

Managing digital records without an electronic record management system

© Crown copyright 2012

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence or email psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information, you will need to obtain permission from the copyright holders concerned.

This publication is available for download at nationalarchives.gov.uk.

Contents

Introduction	4
Purpose	4
Audience	5
Scope.....	6
Definitions	7
Records management policy	10
What is a records management policy	10
How does the policy aid records management?.....	11
Where can I learn more?	13
Filing structures	14
What is a filing structure	14
How does the filing structure aid records management?.....	16
Constructing the filing structure	17
Where can I learn more?	21
Management rules	22
What are management rules	22
Monitoring and maintenance of management rules	24
How do they aid records management?.....	25
Management of metadata	25
Types of management rules	28
Naming conventions	28
Version control for records.....	32
Format of dates.....	33
Where can I learn more?	34
Access control management.....	35
What are access controls?	35

Setting up access controls	37
How do access controls aid records management?	38
Complex access control models.....	39
Monitoring access control allocations.....	39
Other access controls.....	40
Operational limitations.....	40
Where can I learn more?	40
Disposal policy and management	41
What is a disposal policy?	41
What is disposal management?	41
How does disposal management aid records management?	42
Where can I learn more?	44
Email management.....	44
What is email management?	44
How does email management aid records management?	45
Management for rules for email.....	46
Guidance for email management	47
Email formats	47
Retaining emails within the email client.....	49
Alternative email storage.....	52
Bulk email archive storage.....	52
Bulk email archive file format.....	53
Where can I learn more?	53
Integrating management of paper records.....	54
Where can I learn more?	55
Further reading	57

Introduction

Managing electronic records presents a significant challenge for an organisation of any size or sector. For those that store their records in file systems (including shared drives), which have no formal controls in place, the risk of alteration or deletion makes this challenge even greater.

Organisations may have a well maintained paper records system but this is not necessarily appropriate as a template for managing electronic records. This is because of the volume of electronic records, and variety of file formats, combined with the ease of creation.

Electronic records management needs to be very carefully considered and structured to ensure the integrity of the records is not compromised upon capture and they remain retrievable for as long as they are required.

Purpose

The purpose of this guidance is to demonstrate how an organisation can improve the management of records within their file systems by:

- establishing a records management policy
- creating management rules and using them
- developing a classification structure
- introducing email management rules and version control
- establishing user compliance or buy-in

Without these an organisation is at risk of failing to manage records exposing them to risks including reduced business efficiency or potential legal action.

An organisation in control of its records can begin to realise significant benefits including:

- improved business efficiency and effective use of IT resources
- structured management of records retained for legal and regulatory purposes
- support of accurate capture and management of electronic records (irrespective of format) into the file system
- access to records to enable informed and effective decision making

- retention of a corporate memory of transactions, decisions and actions taken by, or on behalf of, the organisation
- protection of the rights and interests of the organisation (and others) who the organisation retains records about
- protection of the characteristics of records as defined by ISO 15489, particularly their reliability, integrity and usability¹
- identification of records required for permanent preservation and archive

Throughout this guidance there are examples using Microsoft Windows XP and Office 2007 (with Outlook). However this guidance is not limited to users of this platform and software applications and should be equally relevant to users of any desk based operating systems and office software applications.

This guidance replaces records management guidance previously published by the Historical Manuscripts Commission, and guidance on managing records in Office 97 published by the Public Record Office.

Audience

This guidance is intended for anyone who controls the management of records within any organisation or part of an organisation. This may be a formally adopted records management role, but it also includes those who manage records as part of their role such as medical or legal secretaries.

Smaller organisations, which do not have formal records management, can use this guidance to create a full programme for improving records management.

Larger organisations, which already have some form of records management, can use this document to develop records management where there needs to be significant consultation and development work.

¹[Digital Continuity advice and Guidance from The National Archives](#) is available where long term maintenance is a requirement. This guidance is principally provided for public authorities and addresses the equivalent long term issues of loss of completeness, availability and usability

This guidance is not restricted to any particular sector or industry. References to specific guidance are given as indicators of best practice in records management. Each organisation needs to consider its regulatory and legal environment which may dictate specific decisions regarding access and disposal of records.

Public authorities should read this guidance in conjunction with the Records Management Code of Practice revised and reissued under s 46 Freedom of Information Act, 2000. Useful references to sections of The Records Management Code have been included in 'Where can I learn more?' where appropriate.

Scope

The focus of this guidance is the management of records stored within a file system using existing infrastructures and resources. It will discuss the process of defining an organisation's need for records management based on the development of a policy and supporting guidelines for users.

Other types of 'basic content services' that offer some form of collaboration and informal document management might be used, such as Microsoft Office Sharepoint or Alfresco. They are not referred to in detail in this guidance. Such applications may support a subset of record management activities but an organisation still needs to develop and implement clear policies and management rules that will build an identifiable records management culture.

These products are rarely coded to implement records management rules without significant customisation and organisations should develop appropriate rules. They should evaluate solutions to support their implementation, managing the risk of records management failures. It may be that the procedures described in this guidance are preferable or alternatively that there is a clear case for deploying a records management application (or ERMS).

This guidance is not intended to be used as a technical manual, nor does it provide an organisation with a full set of policies and management rules. Use the guidance as a basis for best practice in the most suitable manner for their organisation.

Inevitably there will be some technical discussion. This will be restricted to a level of understanding that enables the reader to discuss technical issues with IT or records management specialists where required.

The examples will use Microsoft Windows application suite (including Microsoft Outlook), and are for illustrative purposes only.

The guidance will not discuss use of content management systems nor website management tools.

In practice, organisations will be managing both paper and electronic records concurrently for a significant period of time. This guidance contains information on how the relationship between the two types of record may be managed.

It offers guidance on the management of physical records within an integrated environment but it does not extend to examining systems or applications (specifically for managing physical records such as a library system or tracking system which do not allow for accurate management of electronic records). There is further advice on this topic in a related piece of guidance [Identifying and specifying requirements for offsite storage of physical records](#).

Definitions

This guidance uses some terms in a specific way:

Aggregation

Record assemblies existing within a filing structure (groups of folders) or a folder containing records. In a file system aggregation is limited to folders that contain folders and folders that contain records.

Business classification scheme

An intellectual structure categorising business functions/activities or subjects to preserve the context of records relative to others. It is useful for aiding activities such as retrieval, storage and disposal scheduling of records.

Disposal

A formal decision taken on the final status of a record (or set of records) to either destroy the records, transfer to another organisation for permanent preservation or retain within the organisation's file system for further review at a later date.

Electronic records management system (ERMS)

An electronic records management system (ERMS) is a computer program (or set of programs) used to manage electronic records stored in an associated database. It provides a variety of functions including access controls, auditing and also disposal using a combination of system and user generated metadata.

Depending on the system it can also be used to manage paper records held by an organisation.

Filing structure

A hierarchical structure of folders within a file system which provides a coherent location for capturing records.

The term 'filing structure' is synonymous with the term fileplan. However, this term is not used here as it is typically used to characterise the business classification scheme of an ERMS.

