic records. Capturing e-mail is problematic because:

- messages are often given a lower status than more formal documents in the mind of the end user, even though the actual information content is as significant
- the distinction between ephemeral and important, one-to-one and broadcast e-mail messages is rarely explicitly flagged
- the structure of the information content is poorly managed in a set of messages – for example, a reply may or may not include the text of the original message.

#### Records from an external network

2.8 A similar range of potential records will be received from sources outside the organisation, most probably by means of an external network. Two principal types will be:

- documents and e-mail messages which have been generated outside the organisation, initiating or in response to a communication
- records received from another organisation or branch, which may already exist in, or have been extracted from an electronic or conventional record-keeping system.

Website/Intranet records

2.9 One particular source of potential records which is likely to grow in importance in the near future, for most government organisations, is the departmental Intranet or public Internet Website. The corporate Intranet is increasingly seen as a primary means for the distribution of enterprise-level information, typically containing operational policies, procedures manuals and organisational information resource bases. The public Website may well contain documents which have accountability implications – for example, giving advice or instructions on carrying out some activity.

2.10 This is material which should be captured as formal records; ensuring this happens should be built into the process by which an Intranet or Website document moves from creation to posting on the network, in such a way that control over versions and datestamping is possible. In larger-scale sites, individual documents may have given way to structured textbases which create virtual documents for the viewer ‘on the fly’ as they are asked for by a user. In this case, version control will be particularly important; a similar problem to that presented by the more conventional database.

2.11 Increasingly, websites offer two-way communication, enabling a remote user to send information to the organisation by means of a form-filling process. As mechanisms for electronic government develop, this will undoubtedly become an important source of electronic records which will need to be captured and related to any further responses or resulting actions.

Records converted from a different format

2.12 One method of linking together related conventional and electronic records is to generate an electronic version from the original. This approach can be used in two ways:

- to scan retrospectively back runs of paper records to an electronic format: this is an expensive option which is unlikely to be cost effective in many cases
- to make an electronic copy of incoming paper as it enters the organisation, where this contains significant material.

2.13 These approaches have the advantage of enabling the integrated handling of conventional and electronic records in storage, classification and retrieval, but may have significant processing overheads. The department will need to establish the correct balance between the business advantages which paper scanning offers against the costs of the process.

2.14 In all cases in which paper records are scanned to an electronic version, careful attention should be paid to the legal implications of this action. From the point of view of the Public Record Office, an electronic version of a paper original is acceptable providing it is subject to the proper records management procedures that can demonstrate its authenticity, and that these are correctly audited. However, for records which are required to be kept under other legislation, there may be more particular requirements to be met; in cases of doubt, records managers should seek legal or other professional advice.

2.15 Particular care should be taken to ensure that the electronic records are capable of long-term preservation, and that this is assured before any action is taken on the paper originals. The PRO Client Manager should always be consulted before any large scale conversion exercise of records which may be selected for permanent preservation.

---

### Record capture

2.16 Within a department, documents are created to serve a wide variety of functions and roles. While some will record important aspects of departmental business, others will have no interest to anyone beyond the original creator; and between these two extremes, many documents will begin life as the initial drafts of an individual, and progress through various working versions to a finalised text. In the paper environment, each of these versions will have a separate physical existence, and where appropriate can be placed in a registered file. In the electronic environment, without intervention, later versions may overwrite earlier ones that would have normally been kept in the paper environment; on the other hand, it will usually be inappropriate rigorously to keep every electronic version, however insignificant the changes. In the electronic environment, records managers will need a clear view on documents which should be captured as a record, and on the point within the lifecycle at which those documents should become records.

### What should be captured as a record?

2.17 Records document the business of a department, and are produced by the business processes within the organisation. Within a single-application information system, such as a transactional database, this may be a fairly straightforward process; within an organisation-wide office system which is related to many business processes, essentially the end user will be making day-to-day decisions to determine the significance of documents as records. Records managers should aim to design record capture facilities that encourage users to make sensible and cogent decisions within the framework of a usable and smooth mechanism.

2.18 This will involve supporting the available technical facilities with clear guidance on:

- the boundaries of business processes, and the activities within them which should be documented
- the kind of documentation which should be kept
- the record-keeping requirements attached to each category of record emerging from these processes.

These will then be the effective criteria that end users will apply in determining which documents should become records.

2.19 With the more complex forms of record which are emerging, attention should also be given towards definition of the boundaries of the record itself. Compound records may include nested or embedded objects (for example a text document may include a spreadsheet) which may in themselves be records in another context. An Intranet document is likely to include links to other elements – some of these essential parts of the document itself, others hypertext links to different documents with a separate identity. In capturing the Intranet record, its boundary will have to be defined – the point at which it is considered to be a complete record – which is likely to include only those elements which are tightly bound with the main text rather than background references.

When does a document become a record?

2.20 Declaring a document to be a record is a formal point of transition at which it passes into corporate ownership. Once designated as a record, the document is no longer managed by the creator but by the organisation as part of its corporate information resources. The record should not thereafter be capable of change, and should be placed within a disposition schedule where it will be retained for a set period; when the retention period expires it can be destroyed, or if merited, transferred to the Public Record Office.

2.21 In the electronic environment, where both documents and records exist in the same virtual space, it is necessary to identify and distinguish between them.

A useful schema to help make this distinction is to distinguish between:

- personal workspace, containing personal documents and early work in draft
- group/team workspace, containing early formal drafts and discussion documents
- corporate workspace, containing finalised documents and formal records.

A typical document will progress through each of these working spaces as it

develops into a formal corporate record in organisational terms. A department will apply its own policy on the extent to which such documents fall within the corporate definition of an organisation-wide information resource: some may consider all documents to be corporate records at whatever stage, others will restrict this to particular categories of documents.

2.22 All documents which relate in any way to official business, however, fall within the definition of public records, and this definition may be much broader than that adopted for corporate-level information. For example, records relating to the work of a project or team will be public records – and should be treated accordingly – even though the department may choose not to make these accessible across the organisation. In an unfamiliar electronic environment, records managers may at first find some difficulty in clearly identifying public records, and making explicit their appropriate treatment: in any doubtful cases, departments should consult their PRO Client Manager at the earliest opportunity.

2.23 In the paper environment, the user will be familiar with the types of document that are routinely dealt with and be used to making decisions, with appropriate guidance, about which of these to ‘put on file’. Much of this understanding, however is implicit and tacit; in the less familiar electronic environment guidance will need to be made more explicit both for the user, and to enable the construction of appropriate software facilities that can support the actions required of the user. This will require records managers to categorise and systematise in advance the types of records that will be encountered, as far as this is possible; and to produce explicit user guidance on the actions necessary to ensure the capture of each type. Different policy approaches and business planning decisions will result in the need for different types of record capture – but the final result should be consistent for both electronic and conventional records. For example, a department may have a policy on whether hand-written annotations on some types of draft document are kept on file; if this is so in the paper environment, then electronic record capture facilities will need to take potential electronic annotations on documents into account.

2.24 Consideration should also be given to:

- the extent to which versions of a document in development should be restricted to significant versions only, and the characteristics by which these are distinguished
- the number of working copies, as against a primary record copy, which should be kept

- the balance between extending the range of record capture, and making those records accessible and effective in retrieval and use.

2.25 In a less structured environment, it will be important to link this guidance with that on naming conventions and filing strategies. In an integrated document management environment, clear user guidance will still be important – unlike with paper records, in most document management systems the entire document (with all its versions) is declared as a record, rather than each individual version separately. The user will need to follow clear guidance, therefore, on the point at which it is appropriate to create a new version.

Capturing the record in a managed environment

2.26 With a sound understanding of which documents (and which versions of them) are appropriate to capture as records, a well structured and managed electronic records environment will be able to implement this by adapting or designing lucid and elegant software facilities to support the user community. These should enable the capture of the record content and all necessary metadata to access and manage the record for the entirety of its lifecycle. In some cases, office applications can be set to require completion of a profile form; alternatively use can be made of the document properties feature where this is available. Default values and application program options should be set wherever possible, so that as much of the required information about the record as possible is captured automatically by the system, and as little as possible is required to be entered manually by the end-user. For standard document types, judicious use may be made of template outlines to ensure a level of consistency.

2.27 The expectation is that in a developed electronic records management environment, the end user will directly file the captured record by the method adopted. Adding documents to an existing file/folder (whether in a corporate fileplan or by using structured classification/indexing terms) will, in effect, be making decisions on the future access and disposal of the record. Where retention and disposal schedules, and access rights and security requirements, are attached to a whole group of records at the folder level, adding a new record to a particular file location will be equivalent to making retention/disposal decisions on that individual record.

2.28 It will be important, therefore, that users have a clear idea of the implications of their filing actions, and that there is some means of assessing whether these are being appropriately applied at regular intervals. In this sense, the end user is acting as the first line records manager, and the quality of system design, usability of the technical facilities, and familiarity with the filing structures will be important.

## Capturing records retrospectively

2.29 Where personal computers or unorganised shared network drives are being used as primary records management resources, records managers may wish to consider capturing this material retrospectively in order to gather it under a formal records management regime. The reasons for adopting this course of action include:

- a recognition of a general reluctance to print, and store the resulting paper, on registered files
- the need to secure these records for future corporate accountability and under the public records legislation
- the increased retrieval opportunities offered by electronic storage
- support for better exploitation of the information.

2.30 The problems with the situation this approach aims to tackle – lack of accountability, auditability and limited recording of corporate history – have become characterised as the records ‘black hole’; surmising that the volume of paper placed in corporate filing systems may have significantly lessened since documents began to be created electronically, as the user at the desktop becomes increasingly at home working in the electronic environment. In such cases, only the electronic version of a record will exist by default. To achieve compliance with existing paper based records management procedures, the records manager has to choose either to ignore those documents that might not have the same provenance and authenticity as paper records on registered files, or to attempt to salvage as much as possible and preserve them as records.

2.31 An approach to capturing and preserving records retrospectively is described in section 4 of this document. Once captured, the electronic records must be made available to all who require to use them. This may be achieved by placing them on a central server and permitting access through a local network, or by making available on an Intranet. Alternatively, a stand-alone PC located in the Registry or Library could be used to deliver limited access. Access may need to be restricted because records contain sensitive information; and provision must be made by login access protection or by restricting access to their physical location.

2.32 Once this retrospective capture has taken place, records managers should take steps to ensure that the circumstances which produced this material do not recur, and future record generation is, as far as possible, brought within a managed environment. This can be furthered by encouraging the adoption of procedures such as naming conventions, consistent and structured filing systems, and the use of templates and standard document settings.

---

**Naming conventions**

2.33 Naming conventions provide a set of rules which assist the individual end user in allocating a title to a document at the time of creation, and which provide a framework for the naming of folders that hold a group of documents. Adherence to a consistent naming scheme is good information management practice which should ideally be applied to both personal and working documents, as well as to documents which are corporate records. Maintaining a naming discipline in both areas will help to ensure that working documents which eventually become formal corporate records are appropriately titled and linked to related items and previous versions.

**Record and document titles**

2.34 The definition of departmental standards for document/record/computer file names will make it easier for people other than the creator to retrieve information. Understandable and meaningful file names will simplify the task of finding an individual document, and of linking together related documents. The relative scope for sophistication in titling a document is dependent on the available facilities of the office system in use. Previously, for example, earlier PC-based systems imposed a severe limit to the length of document names (such as those based on the 8.3. letter format used by MS-DOS/Windows 3.1), leading to the widespread use of cryptic filenames impenetrable to anyone other than (and sometimes including) the original creator. More sophisticated operating systems, such as the Macintosh OS, Windows 95/98 and Unix graphical interfaces, allow a much greater leeway in constructing titles.

2.35 In these circumstances, there is an opportunity for the records manager to develop naming conventions which support a more systematic handling of electronic records. A frequent tendency for many people, left a free hand, is to opt for a more naturalistic, verbal-style, expression of the title, rather than a structured approach to naming documents. This tends to locate the most specific part of the title to the end of the title string; unhelpful for sorting and viewing many similarly titled documents when browsing through a title list, and a potential cause of ambiguity and confusion.

2.36 Naming conventions for document titles should aim to:

- give a unique title to each document
- give a meaningful title which closely reflects the document contents
- express elements of the title in a structured and predictable order
- locate the most specific information at the beginning of the title and the most general at the end
- give a similarly structured and worded title to documents which are linked (for example, an earlier and a later version)

- avoid the unnecessary use of dates (remembering that the operating system will date-stamp the document at time of creation and edit)
- avoid the use of generic names which are only meaningful in a personal context
- avoid the use of non-standard abbreviations and words that add no value.

For example:

*Records Management - Working Group - Final Report*

is far more useful than:

*Final report of the working group on records management*

as a document title.

Ideally, a controlled vocabulary system (such as a functional or topical thesaurus) can be used as an underlying standard to specify the relevant keywords which make up a meaningful title, and the order in which they should be combined. Whichever naming convention is used, provision should be made for the use of version numbers.

#### Folder/files

2.37 Most departments have a *Manual of Registry Procedure* which, together with the *Manual of Records Administration* published by the PRO, provides general guidance on managing registered files. These files, through the use of naming conventions, provide the means by which individual documents are held in meaningful record collections and indicate the sequence of events amongst the documents. In conventional records systems, a corporate filing structure will have evolved which should reflect the business and operational needs of the department; it may be possible to reflect this in the electronic environment to ensure consistency between grouping and management of paper and electronic records.

2.38 Where it is not feasible to adopt this approach, the DRO should ensure that clear and consistent rules for allocating names to folder/files are developed. This will be particularly important where electronic records are kept in a loosely structured environment, for example in a Windows-based shared disk drive. Adopting this approach will offer a predictable and easy way to organise, access and share information for the end user, and can incorporate some simple records management procedures: for example, dividing long running collections of records into annual segments by creation of part folders. In the less structured environment, it may be useful to make use of folder titling conventions to identify and manage ephemeral material.

2.39 Conventions for naming folders should consider the incorporation of

rules for:

- allocating unique names to folders that do not rely on an incrementing number
- allocating meaningful names to folders, indicating the contents or use
- using folders to group documents into subject-related categories, and to retain some sense of context
- building a folder-subfolder structure by dividing a broader theme into sub-themes
- developing a rudimentary section- or organisation-wide hierarchical folder structure based on functional or organisational lines
- using folders to assist future management of electronic records, by linking to retention and disposal categories where possible
- the use of 'shortcuts', or pointers from one folder to a document located in another, to prevent inadvertent loss or deletion
- renaming of folders (where this is allowed) to avoid loss, confusion and disorganisation.

---

**Document and record metadata**

2.40 Metadata is information about the individual document or record: a list of its particular characteristics which distinguish it as a unique object from other documents or records. As a document, metadata will include elements such as the document title, authorship, keyword indexing terms, and dates of creation, modification, etc.; such metadata is often known as a 'document profile'. Record metadata will include, as well as the document profile, further information relating to the context and history of the document as a record, such as location within the filescheme, access rights, retention periods, and disposal criteria.

2.41 Metadata provide the information necessary to serve a number of different purposes:

- to provide an adequate description of the record itself
- to support retrieval of, and access to, the record by a range of users
- to locate the record within an assembly or record collection
- to support specific functions within a record-keeping system
- to retain contextual information about the record
- to enable future interpretation of the historical record.

2.42 These metadata should support the business and operational needs of the organisation and should include all the elements required for corporate accountability, statutory requirements, evidential admissibility and audit. Metadata information is an important means of grouping the complete record by associating all documents or other information objects (for example, an e-

mail and attached file) which constitute a single record together. There must be contextual information for each document relating it to other documents within the same classification category in the corporate filing scheme.

2.43 Metadata elements are stored in a profile which should be clearly and indissolubly attached to the record. There are two broad approaches to associating the metadata profile with the record:

- the profile information is tightly bound with the record itself, as one physical object (for example, the document properties information which are a physical part of a MS Word file)
- the profile information is held in one database, and the record content in another, with links between associated records (for example, as in some electronic document management systems).

2.44 In either case, a record-keeping system should ensure that metadata cannot become detached from the record content, or lost in some other way, and can always be transferred as a meaningful part of the record when migrating to a new system platform, or transferring into an approved format for permanent preservation.

#### Recommended metadata sets

2.45 The particular set of metadata which it is possible to retain for a set of records will vary according to the technical environment in which they exist, and to some extent with the type of electronic record itself. Administrators of an enterprise-level document management system will be able flexibly to define a comprehensive set of metadata elements; within a poorly structured Windows environment the possibilities will be far more constrained. Records managers should endeavour to define at least the minimum set of metadata which can reasonably be collected in each situation, that meets the fundamental needs of records management.

2.46 The metadata relevant at the level of the individual document or record can be divided into two groups: those elements relevant to each document whether it is a record or not; and those elements relevant to documents which are also records and which need this information to be managed as records.

#### Document level metadata

2.47 Document level metadata elements are primarily concerned with identifying the individual document as a single entity - by allocating a title, author, version number - and with enabling effective storage and retrieval of this item. The term 'document profile' is often used to describe document-level metadata in a document management or office automation context; in this case,

such document attributes will normally be stored as structured information in a database. In other cases, metadata will be bound up with the document object itself: with the “document properties” information in an MS Word disk file; or in the case of an Intranet document, structured information embedded in the document source as html tags.

2.48 The main generic standard on metadata which has emerged is the Dublin Core, or Dublin Metadata Core Element Set. This is a set of fifteen descriptive elements (which can be extended by the use of qualifiers) intended to provide a straightforward means of describing networked information resources for more effective resource discovery and retrieval. It is primarily oriented towards access, rather than management, and to published material rather than internal records; and therefore does not provide a sufficiently complete standard for records management. Although emerging from an Internet environment, it is sufficiently generic to be useful in a wide variety of situations and has successfully been used as the foundation of several specialist metadata standards, and enables a level of interoperability. Full information on the Dublin Core standard can be found at <http://purl.oclc.org/dc/>

2.49 The term document is here used in a general sense, to include the full range of material types generated by office systems (including spreadsheets, e-mail messages, graphical images, etc) as well as text-based documents. Recommended document level metadata elements are:

***Document/record title:*** the formal title of the document, as it appears in the computer system (equivalent to the computer file title), rather than the alternative title which may be available in a document properties form; the subject line of a e-mail message

***Author or originator:*** the name, rather than login id, of the person or team that is the author of the document; or the person who caused the document to be brought into the organisation

***Date of creation:*** initial creation date, as shown in a directory listing

***Date of last edit:*** date of last changes made to the document

***Version number:*** an incrementing number which enables different physical versions of the same logical document to be linked together

***Subject information:*** keywords or subject terms describing the document

content, whether allocated on an ad hoc basis, or from a controlled vocabulary such as a thesaurus

**Description or comments:** a textual description of the document, which may describe role and purpose, or its relation to other documents

**Document type:** identifying the logical document types – e.g. report, memo, letter – which may be a useful aid to identification or processing choices

**Format:** the physical application format type, equivalent to the filetype of the disk file (e.g. the 3-letter filetype, such as .doc, .ppt, .gif, used in a Windows environment)

**E-mail specific attributes:** metadata elements specific to an e-mail document which should be retained with the content are: the list of recipients to whom the message was addressed; the date and time of despatch; the date and time of receipt.

