



the national archives

Disposal scheduling

© Crown copyright 2004

Version 1

Author: Malcolm Todd

The National Archives
Ruskin Avenue
Kew
Surrey
TW9 4DU
United Kingdom

e-mail: e-records@pro.gov.uk

Website: www.pro.gov.uk/recordsmanagement/

© Crown copyright 2004

1	Introduction	6
2	Definitions & terminology.....	7
3	Benefits	9
4	Comparison of generic and business-specific disposal scheduling.....	10
5	Principles of disposal scheduling	11
7.	Electronic environment.....	20
8.	Getting agreement.....	23
9.	Documentation of disposal activity	24
10.	Further guidance.....	28
11.	References.....	29

[this page is intentionally blank]

1. Summary

Disposal scheduling is an important aspect of establishing and maintaining control of corporate information and record resources.

Not all information can be retained indefinitely: in central government the provisions of the Public Records Acts mean that only those records selected for permanent preservation can be legally retained and custody of those normally has to have passed to The National Archives by the time 30 years have elapsed from their creation.

Determining the *final* disposal of *categories* of information (and possibly also *interim* stages where the final disposal must for some good reason remain indeterminate for the time being) is the normal manifestation of disposal schedules.

As well as representing an asset, information can also impose liabilities on the organisation holding it and the risk of this requires proper and robust management. Getting this balance right represents deciding at the corporate level the answer to the question “*How long is the information required?*”. There may be tensions between conflicting needs that require resolution.

At the time of writing (early 2004), there are further cogent reasons why many organisations need to address these issues. In particular the Data Protection Act 1998 and Freedom of Information Act 2000 have imposed new and more stringent duties on public authorities as regards proper management of personal data and records. Public bodies must take steps to prevent the *ad hoc* disposal of records and ensure that final disposal of records is in accordance with agreed policies and the schedules formulated to implement them.

This is particularly important in the electronic environment where uncontrolled copying of information can very easily take place and frustrate even the most stringent scheduling exercise, requiring an increased stress on implementation and compliance with official schedules. In addition, fully-fledged electronic records management offers a great deal to make this process more orderly, more automated and more secure than has ever been possible in the past at the same time as delivering other substantial business benefits to organisations.

Bearing these points in mind, this guidance gives pointers towards establishing how long information is required in different core business scenarios and also introduces a series of further guidance (already published) from The National Archives on commonly held public records where generic disposal periods can normally be identified across government.

2 Introduction

2.1 Aims and intended use

The aim of this publication is to set out the principles behind records disposal scheduling so that records are kept for as long as they are needed, all legitimate considerations having been considered and balanced. As tools to assist in this, it draws attention to existing generic schedules and give some pointers to the development of schedules that are not covered by the latter.

This guidance entirely supersedes Records Management Standard 5.1 *Disposal scheduling* (published in 2000).

2.2 Audience

The intended audience are primarily central government departmental and local authority records managers, although the principles may be of application outside these sectors and may be of some use to explain the concept to colleagues, including senior managers and auditors.

3 Definitions & terminology

3.1 Disposal, retention, disposition, review

These terms are different aspects and terminology of essentially the same concept. This guidance prefers the terminology “disposal” over “retention” as most consistent with archival practice in the electronic environment and the professional literature.

- “Disposal” in this context does not just mean destruction: it embraces any action taken [or yet to be taken] to determine the fate of records including transfer to a permanent archive. In some jurisdictions, the word “disposition” is used to avoid the negative overtones of the word “disposal”: this is neither the usual nor the preferred UK usage in this context.
- Where it is not yet possible to determine the disposal of the records, they may be scheduled for “Review” at a later date¹. This type of review involves bringing forward the records at a later date at which it is hoped to determine their final disposal.
- “Retention” usually means the length of time for which records are to be kept. Thus it normally represents and will be expressed as a disposal period².

3.2 Schedules

The main administrative use of schedules is to *group / list* (or “schedule”) categories of records to be kept according to the rule contained in that schedule and associate them closely with the rationale for applying those disposal criteria to the records contained in the list. In conventional registered file series, it will normally be the series that is contained in the schedule. As well as being administratively convenient, this provides maximum transparency and auditability to the disposal of records.

A disposal schedule will normally be a combination of a trigger, a period of time and a disposal action to be taken at the end of that period. In some circumstances (particularly in the electronic environment), a schedule will be formed of more than one stage: see section 6 for more details of this.

Typical triggers will be the closure of folder / folder part, the opening of a folder / folder part or - occasionally - the last addition to a folder / folder part where for some reason it has not been possible to follow best practice in closing them. It should be remembered that the Public Records Act 1958 assumes that archival records must be in the custody of the National Archives or another approved Place of Deposit by the time they reach 30 years from creation [s. 3(4)].

¹ review for other reasons, such as determining the current sensitivity of the content of the records is a separate process and is not covered here. Review in the sense of appraising the records for archival value is on the other hand a type of disposal activity since it will determine which are to be retained, which destroyed and which transferred to archival custody. Techniques for this are outside the scope of this guidance which treats them as a generic process mostly identical to appraisal for non-archival purposes

² the terms are broadly interchangeable

A disposal action is normally a “destroy”, “transfer to archive” (decomposing in the electronic environment to “export” and “destroy” actions) or “review” action³.