File system

A method for storing and organizing computer files and the data they contain to make it easy to find and access them. File systems may use a data storage device such as a hard disk or CD-ROM and involve maintaining the physical location of the files.

Folder

A type of aggregation or container within a file system used to store records (and other folders). It is the principal building block of a filing structure.

Management rules

Management rules are set of explicit instructions to users on the organisation's preferred means of managing records. These include direction on appropriate capture, access management and disposal of all records irrespective of format or media.

The term 'management rule' is synonymous with the term 'business rule'. Within this guidance 'management rule' is preferred explicitly for records management within a file system. However either term is acceptable and can be used when producing a rule set for managing records.

Metadata

Data describing the context, content and structure of all records and folders within a file system. In a file system this is essentially user-generated and 'passive' in that it can rarely be used for active management of the records. By contrast, metadata in an ERMS is more functional, often system-generated, extensive and linked tightly to system processes.

Operating system

An interface between computer hardware and a user that manages and coordinates use of computer applications using the available resources provided by a computer's processor.

Record

Information created, received and maintained as evidence and information by an organisation or person, in fulfilment of legal obligations or in the transaction of business.²

Records management

The practice of formally managing records within a file system (electronic and or paper) including classifying, capturing, storing and disposal.

Shared drive

A specialisation of an operating system file system, comprising a shared device (for example, hard disk or server space) used by multiple users and accessed over either a local area network or a wider area network connection.

² See International Standards Organisation ISO 15489 Information and documentation: Records management, two volumes 2001

Records management policy

What is a records management policy

A records management policy can be described as an authoritative statement of intent to manage records in an appropriate and suitable manner for as long as they are required for business purposes. It is intended to form the initial framework or principles which express how records should be managed within the organisation. Where the records management policy comprises part of a broader information management or knowledge management policy, it should still be easily identifiable and available to users.

The international standard for records management ISO 15489³ states:

‘The policy should be derived from an analysis of business activities. It should define areas where legislation, regulations, other standards and best practices have the greatest application in the creation of records connected to business activities.’

The records management policy should not be so vague that no ownership or authority can be attributed to it. It must be signed off at the highest level possible (board level) and it should provide, as a minimum:

- a description of what a record is and the reason for capturing and managing it
- a statement of commitment by the organisation to manage records appropriately and accurately for as long as the records are required
- identification of records management roles and responsibilities for all staff at every level of the organisation
- an explanation of the objectives of the records management policy and how it aids compliance with specific standards and legal responsibilities applicable to the organisation
- detail of the relationship between the records management policy and other policies within the organisation (the email management or data security policies)

³ ISO 15489-1:2001 Information and documentation Records Management Part 1: General; 2001

Creating a records management policy should be the first priority for an organisation looking to improve or consolidate its records management. Do this in consultation with the business, with senior management endorsement and support.

It should encompass paper and electronic records created and managed by the organisation. Management rules for creation and management of electronic and paper records should be explicit and should support the principles laid out in the policy.

There should also be a regular review of the records management policy. The timeframe for review should be at least every five years, but with flexibility to review it if significant changes in the business of the organisation require it (a new business activity or introduction of a new business system).

How does the policy aid records management?

A records management policy provides an authoritative mandate for implementation across the organisation. It exists to reinforce the importance of records management at a senior level and determine its direction within the organisation.

This framework can guide the development of file systems and records management processes. This should lead to overall better understanding and delivery of records management across the organisation.

Within smaller organisations the records management policy may be the single resource for records management. As the principal statement it provides new and existing users with a direction on records management to ensure it is taking place correctly. In this way the policy is directly responsible for guiding the development of records management within an organisation.

In larger organisations it is more likely that the records management policy will provide a broad instruction that record managers can refer to as their authority for promoting records management.

If difficulties with records management activities cannot be resolved at a procedural level with business managers, reference to the records management policy can help in resolving them.

Case study:

An organisation's records management policy clearly articulates a responsibility to comply with legal or statutory regulations indicating that records must be managed to fulfil these responsibilities (for example, response to subject access requests under the Data Protection Act).

Using incremental implementation of the records management policy, users are made aware of these responsibilities and work to ensure accurate records are captured and well managed. This enables the organisation to respond to requests for information efficiently and effectively without loss of productivity.

This case study explains how the successful implementation of a records management policy relies on how well it is implemented. If users are given the opportunity to view and understand the records management policy, it will help to ensure they adhere to it on a day to day basis.

Case study:

An organisation has not produced a defined records management policy. As a result users do not have a clear understanding of what records should be created and retained.

Following an investigation by a regulatory body the organisation is found to have failed to retain specific key records. As a result they are found guilty of corporate negligence through poor records management, fined and reprimanded by the auditing authority leaving them with significant financial and reputational damage.

This case study explains how the successful implementation of a records management policy relies on how well it is implemented. If users are given the opportunity to view and understand the policy, it will help to ensure they adhere to it on a day to day basis.

Limitations of a policy

A records management policy cannot guarantee that users will actively manage records. In order to realise the benefits of the records management policy an organisation will need to undertake other activities and changes to ensure active records management takes place.

The process of implementation required to support the records management policy in improving records management will need:

- creation of accessible guidance on records management such as naming conventions, capturing of emails, and disposal methodology
- development of management rules for the use and management of the file systems
- establishment of a process for monitoring the file systems to ensure records are being effectively managed as intended by the records management policy

These supporting features are a practical application of the records management policy and together provide the actual process of records management as a business function.

Where can I learn more?

Implementation guidance

[Guide 2: Organisational arrangements to support records management](#)

A brief implementation guide developed to help public authorities achieve compliance with the Code of Practice issued under s 46 of the Freedom of Information Act 2000. Intended for the Public Sector its principles are applicable to anyone establishing a records management policy.

Examples of policies

The following are examples of records management policies; we do not recommend wholesale adoption of another organisation's records management policy.

- JISC records management policy
www.jiscinfonet.ac.uk/InfoKits/records-management

- The Financial Services Authority records management policy and standards – RMPS
www.fsa.gov.uk/pages/information/pdf/records_policy.pdf
- Record management toolkit for schools – records management policy
www.rms-gb.org.uk/download/730
- NHS CFH MODEL records management policy
www.connectingforhealth.nhs.uk/systemsandservices/infogov/records

Record Management Code of Practice reference

- [Guide 3: Records management policy](#)
- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Filing structures

What is a filing structure

The filing structure reflects the relationship of business activities through careful structuring of folders (with meaningful titles) 'containing' the records. This structure illustrates what the organisation's business is, and it provides a means of managing its records.

A filing structure provides an environment for presenting a common understanding of how records should be stored and retrieved. This is particularly important not just for users working in a team, but also when working across the organisation by improving the retrieval of content and making it understandable to every user.

If the filing structure is well designed it will allow the organisation to control access more effectively, ensuring that unauthorised users are not inadvertently granted access.