Many of these elements can be mapped to the generic Dublin Core metadata standard; as yet, this has not been extended to a generally accepted metadata set which meet the full semantic requirements of records management.

#### Record level metadata

2.50 Record level metadata are those particular elements which should be associated with documents that have been declared as corporate records, and which are necessary to apply full electronic records management controls. While recognising that departments are at different points of development in the control of electronic records, record managers should take every opportunity to gain control over the collection and application of record metadata.

2.51 Record metadata are primarily oriented towards the management of documents as records, covering areas of access and security, relationships with other records, and with presentational versions of the record. In a properly managed environment, records will be held under the intellectual control of the records manager, and will not be capable of being altered. Metadata relating to some aspects of records management will be more appropriately held at the file/folder level. Recommended record level metadata are:

***File/folder classification or directory path:*** the title of the folder or other record grouping to which the record belongs, and with which it will be managed as one group; this should be identifiable within the corporate file or classification scheme, or include a full directory path from which the relationship with other folders can be deduced.

***Linkage between record elements:*** to enable the linking together of physically separate documents or elements which constitute the complete record (for example, a document attachment to an e-mail message)

***Date registered in system:*** the date at which the document was captured, or declared as a record, and entered into the system

***Audit trail:*** identification of users who have taken significant actions on the record through its lifecycle (for example: create, edit, copy to new version)

***User access restrictions:*** identifying any restrictions on user access groups, which may be in relation to protective markings

***Protective marking:*** level of security classification, which will have implications for user access restrictions

***Sensitivity review date:*** the date at, or time period after, which a review is appropriate

***Presentation versions:*** linking between versions where the same record is held in different formats for preservation and for viewing, or where sensitivity editing has resulted in creation of a variant version.

Capturing metadata from the system

2.52 Most desk-top office packages give the user the option of completing a summary information box. In unmanaged environments, this is where much of the metadata required by records management procedures is likely to be found: some of this will have been completed through default values entered directly by the application; some may have been entered by the conscientious user.

2.53 If default settings are possible, this dialogue box should be set to be completed on first creation of the document, and appropriate guidance issued to users to encourage the completion of useful and consistent information. While this does not ensure that the information will actually be entered, if sensitively

approached it will encourage a climate of good record-keeping in the long term. Care should be taken when the record is archived, migrated into any other format, or captured into a formal record-keeping system, to transfer existing metadata with the substantive content; this is not an automatic process, and often if simple copying or conversion procedures are followed such metadata will not be preserved.

2.54 In a variety of situations the data in document property attributes can be changed inadvertently. A combination of incorrect or ambiguous settings (for example, setting dates to change with edit, save or access actions), and sharing or joint editing of documents between different individuals, can easily produce misleading or erroneous information. Excessive reliance should not be placed on the quality of metadata which emerges from this source unless systematic and well thought-out procedures and clear guidance on their application has been produced. On the other hand, an effective use of this facility in combination with the use of application-level fields and programming tools can produce a rich seam of metadata from an otherwise barren records environment.

2.55 More sophisticated software environments, such as electronic document management systems, will offer much greater facilities for collection of metadata, including the ability to force completion of additional metadata properties by a user before completing the creation and saving process. Similarly, in the Intranet environment, many tools exist for the gathering of metadata relating to existing documents across the network; and these are beginning to become available for the desktop environment. The quality of the metadata acquired, however, will be very dependent on the depth and consistency with which it was embedded in documents initially.

#### Capturing metadata in unmanaged environments

2.56 Clearly, in many cases, the creation of electronic documents predates the development of appropriate management procedures to ensure that an adequate level of metadata is captured. It is possible that records of archival worth may be held in a poorly structured environment with no supporting metadata, and with no apparent relationship between them. File storage on desktop computers does not support comprehensive metadata creation and users can choose whether to enter any; so there is likely to be a paucity of metadata. Records manager should attempt to retrieve what metadata can be made available for records which may be of long-term value, and care should be taken to preserve this information through successive stages of migration wherever possible.

2.57 In such cases, some required metadata may be capable of extraction from the documents themselves (for example, author name in a text document) at the time of transfer to the PRO. Metadata is also likely to be found in directory listings (for example, the computer file information in Windows Explorer) and document properties features. The PRO Electronic Records Accessions Unit may be able to offer advice on these aspects, on a case by case basis.

#### Controlling dates

2.58 A particular problem in documents from office systems relates to the use of dynamic dates. The display dates (as well as some other elements) in document headers and footers may be taken dynamically from attributes held elsewhere in the document metadata – date of last edit, date of printing, current date – and inserted into position separately on each viewing. This can be a useful facility for distinguishing different versions of a document which is still in process of development, but will be a liability once the document is declared as a record, forcing a continual updating of information within a record which should not be changed.

2.59 The DRO should ensure that procedural guidance is available for users to follow which will avoid the problems of dynamic date change and meet the requirements of effective electronic records management. There is no one prescriptive solution and these procedures will vary according to organisational requirements and the particular application packages used; however, dynamic date fields should, wherever possible, be removed at the time a document is filed as a record.

---

#### File / folder metadata

2.60 While record metadata identifies the attributes which apply to the individual record, file or folder metadata identifies the attributes which apply to whole groups of records. This metadata will serve four main functions of electronic records management:

- grouping records together – providing an identifying label under which similar records can be grouped together, and which distinguishes separate groups from each other
- showing how groups relate to each other – enabling a linking structure which can show the place of one group within the wider semantic structure of the classification or filing scheme
- enabling management of the group of records as a whole – so that the records can be retained, scheduled and disposed of as a consistent group
- enabling access to the group of records as a whole – to demonstrate the narrative context in which records should be understood.

Folder level metadata can also be used to link together conventional paper and electronic filing structures, where these are not in themselves identical; and are an essential element in linking hybrid assemblies where electronic and paper records are contained in one folder.

Recommended folder  
metadata set

2.61 The recommended metadata set at the folder level is:

- **File/ folder title** or record assembly title : the formal, controlled title of the record grouping, whether a numerical, structured heading, or controlled thesaurus terms. In poorly structured environments, this may consist of a folder path within the directory hierarchy, identifying the folder within the context of its owning folder
- **Subject terms**: any subject terms, or keywords, used in addition to the folder title itself
- **Description or comments**: a textual description of the folder content, which may be used to identify role and purpose, or its relation to particular business uses
- **Access restrictions at folder level**: identifying restrictions on access to the folder as a whole by indicating allowable user access groups
- **Physical location**: physical storage location of the folder and its contents
- **Open/close dates**: the date of folder creation (or on which the first record was added) and the date of closure (or on which the last record was added).
- **Related file/folders**: relationship to other folders, in either a parent-child hierarchy or horizontally to those containing related material
- **Barcode** (paper): identifying label for paper files, or the paper element of hybrid assemblies, only
- **Retention period**: the standard period of time for which records in this group should be retained in the department
- **Disposition**: the action to be taken at the end of the retention period
- **Archival value**: to identify folders which may be candidates for permanent preservation in the Public Record Office
- **Disposal action**: the action that was taken at the end of the retention period
- **Disposal date**: the date this action was taken
- **Disposal authority**: authorisation for the action to be taken.

Folder level metadata should be retained after record groups have been destroyed, to document the action that was taken on the records as part of the formal scheduling process.



## 3 : Managing and maintaining records

3.1 This section deals with:

- corporate indexing and filing systems
- retention and disposal schedules for active electronic records
- the management of access and user groups
- authentication and audit management
- legal admissibility of electronic records
- managing e-mail as records
- managing records on websites, Intranets and the GSI
- reviewing record-creating systems and maintaining awareness.

---

### Organisation, access and retrieval mechanisms

3.2 The need for a form of structured organisation for records is discussed in the first volume of this guidance, and is not repeated here at length. Organisation and retrieval are complementary activities, which together determine the sophistication with which the record collections can be accessed and made available for use. Both pre-coordinated, controlled vocabulary, methods of organisation and post-coordinated, keyword-based, systems are needed to provide a range of sophisticated access mechanisms. The former provides the user with a predictable method of context navigation, positions a set of records in relation to others, and enables their management as one group; the latter provides flexible access to record content, bringing together records with similar topics that have been separated by the primary filing scheme. Sophisticated access mechanisms are needed to:

- prevent time wasted by the user in looking for records or particular content
- prevent time or effort wasted in using a non-current version of a record
- provide a common corporate view of the information resource
- present a record within the context of a narrative of events to which it relates
- enable the common management of physically separated records as one group
- enable the user to search one common access space using consistent descriptors.

At the present time, search engines cannot provide a reliable and usable method of delivering these requirements. A record can be lost, even though it is present in a storage and retrieval system, because it is not capable of being found.

Corporate filing/indexing systems

3.3 Electronic documents can take a number of different logical forms and physical formats; whatever the document, there needs to be some form of corporate filing structure in existence to prevent the loss of records and to facilitate access. This filing or indexing structure, through the use of naming conventions, provide the means by which individual documents are held in meaningful record collections and indicate the sequence of events amongst the documents, establishing a narrative of events. Operating system file directories do not offer this function; however, effective electronic records management (as opposed to electronic document management) requires this, either as part of the original design specification or by having it added to an existing system.

3.4 The type of folder or file reference adopted needs to be flexible, with the potential to expand to meet changing departmental requirements. The file structure and naming conventions should reflect the wider business need of the creating department and not just those of the immediate users. The principles which inform existing registry practice should be closely examined and, where appropriate in this new context, used to develop the design criteria for naming conventions in electronic form.

3.5 A hierarchical map of business functions and activities can be used to help with the creation of a corporate filing plan or directory structure. The functional map can be used in conjunction with a functional thesaurus (for example, the Keyword AAA thesaurus used in public administrations) to establish naming conventions for the structures in which the electronic records are organised. Such an activity-based structure reinforces the concept of electronic records as a coherent corporate resource, rather than relying on the vagaries of naming emerging from individual workgroups or sections, and will reflect the functional business nature of the department, rather than a more transient organisational structure. Responsibilities for creating and managing lower level sub-directory structures should be clearly assigned, where this ability is devolved to teams or branches, to ensure consistent use of the terminology.

3.6 It may not be appropriate simply to automate a method of organising and filing which has evolved from use with paper records; the nature of electronic records may make certain aspects no longer relevant, whilst others will assume a greater importance. In particular, where faults have been identified in a paper record keeping system, the introduction of electronic record-keeping offers the opportunity to reconsider methods and mechanisms.

The method of organisation used should:

- provide a hospitable and extensible framework for adding new records
- enable management of records at folder level or higher
- be flexible in direct access to content and provide browsing facilities
- be consistent with, and capable of mapping to, the paper filing system
- reflect business needs and usage.

### Managing versions and auditing actions

3.7 To remain an authentic representation of events, once declared as a record, a document should not be capable of being changed. Since electronic information is more vulnerable to accidental or deliberate editing, without leaving any traceable evidence within in its own content, record-keeping systems must take special measures to prevent retrospective change to corporate records and to record other significant actions taken on them.

3.8 The degree to which a particular document can be revised and re-versioned before being filed as a record should be a matter for corporate procedures and user guidance. After a document is stabilised as a record, the ability to edit and make changes to the document should be prevented, as far as is possible within the available technology; the degree to which the authenticity of a record can be demonstrated for legal and accountability purposes will be largely determined by the success of these restrictions. Where it may be necessary to gain update access to maintain the record, to edit the metadata, and take any other action which will modify an attribute of the record, pre-determined procedures and roles should be adhered to and fully documented.

3.9 New and related versions of the record can be created by making and editing a copy, and saving this as a new record; for example, it may be appropriate to retain various versions of a document as it passes through draft to finalisation. The record-keeping system should be capable of linking together versions of the same record, either automatically by the system or through the use of strict naming conventions, to ensure that the latest version is retrieved by a user search. The user should be aware that earlier versions of the record exist in the system.

3.10 An audit trail should be kept recording significant actions which have been taken on a record, including the date of the action and identification of the individual responsible. Actions taken should include:

- any changes which affect the status of the document as a reliable record
- any change to the metadata, or profile, describing the record
- copies made of the record to create a new version.

Although it may be possible in some record-keeping systems to track all activities relating to the record, including all read and retrieval access, it may not be sensible to do so in all cases. Records managers and systems designers should give careful thought to the extent which this information will be useful and the long term use which will be made of accumulating such detailed data; it may be appropriate to restrict this ability of electronic systems only to certain categories of record, or to certain groups of users.

Retention and disposition  
schedules

3.11 The responsibility for maintaining and managing electronic records must be placed with managers with appropriate expertise and authority who will ensure that electronic records of continuing value are actively managed during their operational lifetime in accordance with these guidelines. The DRO must make these managers aware of their responsibilities under the Public Records Acts by liaising with them on a regular basis to develop procedures which will ensure compliance with these guidelines.

3.12 Corporate procedures will be most effective in a networked environment, where shared networked servers and disk drives can be used for all official business, and adherence to departmental procedures can be more easily assessed. It is much more difficult to assess compliance in cases where users hold definitive copies of documents in electronic form on local PCs. The DRO should review and dispose of such records on a regular basis, in conjunction with users and according to the approved disposition schedule.

3.13 Where the disposition scheduling is embedded into a record-keeping system, records managers should check regularly that the necessary procedures are up-to-date, known about, and are being followed. All electronic records for which the useful life can be pre-determined should be given fixed retention or disposal periods, with instructions for their disposal held as an element within the metadata, and managed at the file/folder level. Users of these records should be made aware that by adding a record to such a group, they are making retention and disposal decisions. No document of long term value should be added to collections which do not have the appropriate scheduling; the DRO should be alerted in cases where it may be necessary to vary the disposal status of the record group due to a change in use or organisation.

3.14 Retention and disposal schedules for electronic records should be consistent with those for paper records, and as far as possible applied throughout the organisation, where storage may be distributed across several different physical sites. Similarly, records managers should attempt to identify

secondary, or working, copies of electronic records which have also been scheduled as primary copies and apply the appropriate disposal decisions; user guidance should be provided on the treatment of electronic documents which have been printed to paper and filed as a paper record.

3.15 As with paper files, where a series has an unlimited lifespan, some form of chronological segmentation within record series may be necessary to permit the treatment of records in whole blocks for disposal or transfer. This can be achieved by, for example: dividing record blocks into annual groupings by closing the folder to which new records within a series are added regularly on an annual basis; or simply by allocating a formal structured date field to the document attributes which enables segmentation of records by date range.

#### Hybrid assemblies

3.16 In many cases registered files of paper documents are likely to exist alongside electronic record folders where it is desirable to hold certain documentation in paper form – for example, incoming correspondence. In these circumstances the paper files will not duplicate the electronic folders but their content will augment the electronic version; together they combine to form hybrid assemblies.

3.17 Where hybrid assemblies are required it is important that the linking references identifying the two types of record maintain and display relevant relationships, so that the links between an electronic folder and its related paper file are clear to the users and easy to understand. Care must be taken to ensure that this relationship can be easily identified by both the creators and future users of the data, and that the accompanying metadata is maintained along with the electronic folder and records.

---

#### Access management, accountability and audit

3.18 In the electronic environment, records managers are unlikely to be the physical guardians of electronic records; these will be in the keeping of IT providers or personnel. Issues relating to the security of records, and control of access to them, will have to be re-thought, since this can no longer be achieved by keeping under lock and key or within a central Registry. Records managers will need to develop procedures which are more appropriate for this new environment. It may be appropriate for recommended users to have the ability to create new folders, review disposition settings, and monitor or quality assure system performance.

3.19 This will involve a cultural change for both record managers and IT providers. Traditionally records managers have controlled the storage of files

once they have ceased to be actively used. Where electronic records are involved this work will be undertaken by the IT provider; however, the role of the IT provider will also change as they will now require explicit authorisation from the records manager before any decision to delete records or modify management information is made. This new relationship will also have to be documented in an appropriate manner to facilitate audit.

3.20 The characteristics of the information security measures in place will determine the degree of trust which can credibly be lodged in the record-keeping process, to ensure that once declared as a record and captured within the corporate filestore, the content or context of original use cannot be amended in any way. The record is only able to demonstrate accountability to the extent that a trusted record-keeping process has been instituted and has gained reputation and acceptance. Because of their nature, electronic records are more vulnerable to challenge on this issue than their paper equivalent; one aspect of asserting intellectual control of records is to develop constraints in this area. This will be a particular problem in situations where records are kept in a loosely structured network environment with little or no control over types of access rights or audit trail reporting. Here, it will be necessary to develop procedures that document the activities in order to provide appropriate audit trails. Consideration should be given to creating an audit trail demonstrating compliance to *PD0008, A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically* as proposed in the *BSi Compliance Workbook, PD0009*.

3.21 The key characteristics of an effective approach to managing the security and access of records deal with issues of:

- *authentication* - assurance of the identity of an end user; that end users are in fact who they claim to be, that they are the true originators of records to which their names are attached
- *authorisation* – that a particular user is sanctioned for a particular function, for example, to be able to create a new version of record, or to alter the filing or retention decisions pertaining to a group of records
- *confidentiality* – ensuring that content access is granted to those who should have it, and not to those who should not
- *integrity* – evidence that the contents of the record, including metadata and format, have not been altered since the document was declared as a record, as a result of control procedures which would prevent this

- *non-repudiation of transmission* – protection against denial by an individual originating a communication which is stored as a record, as a consequence of assurance gained from the previous four characteristics
- *non-repudiation of receipt* – protection against denial by an individual in receipt of a record.