3.3 Unit of management: normally the folder

Typically, the unit of management for most records management purposes is the folder (‘file’) or folder part⁴. Disposal may be managed at a higher level: typically this has been understood and administered in the paper environment at registry series level. Mapping this into the electronic environment requires understanding of business classification scheme design, ERMS disposal functionality and the ‘class’ entity derived from the MoReq standard⁵.

It is particularly important that the integrity of the folder aggregation is observed strictly for disposal activity including in the electronic environment⁶ and *ad hoc* removal of records from folders (sometimes known as “weeding”) is not practised⁷. One of the purposes of disposal scheduling is to demonstrate transparently that disposal has been carried out according to agreed criteria and not according to the personal preferences of individuals.

There will be circumstances, especially in a physical environment, where records, which are not in conventional formats may not easily be aggregated into folders (maps, plans, videotapes, analogue films, etc.). These still require to be brought under the control of disposal policy using a disposal schedule in an appropriate way, i.e. that describes their content, their format and arrangement and allows for their timely disposal.

With records in digital formats where there is an electronic records management solution in place, it should be possible logically to contain any object within folders (including references to physical objects not actually contained within the object repository of the ERMS). Section 7 contains further guidance on what options may be available where this is not the technical environment for electronic records and how disposal may be managed in these circumstances.

³ this means, effectively, that “review” is being used as a term of art as it is not a disposal action at all: see second bullet point on previous page

⁴ when discussing the electronic environment, this guidance uses the terminology and entity model of the *Functional requirements for ERMS* [2002 revision]. This is contained in the *Reference document* [Vol. 3]. Thus a folder part is only a segmentation of folders by time and should not have a separate schedule / disposal rule applied to it, although the execution of the part will happen at different time if the trigger is related to the *part* metadata

⁵ Available from: <http://www.cornwell.co.uk/moreq>

⁶ the continuing importance of the folder in the electronic environment, apart from disposal management, is to provide an intuitive user interface and the ensure the consistent application of metadata to the contained objects

⁷ with the specific and limited exception of non default **record_types** designed to facilitate DPA compliance and explained in section 7

4 Benefits

The main benefits from robust and comprehensive records scheduling are:

- to maximise the retention and ready availability of 'smart' information for the conduct of effective public business, maintain the corporate memory and avoid 'reinventing the wheel';
- to comply with specific legal and regulatory requirements including the Freedom of Information Act 2000 (including the *Code of Practice* on records management made under s.46), the Data Protection Act 1998 and the Public Records Act 1958;
- to support accountability through the retention of records (including the availability of archival records of genuine historical value);
- to demonstrate that the disposal of information assets has been carried out according to an agreed policy;
- to translate the aspirations of the organisational records management policy into direct consequences for categories or series of records and make the disposal decisions and execution with proper authority and auditability;
- risk management: to avoid the costs and potential liabilities of retaining information the organisation does not really need and which is likely to result in legal discovery actions and possible involvement in third party disputes⁸; and
- to minimise the administrative overhead to the organisation.

⁸ public bodies have a general duty to comply with the administration of justice. This guidance does not argue contrary to this duty but it does not imply that all government organisations need to retain all information 'just in case' it may be required for this purpose. The main points are: the proper consideration of the requirement and there may be cogent legal and regulatory (as well as business) reasons for *not* retaining information, plus that it is a legitimate legal defence in some circumstances to have disposed of material appropriately

5 Comparison of generic and business-specific disposal scheduling

The National Archives has published guidance on the retention of generic records (i.e. commonly held record types encountered across government). The schedules already produced are listed in section 11. These have been produced by examining the cross government requirement and any legislative / legal / regulatory mandate to retain information for accountability to the courts, auditors and other authorities. This guidance covers other records not covered by these generic schedules and gives authorities the tools to develop their own disposal schedules.

There may occasionally be special circumstances where the business of an organisation may justify keeping records covered in the generic schedules for periods at variance with those stated: these will mainly be where the organisation has a cross-government responsibility for the activities of other departments, there is an archival interest identified and / or there are regulatory or law enforcement functions involved. It is suggested that these variations are recorded as such in the relevant documentation and where required agreed by internal and external stakeholders.

6 Principles of disposal scheduling

6.1 How long is “as long as needed”?

As mentioned in the introduction, the key is balancing a series of considerations about disposal that may well be in tension to arrive at a considered judgement on how long the records are required.

The following paragraphs draw a distinction between the various business needs for the information and the considerations that may override or reinforce them.

6.2 Supporting the organisational / operational business need

6.2.1 Business benefits

This amounts to keeping the *smart* information, bearing in mind that the business purposes of information may include ones not closely related to the purpose of creation.

This has much commonality with “Knowledge Management” initiatives. Although in the electronic environment information contained in records can be accessed from a variety of searches, the uncontrolled retention of ephemeral information can lead to the proliferation of false drops in the results; too many ‘hits’ can often be as bad as too few.

There is much sound theory on the reuse and repurposing of records through the continuum in professional archival literature, particularly on the University of Monash website⁹. This expounds the notion of identifying the various uses including the archival value before the point of creation, something that comes into its own in the electronic environment (see section 7 below).

In order to safeguard the relatively few important records it is essential to distinguish them from the many more ephemeral ones.