A filing structure may be modelled on the functions of an organisation. Alternatively it may also use subject themes for parts of the structure. In either circumstance avoid using names of business units (or individual users) as this can cause problems such as:

- inhibition of sharing content and information across the organisation
- unnecessary duplication of records causing problems with routine disposal policies

- separate (or silo) work areas within a corporate filing structure making it difficult to shape records management at a strategic level
- legacy filing areas for discontinued work groups and obsolete business units remain in place and unresolved
- reduced efficiency in terms of compliance with the Data Protection Act or Freedom of Information Act

These problems can be aggravated if users move within the organisation, or leave.

There are many approaches to creating a filing structure and even a number of commercially available tools available to aid organisations when designing, or re-designing, one.

Irrespective of the method used to create a filing structure, it must at the very least contain the following attributes:

- a structure that is easily interpreted and which discourages users from placing records in inappropriate locations
- simple names that identify the logical element of the filing structure
- established responsibilities for folder management, to ensure the filing structure is well maintained
- typically a 'functional' filing structure will have three levels (or layers) of folders that act as segregations for information. These levels represent the functions, activities and transactions of an organisation
- the fourth, and usually final, layer sits beneath these. It is defined by the business where the records are to be captured and stored. This prevents users from creating idiosyncratic, locally defined, sub-folder structures below this level, within a particular part of the filing structure, which does not conform to the corporate rules

Example:



This example shows a basic layout of a filing structure in the MS Windows environment. Other systems will use different icons and might display the filing structure slightly differently.

The upper folders or 'Classification Folders' should never contain records. If the expertise is available, identify the upper folders by an icon different to that of a normal folder. This provides a visual distinction for the user. Records are normally only expected to be captured in the fourth (or lowest) level of the filing structure.

This method allows an organisation to implement and manage both access controls and disposal scheduling across aggregations of records in a clear and defined layout. This reduces record management overheads and ensures consistency across the filing structure.

How does the filing structure aid records management?

From the organisation's perspective, there is rarely sufficient standard functionality within a file system that can be used to control the creation, deletion or movement of folders. Most file systems options are limited to a simple on/off option depending on the user's access rights. This provides further complications as folders and records have to be moved (and archived) manually with no audit control. If a mistake is made there will be no report or audit trail that could be examined easily to confirm where a folder (or record) has been moved to.

From the user's perspective, a filing structure helps mitigate this by providing a logical structure which makes it easy to see where a specific record (or new folder) should be located.

Organised filing structures support records management by providing an understandable and accessible location for all records which encourages users to work within it. This helps an

organisation reduce the risk of business critical information being lost within an uncontrolled file system. It also helps motivate users to move records out of personal drives or email accounts where it may be deleted without anyone knowing it existed.

Constructing the filing structure

Designing a filing structure is often a time consuming task, particularly where there has never previously been any formal order or agreed layout for records and folders. There are products that can help with reducing the time it takes to design the filing structure. In all cases it must be thorough and with a focus on usability.

There are proprietary software tools for developing the structures needed to manage documents and records. Such tools can be used to create and maintain a comprehensive range of business classification schemes, taxonomies, thesauri, glossaries, records retention and disposition schedules. However using them will incur additional costs.

More information on these business classification software tools is provided at 'Where can I learn more?' at the end of this section.

Example:



This is an example of a clearly designed and managed filing structure organised in a hierarchy of folders. The names of the folders use a simple structure and basic semantics so that all users can interpret it.

Example:



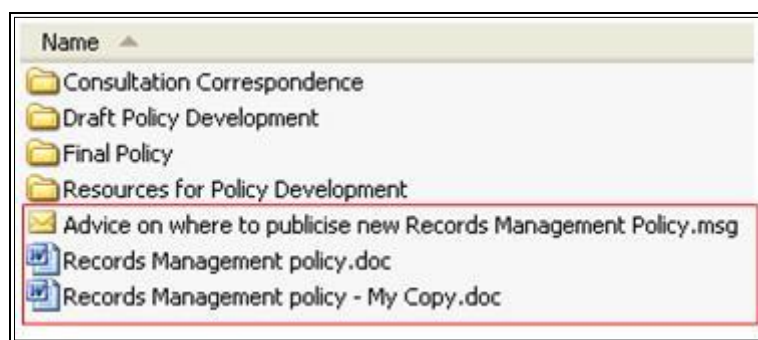
This is an example of a poorly designed and managed filing structure with no control over the hierarchy of folders. It leaves users confused about where to capture records for any given function. For example a new or temporary member of staff may not know where to locate a draft policy.

The visual representation of the folders within a Windows operating system is only for display purposes - the folders portray the file system metadata used to configure related objects on-screen. Users often think (incorrectly) that they are capturing records into an actual folder when in fact they are stored randomly. The records are not located within the designated folder. It is the operating system which displays them in a logical order using the folders as a prompt.

Creation, movement and deletion of classification folders must be carefully controlled and restricted to a sub-set of users, or in smaller organisations, restricted to the records manager. This ensures that any development of the structure is consistent and that there is no inappropriate access or disposal. It will also enable the organisation to prevent uncontrolled proliferation of folders (and potentially sub-folders) by any user who has access to the filing structure.

Much of this will require management rules owing to the limitations of the file system functionality. This is particularly difficult where users have rights to create both folders and records in an area of the filing structure. Without complex coding it is difficult to develop a type of folder that allows only records to be captured into it by a user with access rights. As a result users could place records and folders at the same level of the filing structure.

Example:



This example illustrates how the filing structure can be disrupted by allowing records (outlined by the red box) and folders to exist at the same level.

The relationship between the records, folders and parent folder are unclear with no understanding on how they should be managed. This introduces a further complication; it is often unclear whether the record should be disposed under different rules to the folders and their contents.

The management rules need to be supported by frequent monitoring of the filing structure, correcting any errors. With significant IT configuration, custom scripting may allow a greater level of functionality within the filing structure to prevent end users from adding records at inappropriate levels of the structure.

This guidance does not cover these options as customisation is likely to be expensive.

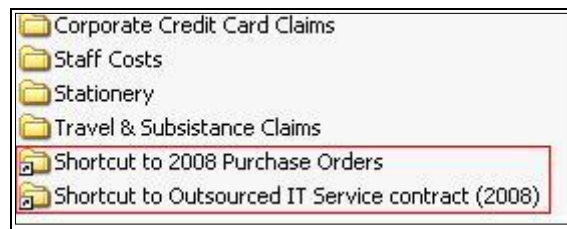
Shortcuts and relating folders

In an ERMS it is possible to create a record or container (folder) in one location but have it appear in multiple areas of the filing structure using a system of 'pointers'.

These pointers are an interactive shortcut to an object that replaces the need for duplicate copies of a record and are coded to resolve any conflicts in access control and disposal management.

Whilst this functionality does not exist in a file system, it is possible to achieve some of the end-user benefits of pointers by using the 'Shortcut' option in systems such as MS Windows.

Example:



In this example two folders (outlined by the red box) were needed in two parts of the filing structure. Having decided the primary location for the folders shortcuts were created and placed in the secondary location. This technique can significantly reduce the amount of duplication present in a filing structure. It will also support organisations trying to respond to requests for information by ensuring only one copy of a record, or location for record exists.