### Access management

3.22 Working documents which have not been declared as a formal corporate record may have access controls placed upon them by their current owners who wish to restrict availability of the document content for various reasons, assuming the policy of the department allows this. Once declared as a record the document comes under corporate ownership and is subject to corporate regulations and procedures. One vital feature of electronic records is their ability to open up access to this corporate information, providing a richer and more accessible information base for the conduct of departmental business. However, there will still be a need to restrict some forms of access to this material – for example, write access to prevent unauthorised changes being made to the existing record – and for certain categories of material (for instance, records with a protective marking) to restrict all forms of access to defined user groups.

3.23 The DRO or other records manager should aim to identify important user groups within the department, and allocate broad functional rights to each group. Relevant user groups might include:

- groups with access to higher levels of protectively marked records
- project teams or workgroups
- records managers who will manage record collections and metadata.

Functional rights which might be allocated in differing combinations to differing groups might include:

- read / retrieval access to metadata or other record descriptions
- read / retrieval access to records contents
- edit rights to change the content of metadata or record descriptions
- copy rights to make a physical copy of a record in order to create a new version
- records management rights to change any retention or scheduling information.

Wherever possible it should not be possible to edit a record contents, without creating a new version; similarly, delete rights (for records, rather than documents) should only be available to system administrators.

3.24 Most document management or electronic records management systems will provide facilities for systematising the allocation of rights in an access control table, and the attachment of these rights to individual documents or groups of documents. In a less structured environment such as Windows, it will be necessary to rely on less sophisticated facilities, such as the ability to mark word processing documents or Windows folders as read-only.

3.25 A digital signature is normally a form of alphanumeric key, which has a similar function to a cash card PIN number. A digitised signature is a digitised representation of an individual's own hand written signature. These signatures of either type should be "bound" to the document, meaning that once signed the document cannot be changed and that the signature cannot be copied elsewhere. Electronic authentication is a technology which is in the process of rapid development; there are a number of competing approaches based on cryptography, biometrics and combinations of the two. Both the UK government and the financial sector have been in discussions to agree a standard that can be used to support electronic commerce. The 1998 White Paper on Competitiveness has called for the establishment of an e-envoy post to further this dialogue, and initial proposals for a Secure Electronic Commerce Bill have been put forward.

3.26 Verification of a signature, confirming that the person signing the document is who they say they are, is not generally considered to be a requirement with respect to the legal validity of a signature under English law. Verification is a data security feature providing the recipient with credentials that the document received has not been changed during transmission, and that the signatory is in fact the person or organisation they claim to be. This is necessary in a networked environment, since the virtual nature of the medium removes the visual and geographical constraints which provide assurance in a transactional relationship based in the physical world. Authenticity of an organisation's information depends on the standard of information security that is established throughout the organisation. This affects the reliability of information that is processed and stored electronically and transferred over the communication networks.

3.27 Although the architecture which will support electronic commerce and electronic government in the UK has yet to be finalised, current recommendations are based on a form of public key infrastructure (PKI). There are essentially three elements to this infrastructure:

- a paired key architecture, using asymmetric encryption based on public and private keys

- the production of encoded digests of messages to ensure that any amendment of messages can be detected by the recipient
- certification services, provided by a third party, which issue certificates as credentials and can vouch for their identity when used – to verify the identity of the holder of the key in use.

3.28 The successful take-up of this architecture will depend on the existence of trusted Certification Authorities, able to establish the network of confidence and trust necessary to any system of business and social transactions. These services will be provided by entities known as Trusted Service Providers, commercial organisations used to working within a regulatory environment. The current approach within the UK, and that outlined in the European Directive on Digital Signatures, is to establish a voluntary licensing regime for Certification Authorities (CAs); digital signatures will have legal force, and those authenticated by a licensed CA are likely to have more robust legal recognition than those by an unlicensed CA. The criteria which will govern licensing, and the type of technology which will support these criteria, are currently the subject of debate.

3.29 Detailed guidance on the records implication of electronic signatures will depend on the outcome of the proposed legislation. Although at present, the use of this technology is largely limited to experimental systems, it is likely that once an infrastructure is firmly adopted take-up will be rapid. Records managers should become aware of applications which plan to use electronic signature technology, and aim to ensure that the records management implications in this important area are addressed by IT strategy planners.

3.30 To ensure access to records in the future, distinctions need to be made between applications which use electronic signatures but do not encrypt the content of the message, and those which use some form of encryption on the message in order to ensure confidentiality. In the latter case, the record will become inaccessible unless a decrypted version (or the means to obtain one) is available. In the former case, in appropriate circumstances, it may be sufficient to document that the digital signature has been correctly assigned and authenticated. From the point of view of the end user, the relevant actions which need to be taken (and can thereby be documented) are:

- identifying the certificate and key pair used to sign the document
- identifying to whom the document was sent
- verifying that the recipient validated the signature.

3.31 In environments where confidentiality is preserved by encryption or similar technologies, the records manager must:

- establish the principles by which accountability, integrity, authenticity, and compliance of information systems may be assured
- specify the role of risk assessment and risk management in the use of cryptographic techniques, data validation, back-up and recovery
- identify the relationships between authentication, security and audit
- understand the role of trusted third parties and certifying authorities
- ensure that authentication is taken into account when systems are specified, designed and developed.

3.32 Strategic direction for the development of technologies capable of supporting electronic government is the province of the CITU unit in the Cabinet Office who, in conjunction with the CCTA will be the authoritative voice on the technical and business IT aspects in this area. The Information and Document Management Association (IDMA) is also currently researching the subject and intends to publish guidance on the issue of authentication during 1999-2000.

#### Encryption

3.33 Encryption is likely to become an issue for records management in the following contexts:

- the use of secure connections across the Internet in citizen interactions
- the use of xGSI (the higher security version of the Government Secure Intranet) for secure communications within government itself
- the development of electronic commerce
- messages requiring privacy which are sent on non-secure media.

It is too early in the development of these applications to give definitive guidance; the Public Record Office will provide further guidance on the records management implications as the use of this technology develops.

3.34 However, a fundamental principle is that records stored within a record-keeping system must be capable of meaningful access in the future. Records which are stored only in their encrypted form will be vulnerable to loss, for all effective purposes, once the means of encryption changes or is replaced. This implies that records should be either:

- stored in a decrypted form, securely and with the appropriate access restrictions, for future sensitivity review and potential release or selection by the Public Record Office

- stored with guaranteed access to an historical archive of the means of decryption, which is systematically maintained in conjunction with the records over time; and with metadata which retains the link with the relevant generation of encryption tools and which locates the record within the corporate filing structure.

3.35 In some departments it will be necessary to establish procedures which enable the flow of information between more secure sections, such as the Private Office, that routinely deal with encrypted messages and documents and other parts of the department.

#### Legal admissibility

3.36 This is general guidance; it is not exhaustive, nor authoritative, and it will not provide all the detail required to address every problem. Where problems of interpretation arise departments are advised to seek advice from the relevant auditing authorities or legal counsel.

3.37 The Civil Evidence Act 1995, does not specify any special conditions governing the use of computer-derived evidence in court. However, in criminal proceedings, Section 69 of the Police and Criminal Evidence Act 1984 states that any statement produced by a computer will only be admitted into court subject to compliance with certain conditions. One of these conditions provides that “at all material times the computer was operating properly”.

3.38 It is recommended that organisations should seek to conform to the provisions of *PD0008 BSi A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (edition 2)*. Legal admissibility is significant if the organisation ever needs to use electronic records in legal disputes. Compliance with *PD0008* cannot assure evidential worth - ultimately this is for the courts to decide – however, non-compliance provides no mechanism to support arguments for evidential worth and without such mechanisms it will be difficult to satisfy the needs of audit. Here the questions to be borne in mind are:

- are the records complete?
- are they accurate?
- are they valid?

3.39 Audit trails should be provided for all information and documents. It is recommended that audit trails should be kept securely, and be available for inspection by authorised internal and external personnel. The trails should be capable of being easily followed by auditors who may not have experience of the technologies in use.

3.40 The Compliance Workbook for Legal Admissibility of Information Stored on Document Management Systems, PD 0009 is designed to establish the compliance of a document management system with PD 0008. It also enables an audit trail of compliance to be produced which must be stored on the records management application as a record held on the system. When completed, this workbook is the organisation's statement of the extent to which its records management complies with the recommendations in PD 0008.

Regulation and audit

3.2.5.1 Audits are required for statutory reasons and as part of an organisation's corporate control procedures. A system should be designed to be auditable and its auditability needs to be demonstrated to prove that it is effective and offers adequate control. It is a pre-requisite, which should be undertaken at an appropriate level and form.

3.41 The BSi report *PD0010 Principles of Good Practice for Information Management* recommends that audits should be carried out at intervals during the life cycles of:

*Documents and information*

- Creation
- Updates and changes
- Storage
- Retention
- Access
- Deletion or destruction

*Hardware and software*

- Specification
- Operation
- Procurement
- Modification
- Installation
- Maintenance
- Commissioning
- Decommissioning
- Testing

Records must be kept of all the hardware, storage media and software systems and applications used to implement an electronic records repository. On a regular basis, annually at most, this inventory must be evaluated against

industry developments to ensure remedial action can be taken in a timely and planned manner. It will be necessary to include contingency funding in annual budgets so that finance will not become an impediment to action.

3.42 When implementing the audit of information and the supporting technologies the following objectives should be addressed:

- to communicate the basic principles that underpin audit, and the audit of information technology systems to all relevant personnel
- to ensure that a successful audit addresses both the technology and the personnel
- to determine the position of audit points, the activities and the information to be audited
- to describe the nature of audits, the characteristics of any audit process and the audit procedures to be carried out
- to identify the roles, responsibilities and skills of the personnel required to deliver effective operational controls to systems.

The Information and Document Management Association (IDMA) and the National Audit Office are currently researching the need for auditing electronic document and records management applications. It is understood that detailed guidance on the subject of audit will be published during 1999-2000.

#### Audit Points

3.43 Audit or control points should be placed at relevant positions in the information and document flows. They may be triggered by particular activities or on the transfer of documents or information. The information which needs to be gathered and checked against specified criteria will include:

- the process being audited
- the documents and information being processed
- the date and time when information or documents pass through the audit point
- the person responsible for performing the work
- any other relevant comments
- the transmission and receipt logs.

3.44 The objective is to ensure that appropriate measures are employed to monitor and document operations and any deviations from designated standards and methods of operation. It is important that all of the procedures used to achieve long term preservation of electronic records are auditable. This means that procedures must be clearly defined and responsibility for their being carried out assigned. It is possible that some existing approaches could be used e.g. total quality management or the ISO 9000 standard.

---

**Managing e-mail as records**

3.45 For most departments at the present time, e-mail represents the most difficult challenge in gaining control of electronic records. It is now a standard element in organisational office systems, and is widely used for the conduct of official business. Used initially in an informal manner for largely ephemeral content, e-mail messages have now become a primary means of communicating formal information, commenting on documents, and making decisions. As such, they are potentially important electronic records, which may have significant content; however, they are little controlled as corporate records, and have a poorly defined internal information structure.

3.46 The DRO must ensure that policies and procedures for managing and storing e-mail are developed and widely publicised. E-mails as electronic records should be managed as part of corporate information resources, with accountability and legal implications, and be retrievable and accessible subject to the organisation's security and sensitivity rules. Electronic messages should be captured and maintained as functioning records. To be available for future access, e-mail messages require their structure, content and context to be preserved as with any other record; to maintain their value as evidence, they must be safeguarded against alterations.

3.47 E-mail messages should be filed as records in the same way as other electronic records with a common use of procedures and decision rules in identifying formal records; whether these are filed in an electronic system, printed to paper, or dealt with in some other way according to established procedures. If the original record is copied to another form, whether as paper or in a formal record-keeping system, then the conditions under which the original record can be deleted should be clearly established. In general, the sender of a message generated from within, and the recipient of a message received from outside, the organisation should be responsible for filing the e-mail as a record. Where messages or attachments relate to joint working projects, there should be a clear understanding of responsibilities in retaining and scheduling the records, and a consistency in their application.

3.48 To preserve its full meaning, the e-mail record itself should include, or be linked to, metadata that describes the context in which the message was created and received, including: subject line, date and time sent, originator and recipients. The department may also retain audit logs of e-mail server traffic for security purposes; if so, these will form a different record that should be separately scheduled according to departmental policy. Document attachments, of whatever nature, should be treated as one component of the e-mail record

along with the textual element of the main message. It will be important to retain the link between message and attachment so that retrieval of one will lead to retrieval of the other; this may be achieved automatically in some record-keeping systems, or purposively on the part of the user by following an explicit link.

3.49 Clear guidance should be provided to users to assist in choosing to save an e-mail as a formal record. An individual e-mail will often need to be interpreted in the context of others when it is part of a larger dialogue or exchange; therefore, an important e-mail should be accompanied by supporting messages which allow it to be seen in its overall setting.

3.50 Records managers should consider, from a records point of view, whether or in what circumstances particular categories of e-mail should include a digital signature, or other means of electronic authentication. Where an authentication mechanism has been used and verified, the verification should be recorded as part of an audit process and this assurance should be included with any eventual transfer of material to the Public Record Office. Records managers should also ensure that e-mail records which have been encrypted for transmission on xGSI (the more secure form of the GSI network, across which classified material protectively marked up to Confidential can be transmitted), or for some other reason, are not held as a primary record in an encrypted form unless necessary for security reasons. Where this is necessary, the means for decryption (in the form of software which can be applied to the message) should be retained to ensure that encrypted e-mail records can be rendered accessible when the record is re-allocated to a lower security classification, and that when transferred to the Public Record Office it can be correctly interpreted. Particular consideration will need to be given to this issue at the time of migration, and of upgrading and replacement of secure e-mail systems.

Mailbox management for good record-keeping

3.51 The method by which e-mails can be best be safeguarded will vary according to the size and type of the office system in use. Record managers should consult with their IT branches to identify and evolve the most appropriate process for their own department. Where an integrated electronic document and record management application has been introduced users can routinely save a copy of messages into the corporate system, where these can then be managed in the same way as all the other electronic records. Even in these circumstances, however, attention will have to be paid to user mailbox management, to ensure that sensible and coherent choices are made about saving and destroying both primary and secondary message copies. In many

circumstances, at the present time, safeguarding e-mail will depend upon instilling effective mailbox management and e-mail etiquette in the user community.

3.52 In most cases, records managers should work with IT branches to develop clear and consistent user guidance on e-mail management to encourage the self-disciplined information management which will produce a higher level of quality and reliability in the records that are generated and stored. In doing so, consideration should be given to producing guidance on:

- the potential for marking individual messages with type indicators, in a specific field or as part of the envelope data, flagging their purpose and relative long-term importance, and the way in which these should be applied by users
- the procedures which the user community should follow in archiving from their personal mailbox to permanent storage at regular intervals
- the policy which is followed by an IT branch in managing overall mailbox storage space, and the frequency and warning with which 'clear-out' practices are carried out
- the procedures for copying messages to a record-keeping system, and subsequent deletion of the original
- recommended e-mail etiquette and good practice in creating and replying to messages, drawing on that produced by CITU and other relevant bodies.

3.53 The production of specific guidance on the construction, content and use of e-mail messages will be a useful method for encouraging good practice in managing messages as potential records. This is, in any case, desirable for effective management of current information; good practice here aids both day-to-day operations and the medium to long term requirements of records management.

Consideration should be given to the following:

- the use of available indicators to show message type
- where relevant, the use of file numbers or other means of reference, to show the body of records to which the message relates
- the disciplined use of subject lines which clearly indicate the content of the message, and the consistent use of the same subject line in a sequence of messages which relate each to the other
- encouraging the categorising of discrete topics into separate messages rather than encapsulating several topics under the same heading, and discouraging the undisciplined use of subject lines where the content of the message has drifted away from the original topic

- restricting an over-use of the mechanism by which earlier text is included when replying, potentially over many generations through the thematic strand, to prevent excessive message length; in conjunction with clear guidance on the frequency at which a record copy of the contents of an e-mail dialogue should be made.

---

**Managing records on websites, Intranets and the GSI**

3.54 The effective control of Website and Intranet records will be an important challenge for electronic records management in the short to medium term future. Discrete electronic documents that are produced by word processor and spreadsheet applications can be seen as a form of ‘electronic paper’, to which the management concepts and mechanisms that work for conventional paper records can be applied with some re-working. In an Internet/Intranet environment, change in the nature of the information and the way in which it is used accumulates to a degree such as to force a re-thinking of these basic concepts and mechanisms. This is due to changes in the boundaries defining:

- the *type of record* – a dynamic hypertext and multimedia document behaves quite differently to the static, linear document produced by a word processor; and does not necessarily have a clear beginning and end point
- the *purpose* for which the record is used – firm distinctions between a record, a document and a publication become less clear; and the boundaries between the personal desktop, the local network space, the departmental website, and the wider network landscape become blurred
- the *process* from which the record emerges – the increased exchange and sharing which the network environment encourages, enables a re-shaping of business processes that are no longer bound by physical and geographical constraints; and will demand from records managers a level of co-ordination between as well as within departments.

These guidelines represent only a first step in developing approaches and procedures in this area, and will need to be further refined as the implications for records management emerge.

3.55 However, this is an area in which development is likely to be rapid: the growth in electronic government will increase the importance of websites as a channel for communication with the citizen. This will be a two-way communication, allowing both the delivery of information published by departments, and the ability of the citizen to communicate electronically with the department via interactive websites. Many departments are developing their own Intranets, developing electronic information in ways which are less like the familiar paper formats; and the Government Secure Intranet (GSI) will increasingly shape the electronic interaction between departments and their records.

---

**Internet Website and  
Intranet records**

3.56 The proliferation of Internet websites are an important area in which to determine the records management implications for three reasons:

- the possibility that material that exists on the website does not have an equivalent and accessible paper copy; observation of practice in other national governments indicates this is increasingly the case
- the implications for departmental accountability of material which is externally available on a website, but which has not been subject to records management procedures; and therefore the need to know what has been made available and when
- the need to preserve completeness and context with the record content (as it was made available to the user) requires the retention of the website document in its electronic form – with hypertext links – and knowledge of its position within the structure of the site itself.