Specific thought needs to be given to:

- Vital records, generally understood as those without which the organisation cannot function¹⁰;
- Emergency records essential to the immediate recovery of the organisation from a major disaster (it should *not* be assumed that these are automatically the same as those in the previous category)¹¹;

⁹ Records Continuum Research Project at: <http://rcrg.dstc.edu.au/>

¹⁰ See guidance on *Business recovery plans*, TNA, 2002 accessible from: <http://www.pro.gov.uk/recordsmanagement/standards/default.htm>

¹¹ vital and emergency records may well be deserving cases for the creation of surrogate copies (e.g. for holding off-site) though it follows that these must themselves be controlled and subject to proper disposal management

- Archival appraisal, including any operational selection policies for Public Records¹².

For the rest, being able to retrieve, store, sustain, preserve the important information and records and the prioritisation of resource allocation to support this should be the priorities once the considerations in the next section have been taken into account. Some records might have precedent value, for instance. Others might be important for supporting evidence-based policy making.

All this requires awareness of for what purpose records might be retrieved by the business. This may seem a facile point but it can be overlooked: many records are retrieved simply for their information content, others for the auditing of the business function, formal [e.g. complaints] review, etc. and these purposes may indicate quite different time periods. See the next section for more discussion of this.

6.3 Supporting legislative and regulatory obligations

6.3.1 Legal compliance benefits: Freedom of Information Act 2000

This subject is thrown into very sharp relief by duty to confirm or deny the holding of information in section 1 of Freedom of Information Act 2000 (“FOIA”). In response to a valid FOIA request, from 1st January 2005, Public Authorities will have either:

- To **retrieve** information (and in most cases confirm or deny its holding), and **release**; or
- To **quote** a valid exemption (applying the harm test in many cases).

Disposal schedules are a very important part of accounting for the legitimate absence of information under FOIA. Demonstrating to requesters, the Information Commissioner or the Information Tribunal that disposal decisions have been made and implemented following due process will defend legitimate public sector records management activity from undue criticism under the FOIA régime. In particular it should serve as a defence against a charge under s.77 that a record has been destroyed with the intention of preventing disclosure in response to a request.

Section 46 of the FOIA provides for the issuing of a *Code of practice* by the Secretary of State on records management and the current version of the Code acknowledges fully the need for proper disposal management.

One of the most radical changes that will be brought about by the FOIA will be that information that has not been identified for permanent preservation will become far more widely accessible and yet may subsequently be destroyed because it does not warrant permanent preservation¹³. This will put public sector disposal management under more scrutiny than ever before. Documentation of disposal activity at the policy, schedule and folder (very occasionally record) level will be particularly

¹² disposal may also be affected by sampling techniques of selecting from case file series. This is outside the scope of this guidance but obviously has to take place before the disposal of the entire series. For further information, refer to TNA guidance on sampling cited in *References*, section 12.

¹³ i.e. prior release of information - either proactively or in response to a request under FOIA – does not *of itself* mean that the information should not be destroyed.

important to account for records that cannot be confirmed as present in response to a request, a complaint to the Information Commissioner or an appeal to the Information Tribunal.

6.3.2 Statute bars on release and retention of information

Exceptionally, there are a number of specific statutory obligations on public authorities to retain, withhold or release records.

In practice a number of the **statute bars** on disclosure have been or are in the process of being removed as part of the preparations for FOIA implementation but public authorities should be aware where they hold information that is the subject of a statute bar to ensure the legal obligation is complied with and formulate disposal schedules accordingly.

For public records, a statute bar on access has no effect on archival selection and transfer unless the bar is explicitly worded to that effect.

6.3.3 Public Records Act 1958

The Public Records Act 1958 imposes a duty [s. 3(1)] on public record bodies to make proper arrangements for the identification, safeguarding and transfer of records of historical interest to The National Archives. This is to be done under the supervision of the relevant TNA client manager [s. 3(2)]. Section 3 (6) demands the disposal of records not selected for preservation either by destruction or by other means approved by the Lord Chancellor. There is no general waiver for records covered by a statute bar.

The following points should be considered when ensuring compliance with the Public Records Acts in disposal scheduling activity:

- The earlier identification of archival records is particularly important with electronic records and is implied in any case by the notion of the records continuum (see also section 7 of this guidance);
- The Grigg system implies a regular system of first review typically between 5 and 10 years of folder (file) closure which is not as widespread as it once was;
- There is an increasing interest in a more 'macro' approach to records appraisal, particularly for electronic records, and this is being considered at the time of writing by a National Archives review of the public records appraisal system;
- It is less universally accepted that the only records likely to be of historical value will be those required for business purposes for longer than 5-10 years;
- The TNA Acquisition and Disposition Policies will have consequences for disposal scheduling. Schedules in departments must be consistent with them. Many departments and their records will be included in Operational Selection Policies formulated within the framework of the Acquisition Policy.

From 1st January 2005, the access provisions of the Public Records Acts will be completely replaced by those of the Freedom of Information Act 2000. There is no

change to the requirement for records selected for permanent preservation to be transferred to TNA or a place of deposit by the 30 year point.

6.3.4 Data Protection Act 1998

Many records will contain personal data of some kind. This has to be processed in compliance with the Data Protection Act 1998. Some of the principal differences between this Act and its 1984 predecessor are highly relevant to disposal scheduling:

- The new definition of all operations, including simply **retention** of data, as “processing”¹⁴;
- The *fair processing provisions* in Schedule 1 are completely independent of the data subject access provisions in Part 2 and impose duties of fairness and proportionality that apply far more widely; and
- The extension of the data protection régime to many manual records.