Use shortcuts with caution. They are merely a link to a record. They do not have any content themselves and pose the following risks:

- if the original record is deleted the shortcut will remain, but no longer pointing to anything
- inconsistent disposal processing is possible as the record manager will not necessarily be able to locate all shortcuts
- there is a significant risk of retaining implied personal data (through the title of the shortcut) or other sensitive information

Limitations of a filing structure

The limitations of a filing structure are largely based on those of the file system that supports it.

The limitations can be summarised as:

- the functionality of a file system presents a significant limitation in the control of creation, deletion and movement of records and folders where a user has access
- a file system's functionality does not prevent users placing records in the wrong folder if they have access to it
- a filing structure will only be effective if users are able to engage with it
- a poorly constructed filing structure will only discourage users from engaging with it and exacerbate any records management issues that arise

These limitations can only be mitigated by strict management rules and a policy of reviewing the filing structure periodically to ensure it is being used appropriately. Additional ongoing training for users and active management by those responsible for records management (either corporately or locally) can help ensure records management activities are being carried out appropriately. This will also help identify departures from recommended practice.

Where can I learn more?

Designing a filing structure/business classification scheme

There is a range of guidance available on designing a filing structure and various groups have created some sector specific guidance.

- [Business classification scheme \[File plan\] design](#)

Example business classification schemes

These examples of business classification schemes are included for illustrative purposes only.

- Local Government classification scheme V2.03:
www.rms-gb.org.uk/resources/92
- JISC Infonet HEI business classification scheme, 2007:
www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-bcs-user-guide

Business classification tools

This is not an endorsed list of software. These examples can be used to aid an assessment of a file system(s) to help build a filing structure, and address redundancy and duplication. Other products may be available and each organisation must assess whether they need such a service at all.

- a.k.a.® available direct from the Australian developers or in the UK via In-Form Consult Ltd:
www.a-k-a.com.au/ or inform-consult.co.uk
- One-2-One Classification software for records management:
www.acs121.com/html/one2one.html
- Active Navigation:
www.activenav.com/

- Keyword AAA:
www.naa.gov.au/Images/Keyword%20AAA_tcm16-47292.pdf
Keyword AAA is a thesaurus of general terms designed for use in classifying, titling and indexing most types of records in most technological environments. To provide a comprehensive controlled vocabulary, use Keyword AAA in conjunction with a thesaurus of functional terms relating to the organisation's specific or core business functions.

Record Management Code of Practice reference

- [Keeping records to meet corporate requirements](#)
- Guide 6: Storage and maintenance of records
- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Management rules

What are management rules

Management rules are set of explicit instructions that direct users in the organisation's preferred means of managing records. These directions specify a variety of activities and should also explain why the rule has been created. Whilst the style and detail of management rules may vary between organisations they should include instructions on:

- appropriate means of capturing electronic records into the filing structure
- clear definitions on what records should be captured into the filing structure and what may be held in a personal drive (such as users' staff appraisals)
- specific criteria for the application and management of access controls
- specific criteria for the disposal of all records and folders with explicit reference to the organisation's disposal policy

Management rules should always be expressed as an instruction and should not be ambiguous in their interpretation. Their purpose is to provide a mandate and authority that helps ensure a level of consistency is applied across an organisation in terms of records management.

Without management rules implementation of the records management policy will be very difficult. Finding a balance between use of software that may automate certain activities and

ensuring users still engage in records management is a difficult balancing act, only managed by implementing effective management rules.

Within a file system, records might be moved and edited without the actions being auditable. Management rules are one of the most practical ways of ensuring that activities within the file system such as capture, classification and disposal of records are carried out with a degree of logic and accuracy by all users.

Management rules provide direction on a range of records management activities and include, but are not limited to:

- naming conventions for folders and records
- management of the filing structure
- allocation of access controls
- management and execution of disposal

There is no standard profile for management rules and organisations may decide how they should be written and made available to users. However there are some basic principles that should be included in the development of management rules. Specifically they should:

- reflect and reference the good practice presented in the records management policy
- be written in natural language (non-technical or Plain English)
- be made available to all users (via an intranet or central guidance library, for instance)
- indicate where specific records (such as vital records for disaster recovery) need to be managed to comply with regulations or other external review processes

The management rules should be framed in terms of their benefit to the organisation and its records management capability. This must necessarily outweigh individual preferences for managing records. To avoid a conflict between these two needs, the management rules should be developed in consultation with the users.

This helps ensure that the rules do not prevent the efficient conduct of business, but also that users are not disenfranchised by an enforced set of rules that does not allow them to do their job.

Case study:

An organisation, having conducted a review of the file system, decides to implement management rules to improve the way users capture records into the system. During the consultation on the management rules, those responsible for records management discover that the proposed filing structure doesn't support the way users need to capture records and as a consequence the proposed management rules would impede business activities.

This case study demonstrates the need to develop the filing structure and management rules in consultation with users so that the organisation develops a good records management culture. This encourages users to feel that the management rules have not been imposed, and they are happy to participate in good records management.

Monitoring and maintenance of management rules

Training and advice on management rules is essential. There must also be a process of monitoring to ensure that users work within the rules.

This requires roles to be created at both a local and strategic level to form a watching brief on use of the filing structure and email clients and to correct and guide where rules are breached or misinterpreted. These monitoring roles should be empowered to report persistent and/or deliberate breaches of the management rules to a senior record management authority.

Occasionally a management rule may become an impediment to business conduct or no longer reflect the environment in which records are stored. The monitoring role can be engaged to evaluate whether a persistent breach of a management rule results from the rule no longer being appropriate or that it hampers users doing their job.

Management rules should be re-evaluated regularly and particularly where changes occur to either the file system, filing structure and the record management policy.

How do they aid records management?

Management rules help mitigate the limited nature of system generated metadata by providing structure and support to users enabling them to proactively manage their records. When combined with routine monitoring, management rules assist in building a culture of records management.

The other benefits of management rules include:

- assistance to users in the conduct of day to day business by providing a common and easily understood framework
- improvements to business efficiency by ensuring all users capture and manage records in a similar manner allowing the organisation to locate information quickly and accurately
- encouragement of awareness of the importance of records management to individuals by highlighting the business reasons/benefits within the management rules
- support for the records management policy by demonstrating a commitment to records management across the organisation
- empowerment of the records managers to challenge poor records management within the organisation
- provision of evidence to external authorities that deliberate and controlled management of file systems is encouraged by use of management rules
- translation of the record management policy into standardised procedures for staff to follow

This is not an exhaustive list of benefits, but gives an idea of how significant management rules are to the use of file systems for records management.