A website may contain significant material, which could influence the actions or choices of an individual viewing the information. Even though the material may have been prepared from word processed documents, there may be no exact equivalent as it appears on the network, and no effective version control of changes and updates. It may be difficult, or impossible, to reconstruct the view that a website visitor had of the material at a particular time, unless some form of co-ordinated management controls are evolved.

3.57 A useful model, which has been used in parts of the United States government, is to integrate records management as one of the processes undergone by information products which are produced by the department (others would include checking for legal liability, and assessing copyright, for example), as they pass from those responsible for producing the information content to those responsible for its dissemination – electronic publication on a website being one form of dissemination amongst other possibilities.

3.58 Responsibilities for records management in relation to websites and Intranets should be allocated between three roles:

- *website (or Intranet) managers*, who should ensure that material with records potential can be captured and transferred to a record-keeping system in a format suitable for preservation, accompanied by appropriate metadata and contextual information
- *content providers*, responsible for identifying material, and versions of the material, that should be kept as a record and enabling its transfer to a record-keeping system

- **records managers**, responsible for liaising with the other two roles to establish retention and disposal schedules for records and providing appropriate mechanisms for taking a record copy.

Records managers should endeavour to raise awareness of the accountability implications for Internet websites, and contribute to the establishment of overall organisational management structures for control of website and Intranet material.

3.59 Intranets and Internet websites may produce two types of record:

- **prepared materials**, produced by content providers for posting onto the website, which may update existing material and require close version control
- **interactive communications** (e-mails, completed html forms) received from visitors to a website, commenting on material posted, contributing to an online discussion, or asking for information.

3.60 Both of these types may need to be retained as a record copy. Records managers should aim to identify categories of material which should be kept as records for accountability or business reasons, and which are not already captured as records in the same form through other channels. These records should be included in strategic appraisal plans, preferably with initial appraisal conducted at the time of creation by the content provider and records manager, and allocated a retention and disposition. Disposition will depend on the nature of the information contained in the record, its potential long term interest, the degree of change in new versions or updates, and the importance to the organisation in accountability terms. Appraisal and disposition should be consistent with other forms of electronic and conventional records.

3.61 An Internet website raises a problematic records management issue similar to that posed by a database - does the website contain records amongst the material which it publishes, or is the entire website a record in itself? Departments may wish to choose between these alternative views depending on the nature and importance of the material which is held on the site. In the first case, it will be appropriate to retain copies of those elements of the site deemed to have the status of records and place them in a record-keeping system with relevant metadata; in the second case, it may be more appropriate to take regular snapshots of the entire site as it exists at regular intervals – daily, weekly, or monthly. The frequency of these intervals will depend on the rate of change in the information content, and the risk and accountability exposure entailed in not being able to reconstruct the state of the site at any given point.

3.62 Whichever of the approaches is chosen, the physical boundaries of the record to be captured will have to be clearly defined, and applied to the format which the material takes. While some documents are simply versions of familiar linear formats, the nature of website and Intranet interaction tends to encourage greater use of a hypertext format, enabling the user to traverse links between parts of the document itself and to other related documents. In most cases, it will probably be appropriate to confine record capture to those elements of the document which are held in the same site (and, usually, which have not been captured as part of another record). However, consideration should be given towards documenting the existence and purpose of uncaptured links, either in accompanying metadata or embedded within the document source itself.

3.63 As a minimum, records managers should aim to develop a historical log listing postings of significant material, which acts as a simple level of metadata. Elements to be considered for inclusion are:

- title of the posting, and its version number
- hyperlinks in the posting, and their purpose
- content provider, or another originator
- dates of posting, modification and replacement
- retention and disposal.

Government Secure  
Intranet

3.64 The Government Secure Intranet (GSI) is emerging as an underpinning technology in the business of government and the delivery of government services. Although the GSI is at a relatively early stage in its operational development, prompt take-up of the service is being encouraged and a rapid development of services is likely. Many, or most, of these services will involve electronic records, and the new networking environment will radically influence the way in which office systems, databases and record-keeping systems are designed and implemented. The shift to working more within a networked environment, in conjunction with general trends in the development of office software systems, and a greater emphasis on the strategic use of information to provide efficiency and effectiveness benefits, will tend to blur previously discrete boundaries between record-keeping systems. This will support greater collaboration and joint working between government departments and agencies, and will have implications for the way in which the Public Record Office works with departments on the maintenance, selection and transfer of electronic records.

3.65 At this early stage in the take-up of the GSI it is difficult to predict the exact direction in which use of the network will develop. Current uses of GSI largely focus on e-mail services, access to external information services and Internet facilities. These, and the other more far reaching developments which will follow on, will require the development and revision of policies and procedures to take account of this new environment. These should ensure that adequate records are physically captured and maintained, and that the value of this information as records (which stems from ensuring their integrity and authenticity) is sustained in these circumstances of greater access and fluidity.

3.66 The extension of internal e-mail systems to include GSI mail, and their interfacing with existing office systems and work arrangements, may provide an opportunity for records managers to establish the more stringent information management disciplines which records management requires, where these are not already in place in the organisation. This can involve both the review and development of existing policies and procedures relating to records and may also present an opportunity to influence the design and implementation of new information systems and the incorporation of record-keeping functional requirements into new systems specifications. The procedures discussed for Internet websites and Intranets should also be adapted for the GSI environment, where the restriction of the network to government organisations makes it likely that a greater proportion of relevant record material will be generated.

3.67 The emergence of the GSI reinforces the need to build and retain a sound logical structure and organisation for the keeping and use of records. New networked applications will increase the sharing and exchange of records within and between departments, and will require a clear understanding about the allocation of responsibilities for managing identified records collections, and the individual records within collections. This will be particularly important in a situation in which a user at the desktop may be unaware of the physical location of a document, at the same time as having a greater ability to access and amend remote information directly. There will be a greater need to maintain a clear and consistent intellectual organisation and structure to collections of records both within and between departments, to ensure not only efficient access to information, but also the context of record creation and use within such a dynamic environment.

3.68 Conventionally, management of record collections has reflected business processes that have been located more or less within discrete departments;

indexing and filing structures have also mirrored this arrangement. With more fluidity in information and record flows, and with the ability to present citizen-focused 'virtual' processes that might involve a number of different agencies or departments, a record collection may be held across several different physical organisations and locations. In these circumstances, a consistent approach to the way in which the content of records are organised, managed and retrieved will be vital for effective records management. Policies and procedures should be developed for dealing with records which emerge from joint projects and joint working arrangements. Where joint working or potential shared systems are under consideration, attention should be given to the control of records within a collaborative system:

- where several departments contribute a copy of material held as records in their own internal systems
- where this material can be updated in the collaborative system
- and in a shared operational system, such as a shared database, where departments do not hold their own primary record copy.

---

**Review of systems related to electronic records**

3.69 The aim of a systems review is to:

- identify and review existing electronic record-creating and record-keeping practices
- measure their performance against the requirements for electronic records which have been derived from business needs
- detect particular problem areas in which performance does not meet requirements.

Systems which produce significant electronic records in the department should be reviewed at regular intervals, appropriate to the rate of technical change, to check that the way the system is being used, and the kind of records it is producing, has not changed significantly.

3.70 Essentially, the systems review is aiming to assess compliance with the records management procedures and requirements within the department. A review of record-creating systems can look at a number of aspects of compliance:

- are appropriate records being created in the first place?
- are the records which are being created adequate for their purposes?
- are end users filing records correctly?
- do record-keep systems handle electronic records appropriately?

3.71 The inventory (see section 4) and system review can be used together as a basis for checking compliance with established procedures and standards, by identifying those record collections to which particular standards or procedures should apply, and then examining actual system practice. This will identify those areas in which immediate or medium-term action should be taken to ensure the continued quality of record-keeping, and will provide background information to aid the appraisal process.

3.72 Analysis of these sources of information will help to identify priority areas where action is more urgently needed, and with developing an overall strategy to deal with them. Resource estimates should be used to prepare a plan for dealing with problematic areas and a timetable for action. This should be co-ordinated with the information strategy of the department, and with other specific programme or work areas. For example, a Year 2000 compliance programme will demand DRO involvement in the migration plan in order to contribute an assessment of the relative value of records which are affected; and may well offer opportunities to influence the specification of modifications or of new replacement systems.

3.73 Actions on problem areas may take one of three main forms:

- dealing with immediate problems or suggesting modifications to existing systems or processes
- influencing the design of new and replacement systems
- adopting policies and standards, contributing to corporate thinking on information architectures and strategies, and influencing information behaviour by end users.

#### Maintaining awareness

3.74 The DRO should aim to maintain a general awareness about the implications of any changes in organisational structure and business policy, information technology systems, PRO acquisition policies, or the legal and operational requirements of the department, in order to identify any changes in record-keeping requirements that should apply to existing systems. A general awareness of systems development plans and developments may enable the DRO to contribute the requirements for electronic records management to new systems design at the systems planning and design stage, so that facilities for record capture, record keeping, appraisal and preservation are built into systems wherever possible.



## 4 : Inventory, appraisal and disposal

4.1 This section deals with:

- the development of an inventory of records (rather than systems)
- the range of information about records which the inventory can maintain
- planning an appraisal strategy for electronic records
- building appraisal mechanisms into systems design
- disposal of electronic records.

---

### Developing an inventory : knowing what records exist

4.2 The department should be aware of the full range of records for which it is responsible, and be able to locate and retrieve those records as necessary. An information and records audit aims to identify and describe the record collections which exist, at an appropriate level of detail. The detail of the audit will vary according to particular demands, concentrating on broader or narrower collections, as long as the level is consistent across the field, and the appropriate information about record collections is collected. DROs should aim to build up and maintain a comprehensive inventory of their electronic record holdings for future use, even though the present policy may be to 'print to paper'.

### Purpose of the inventory

4.3 The inventory of record collections is a primary tool for electronic records management within the department, comprehensively listing the records which the organisation holds and providing a basis for both physical and intellectual management decisions. It is not intended that the inventory be passed to the Public Record Office; it should remain with the records management function of the department and be regularly updated and maintained. The inventory will form a useful point of liaison between the DRO and the relevant Client Manager, in making decisions on management, selection and transfer. The inventory should aim to be comprehensive and consistent in its coverage of electronic records within the department. Since the inventory is a central records management tool, it is concerned with all electronic records (of whatever type), and not simply with those that may in time be transferred to the Public Record Office.

4.4 The inventory is not a list of application systems; instead it should aim to gather information about each identified collection of records. In some cases, the record assembly or collection may be functionally equivalent to an individual computer system – for example, with some larger databases. For less structured records there will not be such a clear correspondence between the two – for example, the same office applications will produce records grouped in

many different business areas. The inventory should systematically list elements about each collection, such as:

- the business functions that the records represent
- the groups who create, use and manage the records
- retention, scheduling, disposal decisions
- classification/filing, access modes, protective markings
- physical software, hardware and media characteristics.

4.5 This should, as far as possible, include the electronic source record from which an electronic or paper record filed elsewhere is derived. If the originally created record is copied to an electronic record-keeping system or printed to paper, and the copy is regarded as the primary record, the original source record collections should be included in the inventory so that the conditions on which they can be destroyed are clearly established. Although it may not be practical to establish this level of coverage immediately, DROs should aim to achieve this position by extension and update over time.

4.6 When the results of an audit are used to build up an inventory of record collections, this can be used as a reference tool in case of system change and migration, policy change in information management strategy, organisational or business change, or changes in the legal and regulatory environment. The inventory should concentrate on logical collections of records grouped by business function or subject matter, rather than by physical location. However, the audit is a systematic approach towards mapping record groups against both business functions and physical systems and provides the link between the two views. This enables the identification of record-keeping requirements which should apply to particular IT systems as well as helping with consistency of appraisal between records held in different technical systems (for example, between paper and electronic records).

How can DROs develop an inventory of records?

4.7 An inventory of record collections is not the same as an inventory of application systems. A general purpose office system will be capable of generating many logical collections of records, each relating to a different function or topic area; and one record grouping may contain records from more than one software application. The systems review process can be linked to information about the records collections contained in the inventory to enable a clear connection between physical computer systems and logical groupings of records in a corporate classification / filing scheme. The information about record collections in an inventory should contain a link to the physical system(s) in which the records are located.

4.8 Wherever possible, the DRO should have available a portfolio of current systems, together with business cases and project initiation documents which identify the business functions and activities to which each system relates. The DRO should be aware of the purpose and business uses of these systems, and of any changes which might threaten the continued viability of electronic records. The DRO should also have the opportunity to actively contribute a records management perspective to the development of the information systems strategy for the department.

4.9 Work which is being done by an IT department on the maintenance of application systems inventories can usefully be drawn upon. DROs can be confident that such an inventory is already in existence in some form; this has been required by each department for Year 2000 compliance work for some time. The DRO does not need to duplicate this work on application system inventories, but should be sure to gain access to the results. This will enable the identification and grouping together of record collections which require action to be taken over the coming months.

Which records should be included?

4.10 All electronic records which the department is thought to hold should be included in the inventory of record collections. This includes:

- records collections whether or not they have previously been of interest to the PRO in paper or electronic form
- electronic records which are normally printed to paper and held in a paper record-keeping system
- records which are held in a separate electronic record-keeping system
- source records which have been copied to a separate electronic record-keeping system.

All these are examples of electronic records where consideration should be given, at the appropriate time, to their safekeeping, disposal or transfer to the PRO. Although the outcome will be different for different records collections, good records management should ensure that appropriate scheduling is applied in each case. In cases of doubt, the department's Client Manager at the PRO should be consulted.

4.11 A sample inventory form is shown in figure 4.1; the DRO should adapt the inventory form to include fields which would be of particular special interest, or to exclude fields which are not relevant or which do not vary between collections, to fit the local situation. However, the fields suggested in the sample form here are given as an example of good practice in conducting an audit of

records collections, and are likely to prove useful for future activities such as appraisal planning or determining the impact of changes planned for existing information systems. DROs should carefully consider the particular elements of information which should be included in planning the inventory: even though some elements may not be used immediately, it may be more sensible to collect them at the same time while there is an opportunity, rather than with more difficulty later.

4.12 The term *record collection* is used to indicate a grouping of records with similar characteristics that can be managed together as a whole group. The management of a record collection will include making decisions for the group as a whole on filing or indexing, on scheduling and selection, and on requirements for migration and preservation. A sensible grouping of electronic records will vary enormously between departments operating under different technological conditions and arrangements, and there is little stable terminology in this area. However, it is most important to be careful in thinking through how the term is used and to apply the definition in a consistent and predictable manner.

4.13 Although the physical form that record collections can take are various, a fundamental goal in establishing electronic records management is to ensure that they are held within a managed electronic environment and are subject to appropriate controls; and where this is not the case, that every effort is made to bring them within one. A managed electronic records environment exists when records can be organised and indexed (by whatever mechanism) for management and retrieval in logical groups which reflect the context of creation and use.

4.14 The inventory should make particular efforts to include all varieties of office systems within its scope, including those office records which have not yet been brought within a managed environment. In many cases, these may be the most vulnerable to loss during Year 2000 conversion, and this opportunity should be taken to gain a closer control of the situation.

---

**The sample inventory form**

4.15 The inventory of electronic record collections is intended to be a tool for records managers to:

- ***identify*** collections of electronic records so that they can be managed effectively
- ***locate*** collections of electronic records within a managed environment, so that they can be physically accessed, organised and intellectually controlled

- *relate* electronic records to departmental functions and to business systems architecture
- *audit* existing electronic records for compliance with Year 2000 plans and the corporate electronic records policy
- *assist* with the planning of an appraisal strategy.

The sample inventory form in figure 4.1 indicates fields which can be used to support these activities.

4.16 The construction and maintenance of an inventory of this nature should, wherever possible, be seen as a corporate responsibility, in pursuit of which the DRO will take a leading role supported by other information professionals. Setting the building and maintenance of an inventory as a goal in corporate electronic record and electronic document policy will help to build this corporate responsibility. The inventory will be important not only for records management but also as a tool for managing data protection and freedom of information processes. The department should seek to build alliances between records managers, information managers and information systems specialists in order to co-ordinate organisational responsibilities for the management of information – ideally, by bringing all these roles together under the same organisational umbrella.

4.17 An assembly or collection of electronic records is a group of records which are related in some meaningful way, and which have been purposefully brought together within a managed environment. While not definitive, some examples are :

- a named *Windows folder*, (which may itself contain sub-folders) containing electronic documents such as word processed texts, spreadsheets, presentations and e-mails that are related to each other in some way, and which is part of an organised structure of Windows folders on a local area network
- a *'virtual' folder* of similar documents (or pointers to documents) within an electronic document management system, which is part of an organised schema of virtual folders, and may contain subsidiary folders
- a set of electronic documents (in a broad sense) which share a *common file reference*, where this is a searchable element of the document metadata and is part of a wider file referencing scheme or corporate file plan
- a set of documents which have been indexed under the same *heading or thesaurus term*, where the heading or term has been selected from a predetermined and consistent listing, and can be used predictably within a search strategy to retrieve all records allocated to this term

- a collection of *interlinked hypertext documents* on an Intranet, which might include text, image, sound or video, and which are viewed as a logical group even though located in different physical storage.

4.18 A set of electronic documents which is brought together simply by use of search mechanisms working on the contents or uncontrolled indexing of a document collection, does not form an organised assembly of electronic records. By its nature, this mechanism cannot be used to ensure complete recall of all, and only, those records which are relevant.

4.19 Where electronic records are found to exist within an unorganised or unmanaged environment, they should be noted in the inventory as far as possible, and arrangements made to bring them into the managed environment. An unmanaged environment might be:

- documents residing in general purpose folders on a network drive, that have no discernible intellectual organisation or method of arrangement
- documents placed in folders on the local hard drive of an individual or workgroup, where the organisation is not meaningful to others or does not relate in an understandable way to some corporate-wide scheme.

4.20 A hybrid assembly of records may contain both electronic and paper records, and should be recorded in the electronic records inventory noting a link which can be used to identify the paper elements of the assembly.

4.21 Where a system holds a large number of record collections, and these are held in a very similar way, it will be sufficient for the “first cut” initial inventory to document the most important records collections in the first instance, or at a broad level of detail.