In practice there are many highly significant implications for disposal scheduling arising from the DPA and records managers compiling disposal schedules will need to have a thorough knowledge of the Act and the guidance of the Information Commissioner on its application. Some of the more significant ones are outlined here: as a bare minimum departments will have to ensure that disposal schedules are consistent with the *Fair processing principles* in Schedule 1 of the DPA. Legal advice may also be required in some circumstances.

- The DPA 1998 reinforces the imperative to dispose of information in a timely, orderly manner and not to retain personal information without good reason. In general this implies a presumption that once the legitimate business use for the information has expired - or continuing to retain it has become disproportionate to the processing¹⁵ – processing should cease, i.e. the personal data should be disposed *unless a further approved purpose of processing applies*;
- Personal data cannot be disposed outside the EEA unless the destination has similar legal protection for it¹⁶ or a contract provides equivalent protection;
- In general, the personal data will be an integral part of the record and will have to be managed as part of it, meaning that the disposal of the record or record assemblies will have to take into account the processing of the personal data. Personal data occurring within individual records cannot be altered or removed without undermining the integrity of the record and **this should not be attempted**¹⁷ There are specific requirements in the *Functional requirements for ERMS* [2002 revision] designed to promote DPA compliance without undermining unduly the integrity of records aggregations: This is covered in section 7 of this guidance.

¹⁴ S. 1(1) includes the wording: “*processing*”, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data.’

¹⁵ The third data protection principle: ‘*Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed*’

¹⁶ this excludes, for example, the USA which does not have an analogous data protection régime

¹⁷ this does not preclude the protection of personal data by extraction techniques when giving access to the records for other purposes. In general however, records management requires that to be accurate a record of an event in the past does not have personal data contained within it updated and this is consistent with the fourth data protection principle

6.3.5 DPA exemptions for research; ‘compatible purposes’

The only rider to add is that there is one relevant exemption - *Research, statistics and historical processing*, contained in s. 33 which may justify continued processing [retention] of personal data beyond the primary and original business purpose¹⁸. This exemption is particularly valuable for the retention of archival records and it should be noted that archival preservation has been accepted by the Information commissioner as a valid special purpose for use in Notification under s.18.

6.3.6 Consistency with other openness legislation

There are other statutory provisions requiring the release of official information, such as the Environmental Information Regulations, local government legislation and provisions affecting the National Health Service.

These measures will have their own interfaces with the DPA and will not generally have such widespread implications for disposal scheduling as the FOIA owing to the lack of records management codes of practice under them. However, there will be some issues to be addressed, for example:

- There will be important provisions governing how the balance works between access and privacy; and
- As mentioned elsewhere in this guidance, control of copies and surrogates will be important. Use of electronic surrogates, e.g. to provide internet access to local authority committee minutes requires control.

6.3.7 Limitation Act 1980

The Limitation Act 1980 prescribes time limits for the commencement of different categories of legal actions, such as recovery / restitution.

This has an important effect on the retention of some government records: after all Government has to manage the risk of actions arising from contracts and duties of care to employees, citizens and so on and retaining records plays an important part in this.

The caveat needs to be entered that any period specified in the Limitation Act should be validated against other requirements before being assumed *automatically* to match the correct disposal period. In many cases, where records have more than one business purpose, the one specified in the Limitation Act will be the longer but this should be checked:

- Public Authorities may have duties of care established in caselaw that go beyond explicit statutory requirements;

¹⁸ Noting clause 2 of Schedule 1 (Fair processing principle no. 2): *‘Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes’*. This needs to be read with the other fair processing principles. Actually establishing what is a compatible (or rather a ‘not incompatible’ purpose) may require legal advice.

- A law enforcement body will typically only be able to initiate court action *within* the limitation period and there *may* not be any persisting business need for the records beyond that. [This will need to be verified];
- Some statutory authorities have powers to seize information in the course of specific inquiries; whether this is a viable alternative to retaining other more general regulatory material will need to be judged on a case-by-case basis.

Further information on many of the implications of the Limitations Act for government departments is contained in the 12 generic disposal schedules listed in Section 11.

6.3.8 Other legislative requirements

Other important legislation relating to the policy and operational remit of the public authority will probably have direct requirements for the retention of records. For example, Companies Act 1985 and the Finance Acts.

Some statutory obligations to retain information should be considered in the light of other legislation that may otherwise impact on its disposal. A number of them date from obsolete provisions that have not been repealed and may not make a lot of obvious sense. Legal advice and the advice of The National Archives may be necessary.

6.4 Supporting cross-government data sharing initiatives

The Department for Constitutional Affairs has public policy responsibility for data sharing initiatives in central government. This has begun with work on data sharing protocols to increase the transparency of data sharing and build public trust. How this policy agenda will develop in the longer term is not yet clear: it is possible for example that a clear business case may emerge for the sharing of records between [central] government departments perhaps supported by some common organisation of common administrative records such as personnel records. This may have an impact on disposal scheduling across government.

6.5 Organisations with legislative and regulatory exemptions on the release and holding of information

This guidance is generic. There will be scenarios where some of it may not apply, for example:

- Defence, security, law enforcement and other bodies where exemptions exist from FOIA; or
- Analogous situations where there is exemption from some of the provisions (i.e. data subject access and – very exceptionally – the data protection principles themselves) of the DPA 1998.

6.6 Link to business classification schemes

Disposal management will depend on the régime in place for the organisation and classification of records. For further information on the main methodologies and the main advantages and disadvantages of each, refer to the TNA publication *Business classification scheme design*¹⁹.