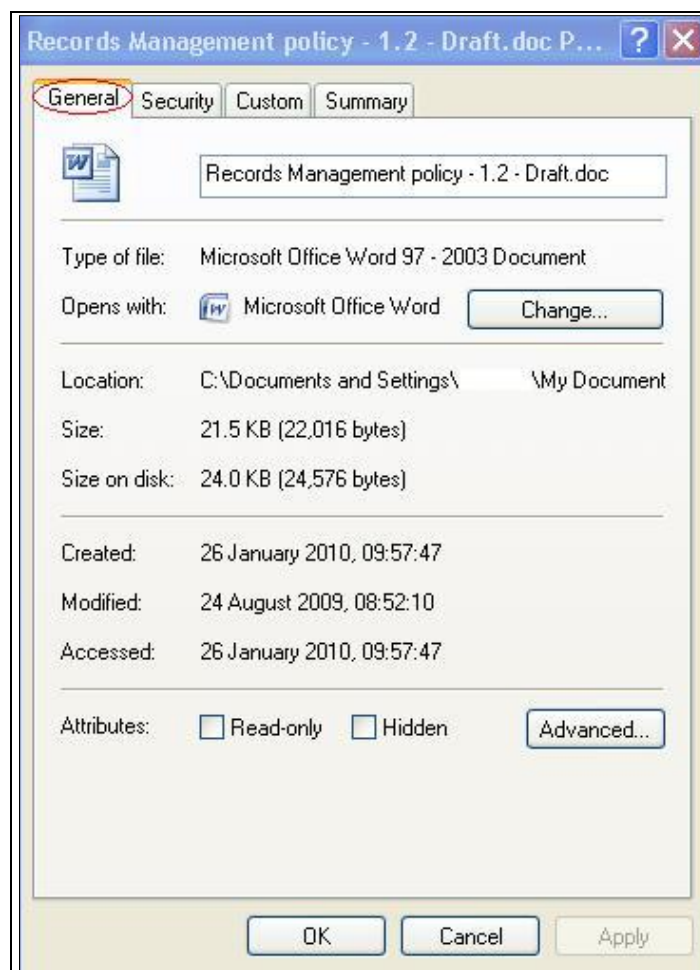
Management of metadata

Within the context of a formal ERMS, metadata is used to provide data about records and folders (details on how long a record should be kept, or determine who may access the record). This metadata is often used by the ERMS to drive functions such as access controls and disposal rules.

In contrast most of the metadata presented within a standard operating system is only informative and cannot be used for active records management.

It is possible to configure the system so that when a user captures a record they are presented with the 'Properties' view for the record. This is a visual prompt for the user to enter some meaningful metadata that can be used to manage the records. In practice this process cannot be mandated and user can still enter meaningless information in if they so choose.

Example:



This example illustrates the limitations of metadata as displayed in a MS Windows file systems. Within MS Windows explorer the 'General' properties tab (circled) displays the following metadata. This metadata is only providing a view of metadata generated by the operating system.

In practice metadata presented in a file system is not completely robust for the following reasons:

- a change such as renaming the record or relocating it is recorded in the 'Accessed' date time field, but not in the 'Modified' date time field
- the field 'Modified' only records a change in the content of the Word document
- if the operating system is incorrectly configured or corrupt (if the server clock is inaccurate) any of the metadata regarding date and time will have no value
- if a record, or group of records, is moved to a new location, there is no audit of this action or any place to indicate a reason for a move if it is deliberate (unless a custom text field is developed)
- very little automated control to reduce human error because there is only a limited set of metadata (user access controls) linked to or enforced by the operating system

Limitations of management rules

Management rules do not provide a replacement for functional metadata. Even the most well defined and structured management rules have limitations. There are a number of reasons why they could cause problems and deter users from engaging in records management activities such as:

- not reflecting how the organisation's business is conducted and preventing ongoing conduct of transactions
- requiring too much effort on managing records to the extent that the business of the organisation cannot be conducted
- not written or defined in a way that all users can understand them
- too prescriptive or rigid to engage users
- cannot be enforced in most standard file systems

These are just a few examples. Ultimately the rules rely on the goodwill of users to engage with them. This can be enhanced with a monitoring process by the records manager or selected individuals in local business units. If suitably empowered by the organisation they can help users to understand best practice and provide an immediate response to queries and problems.

Write the management rules in consultation with users and in accessible language (Plain English). The rules must also be available through the most practical means so that users can quickly find them for reference (via an intranet or central record management resource, for example).

Users must be prepared to engage and work with the management rules and the file system to achieve records management. Once the rules have been established and agreed they must be enforced and followed if their benefits are to be realised. This will require some form of monitoring and process for reporting where the rules have not been followed so that the problem can be rectified and the user provided with information or training.

Types of management rules

There are likely to be a range of management rules that are specific to the organisation, particularly in respect of compliance with specific legislation. The following conventions are areas where management rules will be required for all organisations using file systems.

Naming conventions

Naming conventions help identify records and folders using common terms and titles. They also enable users to distinguish between similar records to determine a specific record when searching the file system.

Naming conventions need not be overly prescriptive or formalised but they must be clear and well defined. Names for records must be meaningful, and convey an idea of the content. Records and folders with a meaningful title based on naming conventions also allow efficient records management judgements to be made without having to explore the content of each individual record.

Without naming conventions there is a significant risk of records being destroyed or lost within the file system. Without standard approaches to naming folders the context of the records becomes meaningless to anyone other than the creator.

Organisations should ensure that sensitive information is never used in the name of a record or folder even where access to the area of the file system is strictly managed. This is to ensure that personal or sensitive data cannot be inferred by casual viewing of a record or folder title.

The use of pertinent security or protective marking information should also not be included in the title of an object. Use of terms such as 'Confidential' could imply a level of sensitivity that would compromise the content of the record or folder by advertising this in the object's name.

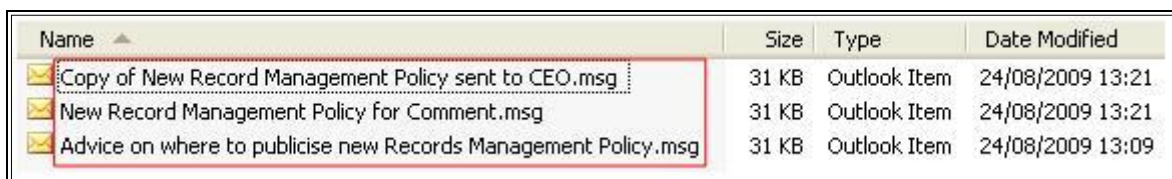
In practice certain records and folders have to include sensitive information. Considered application of appropriate access controls should mitigate accidental disclosure of sensitive information to anyone other than an authorised user.

Naming conventions for emails

There must be specific guidance on naming conventions for emails. When emails are captured from the email client (such as MS Outlook) into a file system they are automatically named using the text in the 'Subject' field of the email. As a result, the prefixes 'RE:' for replies and 'FW:' for forwarded emails may be retained. Remove these to ensure that the title of the record is clear about the purpose and content of the captured email.

In practice email capture is likely to require more detailed guidance as several emails might be captured as part of a longer communication. If all these emails are captured and given the same name, the context and reason for capturing will remain unclear.