<b>Record collection name</b>		<b>Record collection ID number</b>	
<b>Which group(s) of people create records in this assembly or collection?</b>			
<b>Which business function uses these records?</b>			
<b>Dates:</b>	First date/Open date	Last date/Close date	Cut Off date
<b>File reference in corporate file plan, folder path, or other organising reference:</b>			
<b>Reference linking to paper file:</b> (for hybrid paper/electronic collections)			
<b>Who manages records in this assembly?</b>		<b>Which systems physically store these records?</b>	
<b>Subject terms</b>			
<b>Description</b>			
<b>Access constraints</b>		<b>Security protective marking</b>	
<b>Systems which generate records (applications systems which create records for this group)</b>			
System name (s)/ID (s)		Year 2000 compliant?	Actions?
<b>Records output (data transferred to other records collections / systems, or printed to paper file)</b>			
Data transferred		To: (system/data store)	
Printed to paper		To: (file reference)	
<b>Records input</b> (records transferred from other systems, or scanned from paper)			
<b>Scheduling:</b>	<b>Do records have potential archival value:</b>	Yes / No / Pending	
<b>Retention period</b>		<b>Disposition</b>	

Figure 4.1 : Sample inventory form for record collections

Description of elements  
within the inventory

**4.22 Record collection/record collection name**

*Content:* Name by which the assembly can be commonly identified, such as a folder name, file reference heading, subject heading, or database name.

*Purpose:* To make a ready identification of the record collection.

**4.23 Record collection ID number**

*Content:* If available, control number or other allocated identification.

*Purpose:* To make a unique identification of the record collection.

**4.24 Which group(s) of people create records in this collection or assembly?**

*Content:* The workgroup, section, or other end-users who create the records in the course of their work; this may or may not be the same group which uses the records for business purposes.

*Purpose:* To assist mapping of the record collection onto the functional and organisational structure of the organisation, and identify responsibilities for creation and capture of records.

**4.25 Which business function uses these records?**

*Content:* The business unit, or function, which requires the records for its own business purposes, and determines the length of time they need to be retained for accountability, legal and operational reasons. Secondary business functions which also make formal use of the records should be noted here also.

*Purpose:* To assist mapping of the record collection onto the functional and organisational structure of the organisation, and identify responsibilities for determining business requirements for the records.

**4.26 Open date**

*Content:* The date on which the record collection (or file, folder) was opened, or the date from the earliest dated document which it contains.

*Purpose:* To determine the date range of a record collection.

**4.27 Close date**

*Content:* The date on which the record collection was deemed closed.

*Purpose:* To determine the date range of a record collection.

**4.28 Cut-off date**

*Content:* The regular date used to separate parts of a continuing record collection for management purposes (e.g. the end of the financial year).

*Purpose:* To systematically determine parts of a record collection for management and processing.

#### 4.29 *File reference in corporate fileplan or folder path*

*Content:* A file reference label, which locates the record collection within a corporate filing structure, or the folder to sub-folder pathway which physically locates a collection within a computer system.

*Purpose:* To assist mapping of the record collection onto the organised filing structure of the organisation, in relation to other record collections.

#### 4.30 *Link to paper file*

*Content:* Reference or other identifying link to parts of the record collection which are held in paper form, for record collections which are partially held in both forms.

*Purpose:* To identify paper material which constitutes part of this record collection.

#### 4.31 *Who manages records in this assembly?*

*Content:* Identification of the organisational unit responsible for physical management of the record collection (e.g. an IT section) and contact information.

*Purpose:* To identify responsibilities for the physical safekeeping and preservation of the record collection.

#### 4.32 *Which system physically stores these records?*

*Content:* Identifying current physical location of the record collection, e.g. computer system on which held, data archive storage, network location.

*Purpose:* To enable location of record collection.

#### 4.33 *Subject terms*

*Content:* Any subject terms from a controlled vocabulary or thesaurus used, or uncontrolled keywords, which have been allocated to this collection as a whole.

*Purpose:* To locate the record collection within a subject hierarchy.

#### 4.34 *Description*

*Content:* Brief description of the record collection, showing role and purpose of the assembly not captured elsewhere in the inventory entry, and any other important intellectual or physical characteristics.

*Purpose:* To include any further necessary information to distinguish the nature of the record collection, at a broad level.

#### 4.35 *Access constraints*

*Content:* Any restrictions on use of the records (e.g. under data protection), access constraints on user groups, exemptions, etc.

*Purpose:* To determine access rules which apply.

#### 4.36 *Security protective marking*

*Content:* Security marking given to entire record collection, or identification that a security marking applies to elements of the assembly.

*Purpose:* To determine access rules which apply.

#### 4.37 *Application systems which generate these records*

*Content:* System names, or other identifications, of the applications systems (hardware and software) in which records are created for this assembly (either directly by an end-user or by extraction from a larger set of electronic information), together with an indication of whether each of these are Year 2000 compliant (taken from a system audit, and in conjunction with IT departments), and any action that is required to deal with those that are not.

*Purpose:* To enable a system audit, and Year 2000 compliance plan, and to map system inputs into this assembly.

#### 4.38 *Records transferred*

*Content:* Identification of other record collections into which records from this assembly are copied or moved (e.g. extraction of a subset of records into a decision support system for additional manipulation or processing) to form an identifiably separate set of records which have an existence of their own.

*Purpose:* To map outputs from this record collection.

#### 4.39 *Printed to paper*

*Content:* Identification of any paper files in which records from this record collection are filed when printed to paper, and an indication of which record set is formally regarded as the primary record collection.

*Purpose:* To map outputs from this assembly to paper files.

#### 4.40 *Records inputs*

*Content:* Identification of other record collections from which records in this assembly are copied or moved – e.g. the larger collections of which this is a subset.

*Purpose:* To map inputs into this record collection

#### 4.41 *Potential archive value*

*Content:* Indication of whether this record collection should be considered for permanent preservation by the Public Record Office.

*Purpose:* To identify collections of interest to the PRO.

#### 4.42 *Retention period*

*Content:* Scheduling information on time periods and event conditions of retention for this record collection, within the department or agency.

*Purpose:* To enable systematic scheduling of electronic record collections.

#### 4.43 *Disposition*

*Content:* Scheduling information on characteristics and conditions of disposal for this assembly, including potential transfer to the PRO or to UKNDAD.

*Purpose:* To enable systematic scheduling of electronic record collections.

---

### Developing an inventory in an unmanaged environment

4.44 Where records exist in an unmanaged environment (such as a Windows directory) that may have a long-term value, efforts should be made to include them in an inventory. It is unlikely that personal filestores will reflect a corporate filing structure, so a description of the file structure must be produced and the files it contains listed. Textual descriptions should be produced for the file structure that can be used to develop finding aids. This document will represent the architecture of the entire filestore and, if possible, should be held electronically in such a way that it cannot be separated from the constituent documents.

4.45 There is no prescriptive guidance about the level at which such descriptions should be targeted; but the level should be no lower than folder (directory) and often will be pitched at groups of folders one or more levels up the hierarchy.

---

### Planning for appraisal: developing a selection mechanism

4.46 In comparison with conventional records, the timeframe in which effective action to select and preserve electronic records can be taken is foreshortened, due to:

- the pace of technological change in the systems which create, store and access records
- the instability of the media on which records are held
- the danger of technological obsolescence.

4.47 Early appraisal is required in order to avoid the risk of records becoming incomplete or unreliable, or changes in information technology systems causing the loss or degradation of records which have not been migrated to a new system with sufficient forethought. In this context, appraisal should be done at the most within five years of creation of the earliest records within a system; and ideally, an initial appraisal of the records *likely* to be created within a new system can be conducted at the time of system design and installation.

4.48 As with conventional records, electronic records will fall into broad categories:

- many electronic records will only have an ephemeral value and will not need to be kept in the long term
- others will need to be kept for legal and business reasons
- some will be needed for operational reasons and the administration of the department in the longer term
- a proportion will need to be safeguarded for eventual transfer to the Public Record Office.

4.49 Early appraisal, while ensuring that records of longer term value are safeguarded by migration into replacement systems, will also enable the identification of records with only short-term value. Once beyond their useful life, it will be possible to avoid migrating the latter to a new system unnecessarily, offering cost savings as a return on the earlier appraisal work. In cases where a substantial number of electronic records already exist, and where no systematic appraisal decisions have been made, care should be taken to deal with these in a manner which is consistent with a long-term strategy of early appraisal. Some practicalities of planning for appraisal are described below.

4.50 In certain circumstances, appraisal of legacy systems may lead to an early transfer of electronic records into the Public Record Office for managed preservation, to avoid subsequent problems typically associated with old computer systems - that is, records in obsolete formats and lacking in documentation. Material which falls into this state will be difficult and expensive to migrate - if they remain readable at all - and may be lost to the public record. An early physical transfer to the PRO will not, in itself, affect the timescales controlling release of records to the public.

4.51 An appraisal strategy for electronic records should aim to:

- identify which records should be appraised, and why
- develop a strategic plan for appraisal

- develop a mechanism for conducting appraisal appropriate to the circumstances in which records are kept
- enable the recording and prioritisation of any actions which should be taken on the records, as a result of the appraisal.

4.52 In devising an appraisal strategy, consideration may be given to:

- an organisational, or process-oriented perspective, primarily concerned with the business context and operational needs of the department
- a functional perspective, identifying the main business functions, activities, and transactions which produce records
- a subject, or documentation-oriented perspective, which will be informed by the Public Record Office acquisition and selection policies.

For each department, the appropriate balance between these (and other more specialised) aspects will vary according to the local situation. Much can be gained, working within the resources available, by drawing on systems portfolios, business information systems charts and procedure manuals to develop an understanding of the roles and relationships of electronic record collections. Further guidance and practical toolkits for approaches to appraisal will be developed by the Public Record Office in the future.

#### PRO selection policies

4.53 The Public Record Office Acquisition Policy (1998) identifies specific areas which are the guiding criteria for selection and transfer of material into the PRO. The elements in the inventory which describe the subject, thematic or documentation role of the record collections will be of value in assessing the degree to which records meet these criteria.

4.54 Whilst business-oriented perspectives identify operational and business needs and requirements for departmental accountability, content-based criteria will also determine appraisal decisions relating to particular sets of records. In some cases, it may be possible to identify future research value - for example, in documenting an aspect of the interaction of the state with its citizens - which is not readily evident from a purely functional or operational viewpoint. In others, relying on a functional analysis alone may lead to aberrant decisions when considering candidate electronic record collections for permanent preservation; whereas sampling of the contents may indicate that the records do not have appropriate long-term value.

4.55 With departments, the PRO will be developing a set of operational selection policies which will be administered within individual departments and across government. These selection policies will articulate how the overall acquisitions policy bears on the records of departments and agencies in detail, and will apply equally to electronic records as to conventional paper records. These should be taken account of when linking disposition schedules to a category of electronic record, or an element of the corporate filing plan. In cases of doubt, the DRO should consult their PRO Client Manager.

A mechanism for planning appraisal on existing systems

4.56 A broad mechanism for conducting appraisal on electronic records which have already accumulated in existing systems is described below. This uses the information which is kept in the inventory of record collections as the initial basis for identification, and includes business and content-based viewpoints. This mechanism does not suggest the actual criteria which are used to evaluate the records: these will be determined by the PRO selection policy and the operational and business needs of the department.

4.57 Firstly, identify a core business function or other area of primary interest. Secondly, identify collections of records listed in the inventory which fall within this area, and for each collection of records:

- map any record flows into and out of this collection, and to or from other collections, using information in the inventory
- identify any duplicates or subsets of the records, and link these subsets to decisions made on the record collection under consideration
- apply departmental business needs and PRO selection criteria to assess evidential and research value
- apply retention and disposal scheduling to these and any duplicates/subsets
- consider requirements for permanent preservation, and conduct a sampling exercise if necessary
- record the results of the appraisal in a report for future reference
- record any future actions which need to be taken, including future migration needs.

4.58 A detailed assessment of these record groups will involve asking questions such as:

- what are the legal and operational requirements which must be satisfied by record-keeping for the business activity to which these records relate?
- are these electronic records likely to have long-term evidential value?

- are these electronic records likely to have future research value, bearing in mind the strategic objectives and collection themes of the PRO selection policies?
- are there any other electronic records that should be kept for accountability or other specific reasons, which are related to these records?
- are there any related paper records, in hybrid electronic / paper collections, which should be treated alongside these electronic records?
- are the records in this collection created (in whole or part) by information flows from another source?
- do the records in this collection contribute (in whole or part) to the information contained in records in another collection?
- what are the relationships within and between these records and other record series?

4.59 In all cases DROs should seek the advice of their Client Manager before proceeding. Although the principles remain the same as for conventional paper records, the approach will be different and it will take some time before records review staff have sufficient experience in reviewing electronic records to develop confidence in their application. One outcome of this appraisal exercise might be to review the record-creating system or record collection at a later date, where there is a possibility of change in the way it is used or the records that are produced. This can be done on an ad hoc basis or as part of a wider-ranging systems review.

#### Building appraisal into new systems design

4.60 The appraisal of existing systems parallels the process which has conventionally been followed for paper records, where appraisal takes place on sets of records which have already been created and accumulated within a system. In the case of electronic records, this appraisal strategy must necessarily be implemented at a much earlier date to ensure safeguarding of valuable records. With new information systems an opportunity exists to build initial appraisal decisions, at least at an outline or tentative level, into the design of record-keeping systems.

4.61 By linking records management to the business aims and structure of the organisation, initial decisions on retention and scheduling can be made at or before creation of the records. This will enable records to be managed consistently and effectively as needed for business activities, and appropriately disposed of afterwards. In this sense, appraisal becomes part of the design (or conception) phase of the record-keeping system; however, records managers

should remember that there will be a significant proportion of records for which such early appraisal cannot be made, and others in which it will be desirable to revise the initial decision as the long-term value of the records emerges. Systems designers should be careful to ensure that no automatic actions are taken on scheduled records without offering the opportunity for confirmation or revision by the records manager.

4.62 Conducting appraisal at this stage will involve:

- identifying the business functions that will generate records
- identifying the IT systems that support these business functions, and which will physically produce the records
- identifying the record series to be captured
- assessing the characteristics and record-keeping requirements of each series
- allocating initial disposition decisions following from these record-keeping requirements
- designing facilities in electronic record management systems to support management of these requirements.

4.63 Where plans for upgrading or replacing systems require decisions to be made on whether or not data should be migrated to the new system, appraisal should attempt to identify record collections which meet previously established criteria. Reference can be made to the relevant PRO operational selection policy (as these are developed), to the business purpose of the original system, and to the business case and project initiation documents produced for the new systems. Plans should be evaluated against any record-keeping policies and requirements established by the department. Where semi-active or inactive records (together with their metadata) are not migrated to the new system, they should be transferred to a maintained electronic archive within the department, if they are required for business reasons or for selection by the Public Record Office.

4.64 A thorough understanding of the record-keeping environment, and a top-level view of the way in which information systems and technology interact with this, will aid the DRO in influencing new systems design. It will also be helpful in contributing to the development of corporate information policy and in encouraging best practice amongst end user groups.

## Appraisal of poorly structured collections

4.65 Where electronic documents exist with little organisation or structure linking them together in meaningful collections or groupings, appraisal will be difficult. This will be the case where, for instance:

- electronic documents are held on a shared local network drive with little or no systematic organisation or structure in the filing or folder hierarchy
- files and folders are created directly by end users with no established naming conventions, resulting in names that are ambiguous, mysterious or misleading
- electronic documents are held in a document management system that relies upon search technology alone to bring together sets of related records.

4.66 Poor structuring in collections of electronic records prevents the consistent development of collections of records which can be managed as a group, and the easy allocation of individual documents to such collections on creation by the end user. In such circumstances much of the context of an electronic record will be lost. If individual documents are appraised in isolation from their original context, consistent appraisal will not be possible.

4.67 In addition, for electronic records, a document-by-document review is very time-consuming and resource-intensive and is unlikely to be cost effective. While a paper folder can easily be scanned, the physical necessity of opening and scrolling electronic documents is far more cumbersome, unless some specific support for browsing has been built into the information system. Where appraisal has to be undertaken of this kind of material, three main options present themselves:

- appraisal undertaken by the DRO on a document by document basis
- appraisal undertaken by document originators or desk officers
- appraisal undertaken with some form of software support.

4.68 At present, most commonly available software support is limited to simple keyword searching and retrieval, and is unlikely to be effective beyond grouping similar titled documents together (in which circumstances, naming conventions will clearly be useful). While more sophisticated forms of software support - concept agents, analytical search engines, textual visualisation tools - that may help with this area are emerging, it would not be wise to rely on putative future developments to solve the problem.

4.69 Appraisal undertaken at the file/directory level may be assisted by using standard file manipulation tools to provide a basic analysis of document

characteristics, by pre-sorting documents within the disk directory according to various characteristics. For example: sorting documents by date order can help to assess patterns of activity within a relevant date range; and sorting by creator application (such as text document, spreadsheet, etc) will indicate activity that has generated particular presentational patterns.

4.70 Some consideration must be given to those documents that have not been preserved as records by the authors and users and where a number of attributes will either be missing or, if present, may not comply with records management procedures. Consideration should be given to the following:

- authenticity – (is the document as stored the one that was used in the first place?)
- have features been used such as dynamic dates that might undermine the value of the documents as records?
- version control – has any mechanism been used to manage the different versions of a document and can this be preserved with the document as a record?
- audit trails – can the history of this document from creation through to archiving be traced?
- can the documents held in computer file store be mapped onto a corporate records structure, possibly as represented by paper based registered files?
- has only one copy of a document been preserved and, if not, can the primary version readily be identified?
- has the designed file structure been adhered to or are files distributed in an idiosyncratic fashion?

---

## Disposal

4.71 In conjunction with the PRO Client Manager, the DRO should identify those categories of records whose value to the organisation and to the PRO itself can be reasonably predicted. This will include those:

- that require retention for a specified period on legal grounds
- that merit permanent preservation, and which will eventually be transferred to the PRO in one of the approved formats
- that merit early destruction once no longer needed.

In addition, there will be categories where only an initial disposal can be allocated, which the DRO will have to mark for review at a later date. For electronic records, however, this is likely to be after a much short period than has usually applied to paper records.