Some of the practical implications of this are discussed in the next paragraph, but there are wider implications also:

- In a strict functional scheme, a clear policy decision has been taken that the value of the **function** (in business, cultural and accountability terms) should determine the disposal period, rather than the content of any of the records²⁰.

This has far reaching consequences for the monitoring and maintenance issues discussed in Sections 8 and 9 of this guidance: there is no sense in such a fundamental principle being undermined by significant fine tuning.

6.7 Striking the right balance

Information represents a vital corporate asset and needs to be managed so that the 'smart' information is retained and ephemeral information is disposed of.

Information can also present a liability. For example breaches of security could potentially occur at any time in the life of the records. Further, there are risks of legal discovery. Whilst not so onerous as in the United States, where parties to legal disputes in receipt of subpoenas have to pay the professional costs of the opposing party's legal team, the risk is still real²¹. Third party disputes (especially where there is no clearly defined business benefit to retaining the information in the first place) could be particularly onerous.

Balancing these assets and liabilities requires a risk assessment approach to balance the two against one another. Getting this balance right is particularly important with sensitive information: both in the sense of the content generally and sensitive personal data (as defined by the DPA) which may be incidental. Controlled, auditable and documented retention and destruction are essential. It is important to arrive at agreed disposal periods as early as possible, ideally before the creation of the records. This will reduce the resources required to be expended in file-by-file review. Further guidance on methodologies of business classification / records organisation and their potential for reducing this to a minimum is provided in the TNA publication: *Business classification scheme design* already cited.

¹⁹ see *References* in section 11

²⁰ such an approach is commonly supported by different statutory frameworks than those persisting in UK government as discussed in *Business classification scheme design*, pp. 22-23. Sheppard and Yeo (*References*) provide a useful summary of how these can be related to the development of archival science since the middle of the last century. The full articulation of the continuum theory demands that the functional analysis takes into account the archival, cultural and accountability as well as the business value of the **function**. See the Records Continuum Research Project material at <http://rcrg.dstc.edu.au/>

²¹ Sampson, (see *References*) covers the full effect of this situation in the United States. Apart from this difference it also provides a useful guide to the contribution to risk management offered by disposal scheduling

Owing to the challenges (and management costs) of preserving electronic information across platform and software migrations mean that there is a compelling need to identify disposal requirements for electronic records earlier than has often been the case with paper. Section 7 examines some other important considerations for disposal scheduling in the electronic environment.

6.8 Staged disposal schedules (including review stages)

Sometimes staged schedules are required to control the passing of records from one phase of their life to another. Examples might include:

- Where the final disposal cannot yet be determined and will require review²²;
- Where in the paper environment the final disposal can be determined but a further retention period is required before its execution²³;
- Where records (probably electronic records) may be passed from one technical environment or custody to another but still have other continuum phases to enter at later stages. Examples might include where electronic records are presented to websites but retained after their removal from the public web domain or are exported to archival custody whilst a copy is retained for a period in the originating system.

In these cases, the point of the two-stage process is to ensure the passage of the records to the next stage of their disposal is actioned and the final disposal is determined. This is particularly important where there is normally no visible clue to the existence of the records, as with many electronic records.

6.9 Secure, auditable and final disposal

The methods of final disposal will vary with the sensitivity of the records, their format and the disposal action.

6.9.1 Destruction

Destruction actions on physical, paper records may require cross-cut shredding and / or burning in a secure environment. The following methods are recommended as minimum requirements:

non-sensitive (unclassified)

Ordinary rubbish bins should only be used for clearly 'public domain' material. Although FOIA will greatly increase the extent of releasable information, much will still contain personal data. Records may consequently require tearing into small pieces and placed in rubbish bins / sacks for removal by an approved disposal firm;

²² the content of records may be reviewed for other purposes (e.g. sensitivity purposes) and there may well be an overlap, but the stress in this context is on the determination of disposal requirements

²³ in the electronic environment this process decomposes into the reallocation of a separate schedule that was not previously envisaged, so it does not fit the staged schedule scenario in this environment. Where this applies to physical records, some 'bring forward' system is required

*restricted*²⁴

Waste should be strip-shredded and placed in paper rubbish sacks for collection by an approved disposal firm

confidential

Waste should be crosscut-shredded and placed in paper rubbish sacks for collection by an approved disposal firm. The material should be pulped or burnt.

secret and top secret

Waste should be crosscut-shredded or disintegrated using a grille size no larger than 6mm and placed in paper rubbish sacks for collection by an approved disposal firm. The material should be burnt.

6.9.2 Archival transfer

Physical transfer of physical records to a permanent archive should be in accordance with the procedures for transferring custody to that repository (those relating to the transfer of Public Records to The National Archives are contained in the *publication Preparation of records for transfer to the Public Record Office*). [Electronic records require different procedures that are covered in the next section].

6.9.3 Control of surrogates

Any record surrogates (including electronic and microform surrogates) should also be scheduled and controlled. The important point is that procedures need to be in place to ensure that the disposal criteria in the schedule have been implemented properly: i.e. records that are still retained are usable and records that have been destroyed are not accessible because they no longer exist.

6.9.4 FOIA 2000 s. 75 offence

The Freedom of Information Act 2000 s. 75 introduces an offence for the wilful destruction of information that is the subject of an FOI request. This necessitates the institution of a proper procedure to ensure:

- that this type of *ad hoc* destruction does not happen; and
- that auditable, authorised disposal of records in accordance with proper schedules does occur; but
- can be [temporarily] interrupted if a request for an affected record is received.