Example:

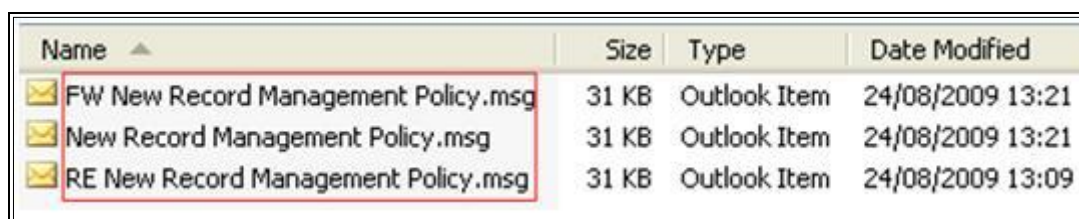


Name	Size	Type	Date Modified
Copy of New Record Management Policy sent to CEO.msg	31 KB	Outlook Item	24/08/2009 13:21
New Record Management Policy for Comment.msg	31 KB	Outlook Item	24/08/2009 13:21
Advice on where to publicise new Records Management Policy.msg	31 KB	Outlook Item	24/08/2009 13:09

This example demonstrates the benefit of providing a meaningful title for each email.

Whilst requiring an investment from the user, they form a coherent set of records with discernable content and relationship to other records within the file system.

Example:



Name ▲	Size	Type	Date Modified
FW New Record Management Policy.msg	31 KB	Outlook Item	24/08/2009 13:21
New Record Management Policy.msg	31 KB	Outlook Item	24/08/2009 13:21
RE New Record Management Policy.msg	31 KB	Outlook Item	24/08/2009 13:09

This example illustrates the problem when users do not actively rename captured emails. There is neither understanding of what each email was created for, nor why it may have been captured.

Naming conventions for folders

The capture and management of all types of records into a file system requires careful planning and structure.

The reasons for providing naming conventions for folders are:

- to ensure consistency of approach in terminology and format for specific activities, such as casework
- to provide all information within a file system with a coherent context and logical frame of reference
- to provide users with a practical means of identifying where records should be captured within any given part of the file system

As with the naming conventions for records (including emails) there must be management rules for users to follow when naming folders.

The rules need not be excessively prescriptive, but ensure that the length of the folder name is not too long. It can become difficult to search and retrieve accurately for folders lower down the filing structure.

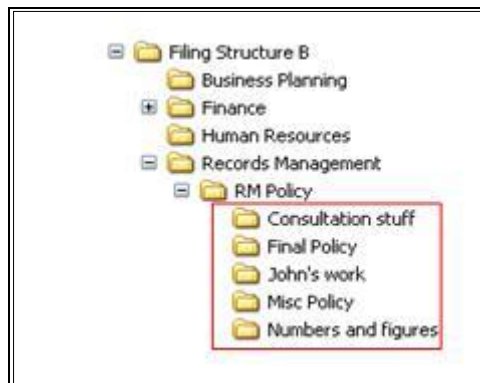
Example:



This example illustrates some of the benefits of providing meaningful titles within the filing structure:

- the hierarchy of the structure is clearly identifiable by the titles of the folders
- peer relationships between folders are clearly identifiable indicating a range of preferred locations for different types of record on a related activity
- at the lowest level of folders (outlined in the box) it is clear what is expected to be captured into each folder

Example:



This example shows a file system where there are no management rules applied to folders. The hierarchy gives some idea of the filing structure, but lack of consistency in naming the folders makes it very difficult to understand the whole structure and where to find specific records.

The folders for records (outlined in the box) provide no means of identifying their content or what should be captured into them. In such a filing structure records management would be impossible and places an organisation at a significant risk of information loss.

Version control for records

The means of indicating a current version of a record in any system is difficult. Management rules can aid this and allow users to name the record indicating the current (and previous) version.

Example:



This diagram illustrates the simple addition of '1.0' to indicate the draft status of a record. If an organisation adopts this simple approach and uses small decimal increments to indicate minor revisions and whole numbers for a major revision, all users can quickly identify which is the current draft or final version.

Example:

Name	Size	Type	Date Modified
Records Management policy - 1.0.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - 1.1.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - 1.2.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52
Records Management policy - 2.0.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52

This example illustrates the addition of a simple decimal system for indicating minor and major changes in the version. In this case 'whole' versions of the document are named using 1.0 or 2.0. Interim drafts are named 1.1, 1.2 and so on.

This is considered best practice, but organisations might use other version numbering for records such as technical drawings. Irrespective of the naming conventions used they must still be explained clearly within the management rules.

Example:

Name	Size	Type	Date Modified
Records Management policy - 1.0 - Draft.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - 1.1 - Draft.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - 1.2 - Draft.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52
Records Management policy - 2.0 - Review.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52

This example illustrates a further suffix added as a one word statement - 'draft' - reinforcing the version numbering and clearly identifying the record's status. Where used, control and monitor these terms for consistently. Any lists of controlled terms must be reviewed, and updated, at regular intervals.

Used correctly these ways of indicating a record version will provide a clear idea of the drafting process and which record is the current one.

Example:

Name	Size	Type	Date Modified
Records Management policy - OLD ONE DO NOT USE!! .doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - Draft.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:51
Records Management policy - 1.2 - Draft.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52
Records Management policy - Final.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 09:52
Records Management policy - My Copy.doc	22 KB	Microsoft Office Word 97 - 2003 Document	24/08/2009 11:17

This example shows the consequence of having no management rules for version control. There is little coherent information identifying versions and their relation to the others. This could have a significant impact on records management activities such as disposal, and will also limit the ability to locate and retrieve the current record efficiently.

To remain effective either a records manager or a local authorised user should monitor the use of naming conventions. The introduction of rules on the creation of version controls really only works where the business recognises a real need for these conventions. If not, they are rarely used and become redundant.

Format of dates

It is very likely that users will want to manage some records, and the folders they are located within by date. Given the range of ways of writing the date, the organisation must choose a

standard format for all users to follow. This will aid structuring of folders and improve the ability to retrieve information when searching.

The most practical way of using dates is in the format Year-Month-Day or 2009-08-21. This is a standard format which allows for easier searching. This is because when searching for older records a user is more likely to know the year, and possibly the month, when a record was created than the exact date.

Where can I learn more?

These examples are included because they reflect best practice as a list of rules. Not all will be suitable for every organisation; management rules should be developed in consultation with users and appropriate to the size, sector, culture and resources of the organisation.

- The Financial Services Authority records management policy and standards – RMPS: www.fsa.gov.uk/pages/information/pdf/records_policy.pdf
- Record Management Society RM toolkit for schools: Creating information management systems: www.rms-gb.org.uk/resources/848.

Record Management Code of Practice reference

- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Access control management

What are access controls?

Access controls determine who can access/capture records and access/create new folders. The allocation of access controls allows an organisation to delegate responsibility for records and folders to their creators and managers. This accountability helps to ensure that records remain authentic and reliable, retaining their integrity and usability.

In a modern records management environment access controls within a filing structure are set to as wide (or open) a state as possible. This means that unless a specific reason can be applied, records and folders should be accessible to all parts of an organisation as a default. This reduces the overhead of managing access controls and it also improves the effectiveness and efficiency in information sharing.