4.72 Electronic records of continuing value will need to be migrated through successive upgrades of hardware and software in such a way as to retain the full content and context. This should include the records themselves together with record metadata, and any other contextual information which affects the meaningfulness of the records and their relationship to each other. Migration should be carried out in such a way as to maintain and demonstrate the authenticity and integrity of the electronic records themselves. Planning of such migration activities will provide the DRO with an opportunity to re-appraise the decisions to retain or delete electronic records in those categories where only an initial disposal has been possible. This will reduce the likelihood of an unnecessary migration of records which will later be destroyed.

4.73 As in best practice with paper records the users of such an electronic record-keeping system need to be aware that electronic records should not be kept longer than the official approved retention period; and that once allocated to an appropriate category, they will inherit the scheduling characteristics of that category. Guidance should be developed that will enable users consistently to identify records which merit disposal in accordance with the established criteria, and to understand the mechanisms by which they can be allocated to the appropriate category.

4.74 The management of all corporate records should be subject to corporate rules and procedures, and electronic records are no exception to this; they should be organised, maintained, stored and protected according to this discipline. They may only be disposed of in accordance with established procedures and time-scales identified in departmental record management manuals and disposal schedules. It is impractical in most cases to adopt a document level approach and normally decisions would be made on groups of records (folders) or even on groups of folders. Having made these decisions, they must be documented and preserved with the records themselves.

#### Destruction of records

4.75 A record should be kept of the destruction of electronic records after this has taken place. In a well managed electronic record-keeping system, this can be achieved by retaining relevant parts of the metadata, which enable an identification of the record to be made, and by adding to this metadata documentation of the record destruction, including date and authorisation for the disposal actions.

4.76 Record managers should be aware that deletion of a document from disk storage is not equivalent to destruction; potentially, the document is still retrievable unless a complete reformatting of the media has taken place, or enough time has elapsed for the freed storage space to be re-used by newly created documents. In such a case, deleted records can be re-constituted by software tools that read the disk drive directly; clearly, for sensitive records there will be security implications that may demand assurance of destruction (by low-level formatting, or destruction, of the physical media) rather than merely deletion of records. Records managers should also endeavour to ensure that, where more than one copy of a record may exist, all copies are destroyed at the same time, including both primary and working copies.

4.77 On the other hand, in a record-keeping system which allows pointers to be linked to a single copy of a record so that it may be accessed from more than one file or folder, great care should be taken to ensure that records marked for destruction are not still required within another context. While more sophisticated record-keeping systems will offer facilities for the maintenance of referential integrity, much greater care will be needed in uncontrolled environments such as Windows where the use of 'shortcut' facilities is unpredictable.

## 5 : Preservation of electronic records

5.1 This section deals with:

- the rationale and major characteristics of a preservation strategy
- approaches to developing a preservation strategy
- the migration of records to a new system platform
- selecting and refreshing physical media
- preserving metadata
- documenting and auditing the preservation process.

---

### Purpose of preservation

5.2 Archiving of data has traditionally been handled by IT personnel but the attributes of this process have very little to do with archiving as it is traditionally understood in the records management community. Usually data was copied wholesale on to duplicate media and held for a prescribed time, and would then be deleted after a specific interval in order to release the media for re-use with new data. There were very few mechanisms to ensure the disposal of the data was managed in an informed manner. The main mechanism to preserve data within the organisation's record system relied upon a policy of print-out to paper and attachment to appropriate paper files; a policy which cannot be sustained in the long-term once the electronic working environment is well established.

5.3 This section identifies the issues to be addressed when considering the medium to long term preservation of electronic records, and seeks to provide the terms of reference for the development of a strategy for the preservation of electronic records. This section indicates the relevant standards and codes of practice to be used and describes the preservation strategy within originating departments, or agencies, as opposed to that within the Public Record Office.

5.4 Preservation of electronic records has to address the following areas:

- purpose
- access levels and multiple accesses
- duration of the preservation period.

5.5 *Purpose* refers to the owning organisation's intentions for preserving the records and their information content. Use or reference to the records may well increase or diminish during the period of preservation as the statutory and administrative climate changes, but as organisations start to develop and profit from their corporate information resources use of preserved records may well increase in ways not foreseen by the creators. Mechanisms need to be provided

to ensure that these variations in demand are adequately addressed. It must be clear why records are being preserved and the terms which govern the period of preservation, including any changes, should be transparent to those individuals entrusted with the preservation of the records. Records which have been rejected for transfer to the Public Record Office should not be preserved for longer than is required by the organisation's disposition policy.

5.6 *Levels of access* must be capable of being defined in response to an organisation's business needs and are likely to vary according to the organisation's information requirements. Records may need to be made available to the entire organisation or to a designated part of the organisation; there may be a series of levels or views depending on user access permissions. As time proceeds, ultimately the chief end user will be the DRO and the records management staff, who will require access for appraisal and final disposition of the records.

5.7 *Duration* of the preservation period will vary according to departmental needs. In most departments this is unlikely to exceed 30 years and may in many cases be far shorter. However, certain departments and agencies will need to hold records for periods in excess of 30 years. It is likely that increased dependence on electronic record-keeping will generate a requirement for organisations to retain data for longer periods, as already happens with paper based records; a relevant example are personal staff files which are kept for many decades. In such cases the long-term preservation concerns are similar to those of the Public Record Office.

5.8 Consideration of business objectives is important when deciding how to transfer records to an electronic records repository. Records managers must note that this remains an organisation's own responsibility and each one must develop appropriate working practices and procedures to care for public records within the context of their own business. Electronic documents which are considered to be the primary record may ultimately be selected for transfer to the Public Record Office if they originate from an organisation subject to public records legislation. In addition, an organisation may wish to preserve electronic documents because the information they contain can be more readily accessed and exploited to the benefit of the business than when it is held on paper in a registered file located in a Registry.

5.9 Wherever public records are concerned, the recommendations of the Public Record Office would need to be strictly adhered to, so that if transfer to the PRO did occur, the records would be held and structured in approved formats. The appropriate PRO Client Manager should be consulted before a final decision to select or destroy is taken.

5.10 Records managers might wish to transfer documents from a desktop computer to an electronic records repository within the department because:

- a project has reached a hiatus such as the conclusion of a phase (for example moving from procurement activity when a contract is let to managing that contract)
- the business changes and the staff move to where their expertise is better employed
- either the hardware platform or the application software proves not to be Year 2000 compliant (see Annex A).

The people managing the contract would require access to the information held in the files, but the documents themselves, providing a historical record, would be stable and not subject to further revision, and as such suitable for archiving.

---

**Developing a  
preservation strategy**

5.11 Where it is intended to hold the definitive record electronically, the preservation requirements are different from those used in IT archiving utilities. Effective preservation depends on the records and IT managers working together to determine the most appropriate method within the context of the departmental IT strategy. This section aims to clarify the issues and business drivers needing to be addressed if preservation is to be achieved effectively.

5.12 If the material being archived is for immediate transfer to the Public Record Office or another place of deposit, the directions contained in section 6 will apply; however, if the records will remain in the department for a period then, obviously, their preservation is the department's responsibility. A plan should be produced to cover the topics described in this section. Such a plan will have long time-scales to cover the entire time that the records will be preserved and accordingly will need to be endorsed and funded by senior management. The plan needs to take account of the specific guidance on preservation provided here. The following parties must agree this transfer plan:

- systems administrator
- records manager
- budget holder.

A policy on continued access by end users should be clearly stated and promulgated to everyone in the organisation not just the IT providers. In order to preserve access rights, organisations need to develop a preservation strategy which will meet all of the operational, administrative and regulatory requirements.

5.13 A preservation strategy is required and it must address all the preservation criteria outlined in these guidelines. In particular policies must be in place to address the following areas of concern:

- loss of records due to media deterioration/obsolescence
- loss of records due to obsolescence of application format so content cannot be read.

5.14 There are two options; the first is to maintain and preserve the original application programs in which the records were created and held and the second is to provide a digital information migration strategy. The first option will only be viable in the short to medium term depending upon a department's IT strategy, IT migration plans and whether the hardware platforms and application software are Year 2000 compliant (see Annex A). Departmental preservation strategies must provide for long-term preservation; that is for periods of five years and longer.

5.15 Where the original application is to be used, it is imperative that the departmental IT strategy makes provision for an annual review of all applications and platforms to ensure that appropriate support is given for all originating technology. It is also necessary to ensure that any policy decision to change to another platform takes account of both the migration requirements of records held in native formats and the requirement to preserve the integrity of the information. It should do this by storing the records together with the contextual metadata in a stable area of the organisation's workspace to ensure they cannot be modified or deleted by users.

5.16 The PRO recommends that a preservation strategy is developed and implemented which should provide mechanisms to preserve data and metadata in a format that is independent of the particular hardware and software used to create them; in this way the integrity of the records should be preserved along with the data content. This approach is explored below, where the preservation issues are categorised in order to inform organisations why they are included in a strategy and the consequences of their exclusion.

5.17 Operating procedures need to address the following:

- compliance with PD0008 and proof of compliance
- migration policies for hardware and systems and application software, including creation of audit trails establishing successful migration with no loss of data
- hardware refresh
- preservation / maintenance of access
- checking of back-ups to prove continued utility and availability.

5.18 Procedures must be implemented so that all necessary tasks are performed to ensure the successful, long-term preservation of electronic records. In addition, the roles needed to carry out these procedures must be defined and built into the job descriptions of members of staff. This latter is to ensure that not only are the procedures in place but that someone is tasked with doing them. The commitment of the senior management and budget holders is designed to make available the resources needed to maintain preservation. These procedures will be long-term and will cover the entire life of the records.

5.19 All activities undertaken as a result of implementing these procedures must be logged on an audit trail and these records must comply with the recommendations contained in BSI/PD0008.

---

**Migration of records to new computer systems**

5.20 Migration is the transfer from one hardware and software environment to another. The objective is to preserve the integrity of the records and to ensure they can be retrieved and viewed in the future.

5.21 Good IT practice requires duplicate backup copies. Ideally there should be at least two such copies:

- *a preservation master*, from which new working copies can be made
- *a security master*, to guard against catastrophic events such as fire or flood.

The two backup copies should be stored separately from the working versions, preferably off-line with one off-site. If new copies are required, the master should always be returned to the secure store dedicated for its use. The CCTA *ITIL* publications provide detailed guidance on this topic.

5.22 In some cases migration may have to be undertaken before it is either appropriate or practical to undertake an appraisal of the records; for example hardware platforms or application software may prove to be Year 2000 non-compliant (see Annex A). Where this occurs the organisation should apply the

corporate migration strategy for the archived records and their associated metadata (which provides the contextual information, such as the folder or directory structure). The record manager should be notified that migration is to take place and consulted prior to work commencing to help ensure the successful transfer of the records and metadata to the new environment. Retention of the metadata as well as the content is important as this shows how the records were held and used; without them users would be less able to view related documents in context and the disposal process would be made more difficult.

5.23 The rate of change of IT, both software and hardware, is likely to shape the timetable for migrating electronic records. In any case, records should be copied on to new media at intervals that meet the manufacturers' recommendations for the medium to prevent the physical loss of data or technological obsolescence. The DRO should liaise regularly with the IT department to establish when migration is likely to happen and to ensure that appropriate procedures are in place to safeguard both the records and the associated metadata. It would be unusual if migration occurred more frequently than every three years.

5.24 The conversion of records which are held in transfer formats and stored on transfer media, to the preservation formats and media comprises most of the steps listed below. This approach, however, is neither complete nor prescriptive and each organisation should devise a plan applicable to its own business environment.

5.25 Before commencing any activity the preservation plan must be developed and agreed:

- records must be transferred and converted to produce a preservation copy
- all the steps must be logged and documented to ensure a complete audit trail compliant with BSI/PD0008
- the preservation copies of the records must be backed up to ensure recovery following a disaster, in compliance with the department's IT contingency plan using off site storage for backup copies
- the presentation copies must be created, including background descriptions and finding aids, and the process must be logged in a similar fashion to creation of preservation copies
- the presentation copies of the records will need to be backed up in a similar way to the preservation ones
- the presentation copies and finding aids should be made available for access either for internal exploitation of their information content or for public access.

5.26 Records should be verified when written to new formats, migrated or copied for refresh or backup purposes, and special note made of any loss of data. This should be conducted according to best practice as specified in the CCTA *ITIL* publication on *Computer Operations Management*.

5.27 All copying of records should be carried out using applications that produce audit trails, have integrity checking and reporting features. Procedures should be adopted that conform to *BSI DISC PD 0008*, which has been recently extended to cover re-writeable media as well as ‘write once read many’ (WORM) technology.

5.28 If the records are earmarked for ultimate transfer to, and preservation in, the Public Record Office consideration needs to be given to storing them in transfer formats compatible with those identified in this guidance as appropriate for that eventual transfer. Departments are encouraged to comply with this list of recommended transfer, preservation and presentation formats in order to minimise the cost of internal migration and facilitate transfer to the Public Record Office when appropriate. Alternatively mechanisms will need to be provided which allow export to the recommended formats when transfer becomes appropriate.

#### Selecting and refreshing physical media

5.29 The media that will be selected for primary access will depend on the support offered by the IT provider, the required levels of access to records, and the separate cost options. The constraints are that long-term availability, however defined, will be required with no degradation of content and quality; as a generalisation, the less volatile the media the better. Although optical WORM media may seem the most dependable there are good reasons to consider using re-writeable magnetic media particularly where large volumes are involved.

5.30 It is necessary to consider how access will be provided over the long term as software formats are dynamic. Critically if the organisation chooses to depend on viewer technology it is necessary to ensure that the selected viewer can access all the formats held within the departments electronic file store. If it does not it will be necessary to migrate the affected files to a format that can be viewed otherwise the material will be inaccessible.

5.31 All forms of electronic media have a finite life which can be affected by environmental factors (e.g. heat, humidity, electromagnetic fields). In order to prevent the electronic records degrading they must all be re-written to new media on a regular basis; the frequency of this will need to be agreed with the media manufacturer but regular checks should be made on the stability of the media at no more than 5 year intervals.

5.32 This will affect all media, master copies, back-ups and presentation copies, whether they are held on optical disks CD-ROM, magnetic disk or tape. When the media is refreshed the activity must be recorded in an audit log so that all actions can be monitored.

---

**Back-up of electronic records**

5.33 The IT providers in all organisations should have policies and procedures for backing-up the records. Nevertheless it is prudent to ensure that the following issues have been addressed:

- media type
- where the backup copies are to be stored
- the number of backup copies to be preserved
- relevant operating procedures, for example, media refresh, migration, software enhancement.

5.34 All of the following checks must be made against all of the copies of the records, both preservation and presentation:

- is the storage environment adequate and does it comply with all relevant standards?
- has there been degradation in the media, and can the information still be accessed?
- do the IT providers plan to upgrade the hardware or software environment; if so ensure that the material held in the electronic records repository will remain accessible. This involves checking (at no longer than 5 year intervals, but sooner if the systems are enhanced more frequently):
  - media accessibility
  - application compatibility
  - systems (e.g. operating system) compatibility
  - that the backup system is functioning correctly
  - that the back-ups of records can be re-installed and read?

---

**Preservation of contextual metadata**

5.35 If records are to be preserved in a usable form consideration needs to be given to the metadata that is required to ensure continued accessibility, and to demonstrate the authenticity which confers their status as corporate records. In the absence of audit trails, for example, authorship may be unclear and it will be difficult to ascertain the business context of a document. Preservation of documents without their contextual metadata will compromise any preservation strategy.

### Metadata in document management systems

5.36 Electronic document management products offer facilities for storing and managing documents, but are not designed to deliver records management. One of the problems that can be encountered in these type of application is the preservation of metadata and file structure as well as maintenance of the links between the metadata and the document.

5.37 In order for a document to gain the status of a record its provenance, authenticity and relationships must be established. There is a risk that document management or group-ware applications will store documents and metadata in such a way that they cannot be exported together, and the links between them are lost. When documents are to be exported from the original application, it is essential to preserve and make accessible the links between them and the relevant metadata.

5.38 If electronic documents have been managed electronically, the metadata describing folder structures, contents and relationships between documents will also be stored in the electronic document management application. When the documents are to be transferred to the PRO, care will need to be taken so that the metadata and the links to the document are not broken. Relevant metadata (which may be derived from the document properties, the directory structure or from the body of the text itself and stored in a description file) is listed in paragraphs 2.45 to 2.49. Once transferred into an electronic records repository, the metadata should be stored in a structured description file, with a separate entry for each document and the entries linked to the documents by the filename used to store the document, and some system that allocates unique numbers.

---

### Export of electronic records

5.39 When the IT provider moves electronic records for any reason, the department must ensure that they can be exported from the target environment to an application and platform independent one. An electronic record is the sum of the document, its context and metadata plus the audit trail to establish provenance; contextual information and metadata must not be capable of being unlinked from the document. Requirements of an export mechanism for electronic records include the ability to:

- treat the record as an entity including context, metadata and audit trail information
- export a record at any point in its life-cycle
- ensure little or no loss of information
- enable the audit trail to be annotated noting any changes
- facilitate the physical transfer of the records.

---

**Environmental storage conditions**

5.40 The environmental conditions for archive storage should comply with the recommendations of *BS 4783: 1981-1993 Storage and Maintenance of Magnetic Media and Optical Disk Cartridges*. The recommended maximum and minimum temperature and humidity levels for most media are 18°C to 22°C with 35% to 45% RH. The *CCTA Infrastructure Library (ITIL) Environmental Management Set - Environmental Standards for Equipment Accommodation* is also relevant. All data storage media should be properly shelved or stored in appropriate furniture or shelving and in accordance with the recommendations of BS 4783. DROs should seek the advice of their IT department.

5.41 It is strongly recommended that the storage and maintenance environment should be designed to minimise the presence of dust. The cleaning programme should be adjusted to ensure that current measures are adequate for storage of this media and the rooms should be inspected on a weekly basis. The *CCTA ITIL Environmental Management Set - Maintaining a Quality Environment for IT* gives guidance on the procedures and standards to be used when drafting specifications for the cleaning of computer accommodation.

---

**Documentation and security**

5.42 Electronic records should be held securely with access by authorised staff only, whether they are held on-line or off-line. Procedures should be measured against professionally approved standards, including *BS 7799 1995: A Code of Practice for Information Security Management* and *BS 5454*. Reference should also be made to the IT department's security policy for the relevant installation. Whichever medium is used to store the preserved electronic records, it should be clearly labelled to indicate their provenance and subject matter and, where appropriate, their security status as masters.