²⁴ the protective marking definitions used here are those from the 1992 revision of the Cabinet Office's *Manual of protective security*

7. Electronic environment

Provided a fully functioning electronic records management solution is in place, there are opportunities for implementing the above principles slightly differently: whilst the principles remain the same, the potential for realising the benefits of them is far greater. For example, an ERMS has the potential to administer disposal systems more globally, lending an unprecedented degree of transparency and auditability to the disposal process as it should become more obvious how policies have been implemented through the system:

- through the creation of rules within an ERMS that can be reused and amended more efficiently;
- through the rule base (scheduling) and disposal execution requirements in the TNA generic *Functional requirements for ERMS* [2002 revision] including the disposal conflict resolution requirements A.4.39 – A.4.43 and the inheritance principle;
- through facilities for the presentation of business classification schemes and the administration and execution of disposal schedules through them in the electronic environment.
- through facilitating different approaches to review of electronic records;
- through the expression of multiple staged schedules and automation of passing from one phase to another [non-mandatory requirement A.4.13];
- through migration (in the sense of taking records to an offline system) requiring far more multi-stage disposals; typically meaning an export and possibly a deletion action);
- where for preservation or sustainability reasons it may be appropriate to build the production of access surrogates into the disposal régime and control it using the same business rules.

7.1 Non default *Record_type* requirements

The generic *Requirements for ERMS* [2002 revision] include specific and limited functionality to promote the better management of personal data without disproportionate undermining of fundamental principles of records management.

For a very restricted type of document, it is permissible to dispose of [destroy] certain records within a folder (non default *record_type* documents) in advance of the disposal of the folder itself. The scenario envisaged is that of a personnel file where the contents should clearly form part of the same aggregation but there are records of both extremely long term (e.g. superannuation) and much more ephemeral value (e.g. annual performance reports / disciplinary).

This relaxation of the aggregation principle is solely designed to promote DPA compliance and is not envisaged to be more widely used. Extending it could undermine the integrity of records aggregations and undermine the operation of record systems in accordance with national and international standards.

7.2 Methods of destruction of electronic records

Deletion should ultimately mean the **complete destruction** of the electronic record (and is the electronic equivalent of secure disposal of physical records). This implies rendering them non-recoverable even using forensic data recovery techniques.

In practice, deleting an instance of an electronic record in most technical environments merely removes an operating system or application link to the object and it is not actually removed when the same storage medium space has been reused several times over.

The Data Protection Act requires that information that is no longer required should cease to be *processed* (for a discussion on the wide meaning of the word 'processing' under the DPA, refer to page 14 of this guidance). The Information Commissioner has consistently held that this means that reasonable steps should be taken to ensure the information is not retrievable by normal methods, normal in this case including restoring using back up tapes etc. (see below). It is the view of The National Archives that removing the normal means of retrieval is sufficient in most environments provided that back ups are also properly controlled to prevent them frustrating official retention policy.

Accordingly, the *Requirements for ERMS* [2002 revision] do not specify the 5 x overwriting of destroyed content as in the US Department of Defense ERMS requirement²⁵, though this may well be required in a high security environment in UK government. Security standards in some departments may lead to them adopting something closer to the DoD requirement in this area.

The other implications are that:

- effective copy control of all kinds is essential, involving both functionality within the ERM solution; and
- procedures must be present to ensure that information captured in the solution or too ephemeral to justify capture there is deleted promptly from the creating client, personal or network drive.

7.3 Back up routines

It is important to ensure that IT departments and / or external IT providers are not frustrating the proper implementation of official disposal schedules by their back-up routines. Altering the rotation and re-use of back up tapes and other procedures can often resolve such potential problems. It is important that IT managers are aware of the importance of complying with official disposal schedules. Back up clauses of outsourced contracts may require to be reviewed.

7.4 Hybrid environment management

Reference should be made to the optional module on the physical / hybrid environments in the *Functional requirements for ERMS* [2002 revision]. Particular attention is drawn to [non-mandatory] requirement B.3.31 and the manner of its implementation. If this requirement is not supported, a separate procedure will need

²⁵ this is sometimes called 'expungement'. The DoD requirement is accessible from: <http://jtc.fhu.disa.mil/recmgt/>

to be introduced to ensure that the physical objects outside the ERMS are actually destroyed.

7.5 Controlling disposal of undeclared documents in an integrated EDRM solution

Not all electronic documents will be declared as formal records within an EDRM solution. Some thought should be taken to ensure that undeclared documents are not retained indefinitely.

Logically, if users have been trained correctly, the undeclared documents should be ephemeral and deletion possible after a period significantly shorter than that identified as the disposal period for the records. The *Functional requirements for ERMS* [2002 revision] *Document management* module contains requirements B.2.19 and B.2.20 to support this. Which of the options are implemented may depend on business rules and user behaviour.

7.6 Managing disposal without full ERM

Outside the ERM environment disposal management is more complex and potentially problematic: indeed imposing structured, audited and transparent disposal in line with organisational policies is an important part of the ERM business case. In addition, there will not be the same potential for aligning the disposal criteria with the business classification scheme and administering both in an integrated and automated manner.

The National Archives has produced a number of guidance products relating to the management of electronic records and documents where there is not necessarily a fully functional ERMS in place:

- *Guidelines on developing a policy for managing email*
- *Managing electronic documents using MS Office 97 on a local area network;*
- *Guidance for compiling an inventory of electronic records collections;*
- *Evaluating information assets: appraising the inventory of electronic records;*

There are some environments where this is likely to be particularly demanding and complex, such as websites and databases / datasets.