Some organisations may provide users with personal drives to store records such as copies of staff appraisals or annual leave requests. Where used these should be restricted in size to prevent users turning them into personal storage areas for business records.

Personal drives have to be restricted to genuinely personal information. They must not be used for storing business records which may be sensitive and require access controls while still sitting in the filing structure (with appropriated limited access controls).

These personal drives are not recommended for storing business records; the rest of this chapter is directed at access management within open shared drives and the filing structure.

Most organisations will already have user profiles that give all authorised staff an email account and access to the file system. Typically this profile also gives access to a personal drive (individual space on the file system) and one or more areas of the file system (sometimes referred to as 'Shared Drives').

Example:



This example illustrates the 'Security' window for a folder in a MS Windows file system. The list of 'Groups' and 'Users' indicate who can access the folder. Those listed have the power to add or remove other users to control access as required. Additionally the administrators can refine the 'Permissions' further to indicate what a user can do within this folder, such as capture new records or create a new folder.

Organisations may wish to create a number of profiles to reflect the level of functionality available to certain users. A typical end-user's profile will look similar to the above example but some of the 'Permissions' might be set to 'Deny' to limit what they can or can't do in particular parts of the filing structure.

Using these basic controls an organisation can begin to form access controls across the filing structure. These can be used to keep as much information as open as possible and appropriate, whilst also ensuring sensitive information is kept secure.

Setting up access controls

Access controls can be set at three levels within a file system - at drive, folder, or record level.

Allocating access controls by individual user requires substantial effort and it would be difficult to monitor or track. Development of access groups reduces this overhead substantially and it can improve the controls placed on any part of the filing structure.

This can be a very useful means of applying quick access (or denying it) to a part of the filing structure by an administrator. However it is potentially limited if an organisation is located over several sites using individual Local Area Networks (LAN). Whilst the filing structure may be represented in all locations, they will not all be updated if access controls are updated. This would require every individual network to be updated to ensure a consistent application. Organisations that use a Wider Area Network (WAN) will not have this problem.

Example:



This example illustrates how access groups can be used to granulate access to the filing structure. In particular, the 'Finance' folder and lower folders need specific access controls. An access group called 'Group A' is created and granted sole access within 'Finance'. This Group contains all users who are permitted to see and access the 'Finance' area.

Below 'Finance', the 'Contracts' folder requires an even greater level of access control and a sub-set of 'Group A' users is selected to form 'Group B'. Using this process an administrator can vary and allocate access controls more efficiently than if they had to select each individual user. By maintaining memberships of access groups instead of individual access to every record and folder the overhead of managing access controls can be reduced significantly.

Whilst file systems work better when configured at the highest permissible level for both folders and records, it is possible to restrict access to individual records and folders. This should not be considered in normal access control allocation. There is the risk that the information will become lost and inaccessible to the organisation if that user leaves (temporarily or permanently), or moves to another business unit.

Successful application of access controls does not rely solely on the creation of appropriate groups. If the filing structure itself has not been constructed in a coherent way it could become very difficult for an administrator to ensure that correct access is being applied across the file system.

How do access controls aid records management?

As a file system lacks much of the automated functionality of an electronic records management system, access controls are one of the few means of formally regulating changes to the filing structure and records.

Access controls help control how and where information is created and accessed. Such controls can help to:

- restrict the number of users who can change or edit records and folders
- reduce the number of users who could inappropriately delete, alter, or relocate sensitive information
- identify and allocate responsibility for records and folders within sensitive areas of the filing structure

Locally appointed record managers, where available, can be given a local administrator profile for a relevant part of the filing structure. This still limits the number of users who can edit access controls, but improves the efficiency with which changes can be requested, made and monitored at a local level.

Any local administrator should work with and be managed by a records manager to ensure consistent governance is applied across the filing structure.

Limitations of access controls

There are a number of factors that should be considered when implementing access controls within a file system. A file system does not offer the granularity or ease of use with access controls as a dedicated electronic records management system might.

Complex access control models

It's easy for access controls to become complicated and difficult to track. To prevent this developing into a significant management overhead keep access controls as open as is practical (so that all users can see but not edit records and folders). This means keeping as small a number of access groups as is required and actively managing them, reviewing and updating them regularly.

Documenting this process is likely to be difficult. Although the server will retain a log of access groups, this may not be presented for easy review. Where an organisation develops access groups they will need to ensure that this is documented externally from the file system to allow review by records management staff.

In complex organisations with a pre-existing access model for paper files, the organisation may view this as a useful referral tool when allocating access to related electronic records in the filing structure. This will not be an exact match but may help with consistent allocation of access.

Monitoring access control allocations

The monitoring and regulation of access controls can be a time consuming process. This is exacerbated by the fact that a record manager cannot always independently decide whether appropriate access has been given. A management rule must be used to ensure that users are added (and removed) to access groups by a records manager (or network administrator) only upon request from another authorised user.

Any user who has full access to a folder or record (to edit or delete content) can also change the access controls if they know how. This could result in other users being 'locked out' of folders or records inappropriately. This type of behaviour must be monitored carefully. For this reason avoid individual access controls as far as is possible.

Changes to the structure of the organisation may also affect specific access controls where users move from one part of the business to another. The organisation will need to ensure these changes are logged so that an authorised user can update access controls appropriately.

The same action would also be required when a user leaves the organisation. Their IT profile must be deleted to prevent anyone from accessing the file system using the account.

Other access controls

A feature of MS Windows file systems is the ability to protect both records and folders with a password. This prevents anyone other than the user from accessing the object, and circumvents the organisation's access controls. Either switch off this functionality or actively discourage it. Passwords are either too simple to offer any real security or they are forgotten. In either case the security of the document is reduced and the organisation risks losing control of its information.

Similarly if a user leaves without disclosing relevant passwords there is a risk the organisation will not be able to change the passwords. Immediate access becomes an issue and it presents a challenge for digital preservation. Scaled preservation operations that convert records to another format can be hampered significantly.

For these reasons we advise that any reliance on password controlled access should be replaced with alternative access mechanisms

Operational limitations

A related issue is the creation and maintenance of user profiles on the file system. Usually this is only carried out by the IT function within an organisation (or an external IT provider). When changes are made (a new user is added, for example) there must be clear communication between the IT staff and those responsible for records management to ensure the user is able to access the filing structure as appropriate.

Where can I learn more?

The implementation of access controls and configuration of folders within the filing structure to support them will require significant IT support. We recommend that the experience and knowledge of the IT function is used to help create a usable and secure environment.

If no such function exists then the organisation will need to consider seeking external advice on this subject.

Record Management Code of Practice reference

- Guide 7: Security and access
- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Disposal policy and management

All organisations irrespective of sector or size need a disposal policy and process to prevent retention of records no longer required for business purposes.

What is a disposal policy?

A disposal policy is a formal statement by an organisation on the appropriate means of disposing of records to agreed disposal schedules⁴. It should indicate how long records should be kept and whether they should be destroyed or transferred to another organisation once they are no longer required for business purposes. The policy may form part of the overall records management policy, or it may be a separate document that forms part of the suite of supporting guidance along with management rules for example.