5.43 The DROs and the IT managers should audit preservation procedures within their department to ascertain the degree to which they adhere to the guidance given here, and the scale of the problem where practice deviates from this. This audit should look at issues such as:

- media longevity
- hardware compatibility
- software compatibility
- audit trail mechanisms.

5.44 Record and business managers need assurance that migration policies are appropriate and are being implemented. The provision of workbooks and registers is essential to ensure consistency, minimise information loss and record actions taken; usually, this record of events will be required to be preserved with the electronic records. Consideration should be given to creating an audit trail demonstrating compliance to *PD0008* as proposed in the *BSi Compliance Workbook, PD0009*.

## 6 : Transfer of electronic records

- 6.1 This section deals with:
- the main characteristics of the transfer process for electronic records
  - software formats used for transfer of electronic records
  - formats for presentation of electronic records
  - physical formats for transfer of electronic records
  - exporting, listing and describing the records.

---

### Purpose of transfer

6.2 This section is designed to provide basic guidance for those departments and agencies where electronic records have been selected for permanent transfer to the Public Record Office. Upon transfer the records will pass into the custody of the Keeper of Public Records, and the PRO will undertake to preserve these records in perpetuity as is done for traditional paper records. This guidance includes the recommended software formats appropriate for migration and transfer to the Public Record Office as well as specific advice on the procedures to be adopted when undertaking a transfer.

6.3 Departments should note that the guidance given in this section is under constant review and when electronic records are selected for transfer the DRO is advised that the relevant Client Manager should be asked to consult with the PRO Electronic Records Accessions Unit prior to work proceeding within the department.

6.4 Formats for accessioning assemblies of electronic records can be grouped to cover the areas of transfer, preservation and presentation. The transfer formats need to be comprehensive in that not only document content, but structure and context must be part of the archived document. The preservation formats should maintain record assembly integrity and, as far as is possible, stability. There should not be too many formats and they should be managed in such a way as to inspire confidence in their longevity. One important aspect of the preservation formats is that they should be capable of easy conversion into a presentation format. The presentation formats should display the archived electronic records in a form that closely resembles their original appearance.

---

### Formats used for transfer

6.5 The formats currently available that meet the requirements defined for transfer are PostScript, TIFF, SGML, PDF and delimited file format (such as comma separated variable). Each of these formats is appropriate for specific record types detailed in the tables in this section. These transfer formats appear to be robust and to have a long life ahead of them. The PRO recommends that conversions are kept to a minimum because any document format conversion, however skilfully achieved, is likely to incur some data loss.

Format name	Application	Comments
<p><b>PostScript</b></p> <p>Transfer issues</p>	<p>Any application designed to run on a desk-top computer will support PostScript printing, but as PostScript is designed to be written to file as well as to a printer it can be used for electronic record transfer. The use of PostScript requires little, if any, enhancement to existing IT applications and is, therefore, an important format for electronic record portability.</p>	<p>PostScript is useful for the transfer of text and graphics-based records created on the desktop.</p>
<p>Preservation issues</p>	<p>PostScript™ from Adobe™ has already existed for over 20 years and files created for early versions are still readable using the latest software releases.</p>	
<p><b>Portable Document Format (PDF)</b></p>		
<p>Transfer issues</p>	<p>PDF is an industry standard format for document description. It was developed and employed by Adobe™ in its Acrobat™ family of products. PDF is designed as ‘electronic paper’ for platform and application independent electronic record access and usage.</p>	<p>This format should not be retrofitted; however, if departments already store electronic records in PDF the PRO will consider them to be adequate for transfer and storage.</p>
<p>Preservation issues</p>	<p>Adobe™ Acrobat™ is a variety of PostScript™ and has many of the advantages including the placement of the standards specification in the public domain by Adobe™.</p>	
<p><b>Tagged Image File Format (TIFF)</b></p>		
<p>Transfer issues</p>	<p>TIFF is a de facto standard for images.</p>	<p>TIFF can be used to transfer image-based records.</p>
<p>Preservation issues</p>	<p>Another Adobe™ public domain format with widespread industry support</p>	

Format name	Application	Comments
<b>Comma Separated Variable or delimited file format (CSV)</b>		
Transfer issues	Delimited format is suitable for spreadsheets and some small. This format preserves the data input to the application, making it possible at a later date to recreate the spreadsheet or database.	Delimited files are suitable for the transfer of structured records such as those held in spreadsheets or databases.
Preservation issues	A vendor supported de facto format for transferring structured data from one table, spreadsheet or small database to another.	
<b>Standard Generalised Mark-up Language (SGML)</b>		
Transfer issues	SGML is an ISO standard for document description. The cost of retro-fitting SGML to existing documents is likely to be too high to be economic, and is not recommended.	If documents exist in SGML format, the PRO considers them to be adequate for document transfer and storage.
Preservation issues	An ISO standard for document description offering the stability of international standards.	

Table 6.1: Transfer and preservation formats

### Formats used for presentation

6.6 When viewed by a reader, an electronic record should appear in a form as close to the original as possible. This can be achieved by using document viewers or proprietary electronic publishing. Viewer technology, while very advanced and comprehensive, is not as broad in its application as electronic publishing. The standard specification of the Adobe™ Acrobat™ electronic publishing product (PDF) is in the public domain, making them potentially more ‘future-proof’.

6.7 Because PostScript, TIFF and SGML can easily be converted to the PDF format, the PRO will use Adobe Acrobat™ PDF as the presentational format for text and image based documents. If the information content from spreadsheet, diary and database packages needs to be kept for re-use in other similar packages, the PRO will use delimited format to export, transfer, preserve and, subsequently, present structured data of this type.

Format name	Application
<b>Portable Document Format (PDF)</b>	Adobe™ Acrobat™ is based on Adobe™ PostScript™ and has many of its advantages including the placement of the standards specification in the public domain by Adobe™. The Acrobat™ family of products is designed to publish electronically a wide range of initial formats.
<b>Comma Separated Variable (CSV)/Delimited File Format</b>	A vendor supported de facto format for transferring structured data from one table, spreadsheet or small database to another. No formatting or formulae are preserved but delimited file format is designed to facilitate export and import of structured data.

Table 6.2: Presentation formats

6.8 The above formats are a first attempt to address the issues presented by the archiving of electronic records collections. In such a rapidly changing environment, they can only be provisional; further recommendations will determine if other formats offer advantages either to complement or improve on those already identified, particularly in dealing with multimedia formats, intelligent documents and documents using dynamic links - where, at present, there are no definitive standards.

6.9 At present, HTML is not one of the PRO's accepted transfer formats; this is because the standard is dynamic, and subject to commercial pressures that render it unstable. To prepare HTML files deemed worthy of permanent preservation for transfer to PRO or to remain in-house they must be converted into one of the PRO accepted transfer formats. In the latter case, if conversion were not completed the department would have to accept the responsibility for continued migration. However, departments should consult the PRO before using HTML files to preserve records deemed worthy of permanent preservation., since this is a very dynamic area.

6.10 In the short term, if records stored in HTML must be archived then care must be taken to preserve as much of the information content as can be achieved while taking into account the exigencies of the business environment. If hyperlinks have been used, the PRO currently recommends that the HTML document is annotated with target web addresses, brief descriptions of their contents and a description of the context and relevance of the links to the main HTML document. The issue of archiving HTML documents will be kept under review. As the use of documents employing dynamic links to other information sources increases and matures across government the PRO will evaluate these developments and refine this guidance

---

**Media and channels for transferring records**

6.11 This section lists the preferred media for electronic records transfer once the records and metadata selected for permanent preservation have been rendered into one of the recommended transfer formats. Ideally, all transfers of electronic records to the PRO could be made electronically, using network technology. However, until the Government Secure Intranet (GSI) is widely established across government, there will not be a secure method of effecting such transfers.

6.12 The physical transfer of the documents requires that decisions concerning the media to be used and transport mechanisms must be taken. There are a number of transfer options using optical or magnetic media and physical transfer. These are listed below in order of preference:

- CD-ROMs and CDRs using WORM technology
- 4 mm DAT tape
- DVD drives
- ZIP Drives
- LS-120, 120 Mb, 3½" diskettes
- 1.44 Mb, 3½" diskettes.

With all of these types of transfer media, it is important to ensure that the media format is common to both the sending organisation and the Public Record Office, otherwise a successful information transfer cannot take place. The PRO can only accept disks or tapes using available applications at the time of transfer. The Client Manager will advise on the correct approach, and can provide assistance from the PRO Electronic Records Accessions Unit in establishing agreement with the departmental IT provider.

6.13 These media formats are likely to require the support of system utilities; for example, backup or datastreaming applications. Systems administrators may prefer selected files to be copied to a non line-of-business computer prior to the transfer; others may even require that the transfer is performed during out of business hours.

6.14 CD-ROMs and CDRs are the most secure media for archival purposes; they cannot be overwritten and they can hold substantial volumes (currently up to 650 megabytes).

6.15 DAT tape does not have the archival advantages of CD-ROMs and CDRs as it is possible to overwrite or corrupt data held in magnetic form. It will hold between 4 to 8 gigabytes of data and is a suitable medium for handling large transfers.

6.16 DVD (Digital Versatile Disk) is a new type of CD-ROM that holds a minimum of 4.7 Gigabytes. This medium shares the archival advantages of CD-ROM with much larger storage capacity. The limiting factor at the moment is that few organisations have the capability of creating DVDs.

6.17 ZIP Drives (manufactured by Iomega) are non-standard drives that can hold between 100 Mb and 250 Mb. They have archival advantages, but are not pervasive throughout the user community; if available in the organisation originating the transfer, the possibility of their use should be investigated.

6.18 LS-120 is an emerging standard of 3.5 inch diskettes holding 120 Mb with backward compatibility with the earlier 1.44 Mb diskette. For archival purposes, it has the same disadvantages of the earlier version; however, its much increased capacity makes it more attractive for the transfer of electronic records collections and simplifies the management of the process.

6.19 3.5 inch diskettes are the least satisfactory of the preferred transfer media because of their intrinsic lack of manageability. They are portable and suitable for small transfers (under 1.4 megabyte) but the medium is fragile and easy to corrupt or lose data if proper procedures are not followed. Use of 3.5 inch diskettes places a heavier than usual burden on the records manager and establishing provenance and authenticity may prove to be difficult. The PRO Client Manager should be consulted before using diskettes for transfer.

## Recommended media

6.20 Selected data in one of the approved transfer formats must be written to one of the recommended media, and wherever possible CD-ROMs or CDRs should be used. If necessary, PRO personnel will backup a copy of the records on to DAT tape. The PRO will require confirmation that use of the hardware and software is acceptable to the department's IT department. Zip and LS-120 Mb drives increasingly are being used in departments, but before being used to transfer records the PRO should be consulted. Where it is not possible to use any of the media recommended, the plan to progress the work should be developed in consultation with the PRO.

---

## Transferring the records

6.21 This section is designed to provide a brief overview of the processes required for the transfer of selected records to the Public Record Office. DROs are advised to consult the relevant PRO Client Manager before undertaking this work.

6.22 The transfer formats and media having been selected, a transfer plan must be prepared indicating all the necessary steps leading to a successful transfer of documents from live file store to an electronic records repository. This plan will describe the resources needed, timings, time-scales and likely impacts on the organisation. The following parties must agree this transfer plan:

- systems administrator
- records manager
- user of the filestore (if any)
- person undertaking the transfer.

6.23 If the option of transferring documents in PostScript format is selected, some functionality for bulk printing 'to file' will be needed; this enhancement to the operating system may have to be obtained from a specialist supplier. The IT provider will have to discover whether there is a requirement to install other software to facilitate the transfer. This could include a utility for printing a record of the file structure or software drivers for the selected transfer medium.

6.24 The transfer medium should be installed so that the filestore can be copied to it. Note that, at this stage a 'copy' should be made, but the material itself should not be moved. This is to provide contingency should any problems or corruption occur during the transfer process. The steps are as follows:

- the file structure should be documented and transferred to the transfer medium
- the records should be converted to the selected transfer formats taking care to keep as much metadata as possible attached to each record

- the converted electronic records should be copied to the transfer medium, if possible maintaining the file structure
- arrangements must be made to manage the physical transfer to the Public Record Office of the tapes or disks on which the copied records have been stored; this must be done in such a way that there is no chance of either the media or the information becoming corrupt or lost
- whether the records are intended for transfer to the Public Record Office or for internal use, some finding aids will be needed; these should be produced by the person managing the transfer in co-operation with the original owner of the documents - in cases where the records are being transferred to the PRO the Client Manager should be consulted on the form and content of the finding aid
- all the preceding steps must be logged and documented to ensure a complete audit trail compliant with *A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BSi/PD0008) Edition 2, March 1999*.

Listing and describing the records at transfer

6.25 It will be necessary for the transferring department to generate a finding aid that will comply with the editorial guidelines prescribed by the Public Record Office. The PRO Client Manager together with the PRO Record Management Executive will advise and co-ordinate this work. DRUID will probably not supply all the required information to support a transfer of electronic records.

6.26 If it has not already been done, the documents for transfer should be grouped into a logical order. Information on dates ranges covered by the documents, original file references and basic finding aid information will need to be added at this stage, if it has not already been added during the inventory or appraisal processes. The PRO reference for each transferred document i.e. piece and item, should be recorded. A spreadsheet program may make it easier to assign these references correctly.

6.27 The (computer) file list can be a simple list, perhaps prepared using a spreadsheet program, providing limited information about the documents. Each file in the list should be given a unique identifying number, for use as a reference in discussions between the department and the Public Record Office during the transfer process. The other essential piece of information that must be recorded is a complete and unique description of the document's current location. For example, in a Windows or class environment the full path of the file should be recorded in the inventory.

6.28 A practical advantage of using a spreadsheet program to prepare this list is that additional columns of information can be added to assist the appraisal, transfer and destruction processes; for example: the basic appraisal decision and its reasons; original file references; and basic finding aid information (that is, a description of the nature of the document, and the dates range that it covers). Not every document will have an entry in every column.

6.29 Often it will be inappropriate to assign a unique Public Record Office document or item reference to every individual document. It will make more sense to amalgamate several documents into one item. The documents to be amalgamated can be indicated by using a sub-item number, in an additional column.

6.30 At this stage no duplicate master set of the records assigned for transfer should be destroyed by the department. It is important to wait until the PRO Client Manager confirms successful processing of the transferred files. Once this confirmation is received, the department should destroy the original files marked for transfer, and any working copies prepared from them. The finding aid information, and the original file references taken from the transfer list by the Public Record Office should allow the department to recall, retrieve and view any desired record, just as is done for paper records.

#### Audit trails

6.31 Audit trails should be maintained to specify actions taken and decisions made at each stage of the transfer recording, for example:

- who made appraisal decisions and when
- who gave authority to transfer or destroy records and when
- which intermediate working copies of records have been generated.



## **Annexes**



## **A : Safeguarding records across Year 2000**

A.1 One of the milestones set by the EROS Programme for electronic records management across government called for the development of plans for safeguarding or disposal of all electronic record collections which are affected by Year 2000 compliance work by 1 January 1999; planning cannot be delayed if work is to be carried out in the following months. A department or agency which does not already have a clearly defined strategy and detailed plans for dealing with the records management issues relating to Year 2000 will need to make rapid progress in this area.

A.2 This milestone refers specifically to the *records* issues inherent in Year 2000 compliance; the programme to ensure that all application systems are Year 2000 ready is a separate one, which is being overseen by the Cabinet Office. It is not sufficient, therefore, to rely on a Year 2000 Unit or an IT provider to carry out this work; it will be necessary for the records manager to be assured that all electronic records affected by this work are being treated appropriately. This may involve making decisions on:

- which records from a system that is being replaced should be migrated to the new system
- the correct retention and disposal decisions for records that are not being migrated to the new system
- the appraisal and disposition of records from systems that are being discontinued altogether
- the physical maintenance of legacy material within the department for a period
- the transfer of selected records to the PRO.

A.3 A comprehensive inventory of electronic record collections will already have been developed, or be in process of development, and lines of liaison should have been established with IT or year 2000 compliance units in order to link this inventory with the results of their work. Linking these two source of information will identify those electronic records which are affected, and indicate the action which is planned by the department as a whole for the information systems on which they are stored.

A.4 In the light of this, DROs will be able to determine the possible range of options which are available for each set of records. For systems which are being replaced, electronic records may be migrated to the new system if they will still be required for operational purposes. If a decision is taken not to migrate the

records, possible options will include preparing the records for transfer to the Public Record Office (via EROS or UKNDAD) in whole or in part, destruction of the records, or perhaps archiving within the organisation for a further period.

A.5 This decision-taking process will involve undertaking a review or appraisal of the affected record collections to determine the appropriate action that should be applied, in consultation with the PRO Client Manager. The plan for undertaking this work will need to be in place as soon as possible in order to feed this work into the overall planning and review process, and to judge the resource implications. The timescales for undertaking the appraisal should be co-ordinated with information system strategy planning on Year 2000 conversion, but will now be a matter of urgency.

A.6 Where development work is being undertaken to convert information systems to Year 2000 compliance, the record manager should use best endeavours to ensure that any implications for future interpretation and use of the records are made explicit and are documented. The records collection inventory, or other form of documentation, should be annotated to show the existence of this documentary evidence.

A.7 In developing a strategy and detailed plan for record-keeping across Year 2000, reference can be made to section 5 of this guidance, which provides guidance on the requirements which should be considered when drafting a preservation strategy and includes references to the impact of Year 2000. A particular area of concern is the maintenance of non-Year 2000 compliant database records some of which may be worthy of permanent preservation. The PRO has provided a solution to this problem when the United Kingdom National Archive of Datasets (UKNDAD) was established in 1998 for the safekeeping of datasets. This service exists to preserve and provide access to databases and other structured data created by government departments. Departments intending to preserve such database records are advised to approach their PRO Client Manager to undertake the appraisal of these records and to determine if they should be selected for transfer to the UKNDAD.

## B : Outline functional requirements

### Information, document and records management

B.1 Records management is receiving new attention as a key technology for managing corporate-level information. Rather than being seen, as in the past, as merely an obligatory burden for meeting regulatory requirements, it is now being viewed as a crucial element in information management strategy for many organisations, particularly with the substantial growth in the number of electronic records and documents that form a vital part of the organisation's information resources.