Further pointers to disposal management in these technical environments is / will be included in specific guidance products²⁶. In addition, there are a number of general principles that can assist with working out strategies for tackling this problem:

- Achieving copy control by business rules about duplication;
- Procedures for deletion of objects no longer required or captured into record aggregations;
- Consideration could be given to IT departments running data purging scripts to dispose of objects from network drives and / or email boxes (though it must be stressed these must be thought through and in line with organisational policies and procedures to ensure the proper capture of records).

²⁶ *Managing web resources*, TNA 2001; guidance on database management is planned for issue during 2005

8. Getting agreement

Main stakeholders

There are a number of stakeholders who may need to be consulted about disposal schedules for records. Examples include:

- [Operational] business managers;
- Senior management;
- IT managers (for reasons explained in chapter 7 as well as regarding records of IT business activity with particular reference to the issue of back ups and final disposal);
- Relevant regulatory bodies;
- [For Public Record bodies] the TNA client manager (operational selection policies formulated within TNA's acquisition policy are also subject to public and professional consultation stages);
- There may sometimes be a need to consult other public bodies (e.g. central government bodies holding records in common may need to communicate to avoid unnecessary duplication or to assist in the efficient handling of FOI requests);
- Legal advice may be required to evaluate correctly the considerations outlined in section 6.

This consultation process requires careful documentation, particularly formal sign-off recording the agreement of the parties to the disposal period decided upon. Discussion of methods of documenting this process is in the next section of this guidance.

9. Documentation of disposal activity

Section 6 of this guidance has already stressed the importance of transparency in the cascading down of an organisation's records management policy, through disposal schedules as a vital part of demonstrating compliance with the Freedom of Information Act 2000.

There are several key pieces of documentation of this process:

1. The corporate records policy;
2. The disposal schedule[s] itself [themselves]. A list of what a schedule may contain and a sample of how it might appear is in the *Annex* to this guidance;
3. Documentation of the process of agreeing the schedule[s] and schedule sign-off;
4. Records of records [or records *series*] review activity²⁷;
5. System audit trails in ERMS and registry / tracking database applications;
6. TNA or other transfer documentation (where applicable) recording the transfer of records to archival custody.

Additionally, there is other documentation that may be required to account for records:

1. Registers, docket books controlling the creation, movement and perhaps recording the disposal of physical records;
2. Database tables controlling the creation, movement and recording the disposal of physical records;
3. Disposal certificates recording the final disposal of electronic or physical records;
4. Electronic metadata stubs [normally at folder level] left by some ERMS solutions after the disposal of the records in accordance with [non-mandatory] TNA generic requirement A.4.71.

9.1 Form of disposal schedules

It is now difficult to prescribe a single model for schedules, not least because in the electronic environment the schedule will probably be deemed to be the rule constructed in the ERMS and linked to other documentation by an identifier code. ERMS functionality will normally support the production of reports on the schedules existing in the system.

²⁷ this is important to avoid allegations of ad hoc review such as have proved so controversial in the *Heiner affair* in the Australian state of Queensland

A disposal schedule or closely-associated documentation needs to contain the following minimum information:

- Citation of the authority for the schedule including the corporate records management policy, business unit[s] and any applicable TNA operational selection policies;
- Clear identification of the records series / classes covered and any division principally responsible for their creation or the use and, against each, the disposal trigger, period and action;
- Some thought needs to be given to “clear identification” to avoid ambiguity.
- Formal sign off by appropriately responsible persons from the records management function, business unit[s] and – for Public Record bodies – the TNA client manager.
- Non-organisational business classification schemes require a far more high-level corporate approach to schedule agreement and documentation than previously as there may be no identifiable ‘owner’ or ‘user’ other than the organisation as a whole. An appropriate and senior body will need to be identified to agree and sign off schedules in these circumstances.

It is recommended in general that modern disposal schedules are corporate documents rather than applying to single business units. This is especially important where there is a functional classification scheme and / or records sharing is very widespread (as it should be in the electronic environment).

A tabular format will be the best for most applications and for large organisations a database may be the most convenient. This should ideally be designed to include any multiple stage disposal schedules.

Sign-off will have to be by an appropriately senior body, although there will have to be discussions with business units before this.

9.2 Exception handling and documentation

Very occasionally, there will be exceptions made to disposal schedules applied to individual or groups of records. Examples include:

- Disposal (destruction) ‘holds’ placed on records owing to litigation, Inquiries, FOI requests, etc.;
- Disposal conflicts arising from classification scheme administration (see Functional requirements A.4.39 – A.4.43);
- Temporary backlogs in appraisal activity.

These clearly need to be kept to a minimum and resolved as quickly as possible. This means documenting them, the reasons for them and bringing them forward for resolution.

If a 'macro' approach has been taken to scheduling, e.g. as can be implemented within an ERMS provided that is the policy and the business classification scheme is suitable, external events may trigger the reassignment of retention schedules at a finer degree of granularity. E.g. a legal case achieves some notoriety or goes to appeal, long term health implications emerge in a particular occupational sector.

This may not necessarily call into question the retention criterion set for the class ([sub-] series) as a whole, although it does provide an opportunity to review this and this is recommended if it becomes a common occurrence. Rather it should be viewed as refining the allocation of disposal periods and demanding that for some records they are set at a lower level to keep pace with the emerging business requirement. This should bring the 'exceptions' back within the disposal schedules and the records management policy.

ERMS packages should readily support the inheritance of disposal schedules from a class to descending classes and folders as well as the possibility of overriding these at a lower level. Some (those meeting the non-mandatory retrospective inheritance requirements A.4.22 & A.4.23) will also recognise these exceptions when the high level schedule is replaced. All will provide a degree of auditability to disposal scheduling [re]allocation activity.

Disposal policy needs to be implemented consistently and schedules implemented promptly, particularly if it is to be demonstrated that records that have requested (e.g. under FOIA) have been disposed of according to due process and not owing to *ad hoc* decisions.

9.3 Monitoring and revision of disposal schedules

Disposal schedules should be reviewed regularly to ensure they are still working correctly. This is a necessary part of monitoring the performance of records management policies and procedures generally.

The business need for types of information may decline or increase (persist for a longer period than previously identified). Internal reorganisations may prompt restructuring of the classification scheme and the reallocation of schedules or the identity of those responsible for the records²⁸. Occasionally, it may be that there are changes to the external requirements for an organisation to retain records, such as:

- Identification of gaps in disposal schedules (records not covered by the existing ones);
- New legislation, regulations or regulatory direction (including codes of practice);
- Practice directions of the Information Commissioner;
- Changes to auditing practice;

²⁸ this could be greatly reduced with functional classification schemes

- Greater public interest in policy or operational issues increasing the need for public or parliamentary accountability;
- Increased levels of litigation.

The aim must be to maintain a robust audit trail that can account for the records. Further guidance is contained in another TNA Standard: *Documentation of records work*, including how rules of thumb can be established for deciding on the retention of these items themselves²⁹.

²⁹ e.g. once a record has been created denoting the settling of the disposal of an entire series, that can potentially replace the need to retain the information on individual records or folders

10. Further guidance

For Public Record Bodies, the National Archives client manager function will normally be the first source of advice and guidance on disposal management.

Other public authorities can take advantage of the products of the TNA Records Management Advisory Service launched in 2003. This is to promulgate good practice in records management to local government and other public authorities outside the public records system.

Professional bodies such as the Society of Archivists Records Management Group and the Records Management Society also produce guidance. Some of it is sector-specific and designed to fill particular needs / share the experience of professional colleagues.

See also the *References* in the next section of this guidance.

11. References

11.1 Legislation of the UK Parliament³⁰

Public Records Act 1958
Local Government Act 1972
Local Government Act, 1974
Limitation Act 1980
Local Government (Access to Information) Act, 1985
Access to Health Records Act 1990
Local Government (Wales) Act 1994
Data Protection Act 1998
Freedom of Information Act 2000
Health and Social Care Act 2001

11.2 Statutory codes

Lord Chancellor's Code of Practice on records management (made under s.46 of the Freedom of Information Act 2000)

accessed from <http://www.pro.gov.uk/recordsmanagement/foicode.htm>

[*Action plans* for various public authorities to comply with the Code are accessible from: <http://www.pro.gov.uk/recordsmanagement/access/default.htm>]

11.3 TNA publications

The model schedules currently in existence for records commonly held across government are accessible from: <http://www.pro.gov.uk/recordsmanagement/standards/default.htm>, and are as follows:

1. Buildings records
2. Personnel records
3. Accounting records
4. Health and safety records
5. Contractual records
6. Project records
7. Complaints records
8. Press office and public relations records
9. Information management records
10. Central expenditure records
11. Internal audit records
12. Parliamentary records

³⁰ pre- 1988 legislation is available from <http://www.hmso.gov.uk/acts.htm>. The Public Records Act 1958 is on The National Archives website at: <http://www.pro.gov.uk/about/act/act.htm>

Acquisition policy, 1998
Operational Selection Policies, 1999-2003
Business recovery plans, 2002
Case files sampling techniques, 2000

accessed from: <http://www.pro.gov.uk/recordsmanagement/acquisition/default.htm>

Managing electronic documents using MS Office 97 on a local area network, 1999
Guidelines on developing a policy for managing email, 2003
Toolkit for compiling an inventory of electronic records, 2000
Appraising the inventory of electronic records, 2000
Business Classification Scheme Design, 2003

accessed from: <http://www.pro.gov.uk/recordsmanagement/standards/default.htm>

Requirements for Electronic Records Management Systems [2002 revision]

accessed from:

<http://www.pro.gov.uk/recordsmanagement/erecords/2002reqs/default.htm>

11.4 Data Protection and freedom of information

<http://www.informationcommissioner.gov.uk>

11.5 Records management textbooks

Hamer, A. (1996) *A short guide to the retention of documents*. Institute of Chartered Secretaries and Administrators

Sheppard, E. & Yeo, G. (2003). *Managing records: a handbook of principles and practice*, Facet

Kennedy, J. & Schauder, C. (1998). *Records management: A guide to corporate record keeping*. 2nd ed. Longman

Sampson, K. (1992) *Value-added Records Management: protecting corporate assets and reducing business risks*, Quorum

11.6 Other resources and publications

Monash University Records Continuum Research Project: <http://rcrq.dstc.edu.au/>

Design and Implementation of Recordkeeping Systems [DIRKS]: see <http://www.naa.gov.au/recordkeeping> or <http://www.records.nsw.gov.au/publicsector>

Records Management Society (Local Government Group) 2003 *Retention guidelines for local authorities* available from: <http://www.rms-gb.org.uk/>