B.2 *Information management* describes a range of activities aimed at the management of information as an active corporate resource. Information existing in an organisation must be actively managed in order to be drawn on as a resource, needing consistency in requirements planning, co-ordination of information strategy, and coherence in policy implementation. Records form part of the corporate memory of an organisation, consisting of information which has been validated and recorded, and represent a formal, structured information resource to be managed within a broader information strategy.

B.3 The records management system should aim to support a knowledge-intensive use of records as information resources, in accordance with the business needs of the organisation, whilst also maintaining the completeness, integrity and reliability of the record itself. Electronic records are able to unlock the knowledge previously distributed in paper files, and the disciplines and structures of records management are vital value-adding elements to this resource.

B.4 *Document management* software addresses a common organisational problem - the inability to retrieve and manage poorly structured electronic information in an efficient manner. Document management describes the ability to capture, describe and categorise, store and retrieve, share and reuse electronic documents regardless of specific format. This includes: details of paper files; word processor documents; e-mail (and attachments); spreadsheets; video, audio and multimedia documents. The software allows documents to be associated with indexes that describe the document file, such as type, author, recipient, and format; additionally, the software may track revisions made to documents and link versions together, as well as providing added security features.

B.5 Generally speaking, unless the document management system has had specific, deliberate records management functionality designed in, it is not likely to meet the full requirements in this area. This additional functionality is needed to meet the records requirements of authenticity, integrity and retention of context. EDMS products will normally offer an “archiving” function, which describes a process whereby documents can be moved off-line onto less expensive storage media. This contrasts with an electronic records management application which will provide a function to ensure that records can be exported from the application to another platform whilst ensuring that the records are still properly classified and organised, and retain their features of integrity and authenticity.

B.6 *Records management* incorporates capabilities to preserve the security, authenticity, integrity and permanent preservation of documents. The archival function within records management is concerned with “identifying, safeguarding and preserving archival records and ensuring that these are accessible and understandable”. Sophisticated electronic records management systems will therefore include not only functions necessary for document management, but also features supporting these longer-term perspectives. These include: the association of contextual and structural data within a document; the construction and management of audit trails; document version control; support for disposition scheduling; and maintenance of the relationships between records in files, file series, and the corporate filing plan.

B.7 Traditionally, government organisations performed records management in response to statutory regulations and the need for audit, the requirement for public accountability and as protection from liability. The disciplines of records management grew from these business requirements; today, the capabilities of records management systems are being expanded to include electronic records within this framework, and many organisations now look at their records repositories as valuable corporate assets rather than as liabilities.

Records capture

*Records management systems (RMS) should provide the capability to:*

B.8 Capture and store electronic records regardless of format. These types of electronic record include: text documents; spreadsheets; graphical images; presentation software products; e-mail messages together with all attachments; HTML and XML documents, together with appropriate links; desktop publications; electronic diaries; facsimile in electronic form; scanned images of paper documents and text resulting from an OCR process; voice messages and video clips; and compound multimedia documents.

B.9 Capture records that have been created as documents directly from a user application, or by a deliberate action which enters a previously created document in the records management system.

B.10 Capture records profile metadata directly from desktop and other relevant user applications as far as possible, and ensure that captured metadata is indissolubly linked to the record itself.

B.11 Capture and store profile information about non-electronic records, such as paper files, including location and access information.

B.12 Hold (potential) records in a queue for review before 'registering' in the records management system. Review may be carried out by an authorised user, who may be other than the document originator.

B.13 Accommodate the drafting process without creating a record, by allowing versions of a document to be created without automatically creating a new record on each occasion.

B.14 Capture a record as a result of document transfer from a different application or document storage system, or through a scanning process.

B.15 Capture all parts of a record, which may be in different formats, and maintain the link between the parts, without compromise to record integrity.

B.16 Offer an import/export facility which allows for the bulk loading of records of all types as a batch process, capturing as much metadata as can be supplied from source and flagging those records which require manual intervention before final integration into the system.

Structure and  
organisation of records

*The RMS should be capable of:*

B.17 Associating groups of records together, so that they can be assembled within a file category, or other record grouping for purposes of retrieval, viewing, processing or disposition. Records should be assigned to a file category at the time of capture.

B.18 Linking file categories together into functional groups or series, so that a single file category can be located within a corporate filing plan. supporting flexible naming conventions. Naming conventions may choose to be highly

structured to reflect a hierarchical arrangement, relate name elements together in a network or faceted relationship, or use a specific coding mechanism.

B.19 Allowing users to view the file structure, in whole or in part (unless there exist access restrictions), in a manner which reflects and ensures conformity with the corporate naming convention, but restricting the ability to create/edit new elements within the filing structure to authorised users only.

B.20 Maintaining this filing structure across either a central records repository or a network of distributed repositories, so that the filing structure is consistent and complete.

B.21 Allocate a disposal schedule to an element of the filing/indexing structure, which all records belonging to that element will inherit. The records management system will utilise this schedule to support maintenance and record-keeping within the system. All records are assigned to a file title on capture, and will therefore automatically acquire a retention and disposition schedule already assigned to that file.

B.22 Bring like records together so that they can be planned and managed as a group, retaining explicit links between records and the narrative context of their creation and use.

B.23 Ensure that entire groups of records can be faultlessly retrieved as a whole, with no loss of individual items, by providing complete recall of records which have been filed under a retrieved title or heading.

B.24 Separate records by type, so that they can be managed as a rational unit for accountability, operational and selection purposes.

Management and control

*The RMS should be able to:*

B.25 Ensure that a record, once 'registered' in the system, cannot be changed or altered in any way except by creation of a new version, including the application of sensitivity editing.

B.26 Ensure that all relevant original characteristics, attributes and metadata are retained in creation of a new version, and that versions are linked together for retrieval and display purposes.

B.27 Identify a document owner and apply allowed restrictions which an owner can impose upon record manipulation.

B.28 Offer check-in and check-out features for records and groups of records, so that access and version control can be audited.

B.29 Identify primary record copies, and distinguish from any other copies.

B.30 Maintain an audit trail of actions carried out on a record, details of which can be set by organisational policy.

B.31 Provide any other facilities necessary for maintaining the integrity of the record.

B.32 Provide facilities for maintaining the record in its original format, or an equivalent format which maintains all aspects of the record that are inherent in the original format.

B.33 Provide any other facilities necessary for maintaining the authenticity of the record.

B.34 Display all elements of the record together as a consistent unit on retrieval.

B.35 Manage records and groups of records according to the requirements of security markings, and provide facilities for monitoring access.

B.36 Control visibility of, and access to, records and groups of records in relation to user group categories and classifications.

B.37 Control the visibility of, and access to, functions within the records management system by user group categories and classifications.

B.38 Define active, semi-active and inactive periods.

B.39 Offer flexible search facilities on record content and record metadata, within security and access restrictions, including Boolean, extended Boolean, and probability-based search models, with relevance ranking facilities.

B.40 Enable the integration of various search facilities without compromising the integrity of the records.

Appraisal

*To support the appraisal process, electronic records management systems should have the capability to:*

B.41 Enable the allocation of disposition schedules to a category of electronic record at or before the creation of individual documents.

B.42 Link disposition schedules to an element of the corporate file plan, or other subject-based organisation of records.

B.43 Ensure a pre-defined schedule is associated with each document as it enters the system, unless an exception or override is in force.

B.44 Automatically track the disposition schedules of records, over varying periods of time.

B.45 Track, and be able to retrieve, those records which are marked for transfer.

B.46 Schedule a file or file series for destruction (at an appropriate point), permanent preservation, or review.

B.47 Schedule according to: chronological ageing, where disposition occurs after a fixed period of time has elapsed; conditionally, where disposition occurs after a particular condition is met, or an event has occurred; or a combination of both time and conditions.

B.48 Alert the records manager at the appropriate time when review decisions need to be made, and allow the records manager to confirm that particular conditions (for conditional ageing) have been achieved.

B.49 Enable selection at the document level for retention or permanent preservation.

B.50 Override selection and de-selection decisions, re-allocate disposition schedules to a group of records and allow exceptions to be made to these categories.

B.51 Identify and list those records eligible for transfer or destruction as the scheduling comes into force.

B.52 Extend retention period of individual files or record categories, which are required beyond their scheduled disposition because of special circumstances.

B.53 Ensure consistent appraisal is applied to a variety of electronic record physical types, in various formats, and including e-mail and e-mail attachments.

B.54 Link appraisal decisions made on electronic records to any related paper records of which the system is aware.

B.55 Enable both interim and final disposition decisions.

B.56 Retain audit trails which document the disposition of records.

B.57 Make global changes to the record categories and disposition categories, and alter their relationship to an element within the filing plan or subject scheme.

B.58 Control authorisation for creating, editing and deleting disposition schedule categories and record categories, and allocating to files and documents.

B.59 Reporting mechanisms to show the current appraisal state of all records within the system, and the current state of appraisal mechanisms.

#### Preservation and transfer

*In order to support the effective transfer of electronic records once selected, records management systems should have the following capabilities:*

B.60 The export of assemblies of records complete with context, metadata, and associated links from the system to a platform and application independent electronic repository.

B.61 Transfer must follow the approach outlined in sections 5 and 6 of the these guidelines.

B.62 The format of the records for transfer conform to the following transfer and preservation formats :

- PostScript
- Portable Document Format (PDF)
- Tagged Image File Format (TIF)
- Comma Separated Variable or delimited file format (CSV)
- Standard Generalised Mark-up Language (SGML).

B.63 Metadata describing folder structures, contents and relationships between documents stored in the electronic document management application should be transferred with the records, so that the metadata and the links to the document are not broken. Metadata should comprise the following:

- title and subject of the document
- author including the sponsoring organisation
- date created
- filing address or directory path or file reference (as far as electronic documents are concerned these terms should be synonymous)
- indexing information
- access permissions and controls.

B.64 Metadata should be included in a structured description file, with a separate entry for each document and the entries will be linked to the documents by the filename used to store the document. The folder metadata should also be included in the description file.

B.65 The contents of the structured description file should be capable of import to a spreadsheet or database.

## C : Relevant standards

C.1 Standards and codes of practice are still evolving and where these do exist are often the subject of revision and care must be taken to ensure that the latest version is used. A list of those which are particularly relevant are:

- *BS 7799 Code of Practice for Information Security Management*. British Standards Institute, 1995.

*BS 7799* is being revised and a new edition should be published shortly.

- *BS 4783 Storage, transportation and maintenance of media for use in data processing and information storage*. British Standards Institute, 1988.

- *BS 5454 Storage and exhibition of archival documents*. British Standards Institute, 1989.

- *PD0008 A Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (edition 2)*. British Standards Institute, April 1999.

The second edition of *PD0008* covers re-writeable media in addition to WORM media and workflow.

- *PD0009 Compliance Workbook for use with PD0008*. British Standards Institute, 1996.

- *The Principles of Good Practice for Information Management: PD0010*. British Standards Institute, 1997.

- *Design Criteria Standard for Records Management Application Functional Baseline Requirements DoD 5015.2 – STD*. US Department of Defense, November 1997.

The US Department of Defense standard on software applications for electronic records management. The standard is at:

<http://jitic-emb.army.mil/recmgt/> which also contains information on the related Certification Testing Program.

- *Dublin Core Metadata Element Set: Reference Description*. Dublin Core Metadata Initiative.

[http://purl.oclc.org/dc/about/element\\_set.htm](http://purl.oclc.org/dc/about/element_set.htm)

The principal metadata element set standard for information resources in a networked environment. The progress of Dublin Core is closely associated with the proposed architecture for supporting metadata in an IP environment called the RDF (Resource Description Framework) Metadata and Syntax specification

(<http://www.w3.org/TR/REC-rdf-syntax/>).

- *Guide for managing electronic records from an archival perspective*. International Council on Archives, February 1997.

[http://www.archives.ca/ica/cer/guide\\_0.html](http://www.archives.ca/ica/cer/guide_0.html)

- *Corporate memory in the electronic age : statement of a common position on electronic recordkeeping*. Australian Council of Archives, 1996 has been drawn on in section 1.3

<http://www.naa.gov.au/govserver/er/html/corpmemw.htm>

## Index

*The numbers following each index entry refer to paragraph numbers in the text*

- access 3.2, 3.30, 2.31
- access, preservation 5.13
- access, strategies 1.40-1.41, 1.45-1.46
- access management 2.61, 3.18, 3.22
- access rights 3.23
- acquisition policy 4.53
- appraisal, early 4.49
- appraisal, mechanism 4.56-4.59
- appraisal, new systems 4.60-4.64
- appraisal, planning 3.61, 4.46-4.50
- appraisal, review 4.59
- appraisal, software support 4.68-4.69
- appraisal, unmanaged records 4.65-4.70
- appraisal strategy 4.51-4.52
- attachments 3.49
- audit 2.15
- audit, preservation 5.43
- audit, records 4.2
- audit, technology 3.41-3.43
- audit points 3.44
- audit trail 2.51, 3.10, 3.20, 3.39, 5.35, 5.39, 6.31
- authentication 3.21, 3.25-3.32, 3.26
- authorisation 3.21
- back-up 5.21, 5.35
- business processes 2.18, 4.25, 4.52, 5.8
- capture, principles 1.22-1.25
- capture, retrospective 2.29
- capture, strategies 1.26-1.31
- CD-ROM 6.14, 6.20
- Certification Authorities 3.28
- classification 2.60, 2.51
- completeness of record 2.4, 2.19
- compliance 3.71
- compound records 2.19, 2.4
- creation 4.24
- creation, principles 1.22-1.25
- creation, strategies 1.26-1.31
- DAT 6.15
- dates 4.26-4.28
- dates, dynamic 2.58
- dates, metadata 2.49, 2.51, 2.61
- declaring as a record 2.20, 2.23, 2.59
- delimited files 6.5, 6.7
- destruction 4.75-4.77
- digital signatures 3.51, 3.25, 3.29
- disposal 2.27, 2.61, 4.71-4.77
- Dublin core 2.48
- DVD 6.16
- EDMS 2.45, 3.52, 4.17
- EDMS, metadata 5.36-5.38
- electronic signatures 3.25-3.29
- e-mail 2.7, 2.8
- e-mail, managing 3.46-3.54
- e-mail, metadata 2.42, 2.49, 3.49
- encryption 3.30, 3.33, 3.51
- Excel 2.43
- exchange of records 2.8, 3.65, 3.68, 4.38,
- exporting records 5.39
- files, metadata 2.60
- filing 2.27
- filing system 3.3, 3.6, 4.29
- folders, metadata 2.60
- formats 5.28
- formats, physical 2.49, 5.33, 6.11-6.19
- formats, presentation 6.6-6.10
- formats, software 6.4, 6.5
- GSI 1.16, 3.33, 3.51, 3.56, 3.65-3.68
- HTML 6.9-6.10
- hybrid assemblies 2.60, 3.16, 4.20
- hyperlinks 3.63
- integrity 3.21
- Intranets 1.16, 2.47, 2.9, 2.19, 2.55, 3.57-3.64, 4.17
- inventory 3.72
- inventory, contents 4.11, 4.17
- inventory, coverage 4.10
- inventory, purpose 4.3-4.6, 4.15
- IT, effect on records 1.6-1.9
- Keyword AAA 3.5

- legacy systems 4.50
- legal admissibility 3.36
- LS-120 6.18
- mailbox 3.52
- managing records, principles 1.32-1.36
- managing records, strategies 1.37-1.42
- media, physical 5.29-5.32
- metadata 2.26, 2.40, 4.17
- metadata, disposal 4.75
- metadata, preservation 5.16, 5.35
- migration 2.44, 2.56, 4.63, 4.72, 5.20-5.28
- multimedia documents 2.3
- naming conventions 2.33-2.39, 3.4
- networks, wide 2.8
- networks, local 2.6
- obsolescence 5.23
- operational selection policies 4.52, 4.55, 4.63
- paper records 2.12, 3.14, 3.17, 3.6
- PD0008 3.40, 5.17, 5.19, 5.27, 5.44, 6.24
- PDF 6.5, 6.7
- policy packages 1.16-1.17
- Postscript 6.5
- preservation, in department 5.10
- preservation, planning 5.25
- preservation, principles 1.43-1.46
- preservation, purpose 5.2-5.10
- preservation, strategies 1.47 1.51
- preservation, unmanaged records 4.44
- preservation strategy 5.11-5.20
- print to paper 1.13, 1.9, 2.30,3.48, 4.39
- procedures, developing 1.15-1.18
- procedures, need for 1.5-1.14
- profile, document 2.41, 2.47
- properties box 2.26, 2.53
- protective markings 2.51, 3.23, 4.36
- public key infrastructure 3.27
- public records 2.22, 5.8-5.9
- record collection 4.12
- record-keeping system 1.3, 1.11
- referential integrity 4.77
- requirements, record-keeping 2.18, 4.62
- retention 2.20, 2.61, 3.11, 4.42
- retrieval, information 3.2
- sampling 4.54
- scanning 2.14
- scheduling 2.60, 2.61, 3.11, 3.61, 4.43, 4.55, 4.73
- security, preservation 5.42
- segmentation 3.15
- SGML 6.5
- shared systems 3.69
- software formats 6.5
- source records 4.5, 4.76
- sources of records 2.5
- spreadsheets 2.3
- storage, environmental 5.40-5.41
- systems design, appraisal 4.60-4.64
- systems review 3.70-3.75, 4.6,4.7, 5.15
- templates 2.2.6
- text documents 2.3
- thesaurus 2.36, 2.49, 2.61, 3.5, 4.17
- TIFF 6.5
- titles, document 2.49, 2.34, 2.34
- titles, files 2.37
- titles, folders 2.37
- transfer process 6.21-6.24
- transfer, listing records 6.25-6.30
- user guidance 2.17, 2.28, 2.32, 2.54, 3.50, 3.53, 4.74
- verifying copies 5.26
- version control 2.16, 2.24, 2.51, 3.7
- virtual documents 2.10
- website records 2.9, 3.55, 3.57-3.64
- Windows 2.34, 2.38, 2.45, 2.57, 3.24, 4.17, 4.44, 4.77
- Word 2.43, 2.47
- workspaces 2.21
- WORM 5.27, 5.29
- Year 2000 3.73, 4.14, 4.9, 5.22, 5.14
- ZIP drives 6.17