Additionally the policy will need to be supported by disposal schedules that identify types of records and provide the detail on how long they should be kept for and whether they should be destroyed or transferred to an archive⁵. The process of disposal supports legal obligations, such as destroying collected personal data when it is no longer required.

What is disposal management?

Disposal management is the formalised process of assessing records to determine how long they should be retained and how they should be removed from the file system. The removal

⁴ Sometimes referred to as retention schedules

⁵ Transfer to an archive is likely to be an issue for only a small proportion of an organisation's records

should be based on the established disposal schedules and follow an agreed process for either destruction or transfer.

In normal circumstances records are disposed of by aggregation or collections of records in folders. Disposal of individual records is normally to be avoided because of the overheads in selecting and deleting individual records. Disposing of aggregations of records is far more efficient and ensures a greater security that related records have been disposed of correctly. This is important in a file system where there are no formal disposal management tools (which are available in an ERMS).

The disposal process should include appraisal of records to understand their current context and content to decide whether they can be removed from the file system. This is important as some records, while due for disposal under an allocated disposal schedule must be kept for another purpose such as a legal investigation.

For this reason disposal management should never be a fully automated process. Even if a record manager is confident that types of records routinely created (such as meeting minutes) could be disposed of, there should still be a means of checking whether they must be retained for a reason other than their original purpose.

Records should never be disposed of on an ad hoc basis or at the discretion of individual users unless there is a specific reason such as:

- it is a duplicate record not required to support the business
- it wasn't needed to be captured as part of the corporate record (such as a casual email correspondence)
- it is an early draft that no longer reflects or aids the development of a final record

This process must be supported by clear management rules and be monitored by the records manager.

How does disposal management aid records management?

In essence, without a controlled disposal management process defined by a policy and supported by disposal schedules, the organisation risks losing control over how many records

are held indefinitely, taking up valuable storage space. The disposal management process helps reduce this risk by:

- reducing the volume of out of date records no longer required for business purposes
- ensuring that personal data is not retained beyond its intended purpose
- improving the efficiency of a file system by freeing up space on servers
-

It will be difficult to support this process in a file system, but it can be aided significantly by:

- grouping activities together to reduce the overhead in searching and reviewing types of record due for disposal (for example, financial transactions)
- closing folders with a clear time limit where it suits the business process and opening new ones (at the end of a financial year or project, for example)
- using naming conventions to help readily identify types of records
- introducing a custom metadata field 'Properties' in the folder or record that allows users to allocate the correct disposal schedule

Limitations of disposal management

Disposal management as a process is not supported by a file system without specific records management software. This makes disposal management a very difficult process to control within the file system for the following reasons:

- disposal activities have to be done manually including allocation of a disposal schedule, executing it and recording the event
- users might not provide disposal information consistently in a custom metadata field (where available)
- audit data is not readily available because actions occurring in the file system are recorded in one long list in server logs
- a typical server log does not provide specific reports of record deletion without a bespoke PERL script and it will not be accessible to record managers without IT support

Some organisations may wish to configure the filing structure so that only authorised users can delete or remove records and folders. Take great care with this approach as it can become unmanageable.

However an organisation decides to control disposal it should be designed in consultation with users. If the file system (and filing structure) is configured too rigorously users may disengage from it altogether leaving the organisation exposed to considerable loss or mismanagement of information.

Where can I learn more?

- The National Archives advice on retention and disposal:
nationalarchives.gov.uk/recordsmanagement/advice/schedules.htm
- Andrew C Hamer, The ICSA guide to document retention:
www.icsabookshop.co.uk/disp.php?ID=633

Record Management Code of Practice reference

- [Guide 8: Disposal of records](#)
- www.justice.gov.uk/guidance/foi-guidance-codes-practice.htm

Email management

What is email management?

Email is the primary correspondence tool of communicating information within an organisation, between businesses and with members of the public. For any organisation, a failure to manage emails indicates a failing in records management generally.

The scope of this guidance does not extend to all aspects of email management such as establishing protocols for responding to emails, sharing mailboxes or other functionality provided by email clients such as MS Outlook. This section covers the management of emails as records and the means of ensuring they are captured and managed so that they are accessible and usable to all relevant parts of the organisation. Unless stated this guidance refers to the use of all types of mailboxes; specifically those used by multiple users (shared mailboxes) and individually managed mailboxes. The issues arising from the use of either type of mailbox are comparable.

An email is often perceived differently from other formats of electronic record (such as a spreadsheet or text file). As a result users do not always manage emails with the same consistency as they might other records. In practice an email is no different to any other electronic record containing content and metadata and is as unique as a text document or spreadsheet produced with any proprietary software application.

Organisations must train users in how to distinguish between the emails they need to capture for business purposes and the ephemeral communications. The difficulty of this task will vary depending on the volume, content and type of email an organisation or individual receives and produces.

How does email management aid records management?

The ease of composition and transmission of email means that a large number of emails can be created very quickly. This volume can become unmanageable and create a significant risk for the organisation. Capturing emails from an email client into a filing structure helps to place this information in context with other related records. It also ensures that all records, irrespective of format, receive the same level of management in terms of disposal scheduling.

Example:

Name	Date Modified	Type
Copy of Record Management Policy to CEO for approval.msg	24/08/2009 13:21	Outlook Item
Invitation to comment on Draft Record Management Policy.msg	24/08/2009 13:21	Outlook Item
Records Management policy - 1.2 - Draft.doc	24/08/2009 09:52	Microsoft Office Word 97 - 2003 Document
Records Management policy - 1.3 Draft.doc	24/08/2009 09:51	Microsoft Office Word 97 - 2003 Document
Records Management policy - 2.0 Consultation Draft.doc	24/08/2009 11:17	Microsoft Office Word 97 - 2003 Document

This example illustrates the value of capturing emails into the filing structure. Not only can a user see the full process of draft developments but they can also see related communications and build the full picture of this particular activity. To help users understand this and to ensure important emails are not kept in mailboxes, an organisation will need to develop the following:

- management rules that provide clear direction on which emails should be captured out of mailboxes into the filing structure
- training for users to recognise emails as records that need to be captured and managed like all other types (or format) of record

- functional limits to mailboxes to control the amount of emails that a user can keep for any period

Management for rules for email

Management rules for emails depend on other factors outside of records management. These are related to the business process behind responding to and creating emails and include:

- email etiquette, appropriate language
- management of email strings (separate emails for separate subjects)
- titling of the email 'Subject' field to ensure the reason for communication is clear and re-titling it if the string changes subject
- acceptable circulation methods of emails (only include those who need to know, for example)
- circulation of links or references, rather than proliferating uncontrolled copies of documents of unclear status

Emails left in mailboxes are of limited use to the wider organisation, not only in terms of conducting business operations, but because they remain inaccessible and cannot be managed corporately.

Training and technical responses to this problem are a necessity but an organisation must also document a preferred formal process for email management. This does not have to be a lengthy detailed document, it could be a short list of 'do's and 'don't's for capturing and managing emails. Rules will depend on organisational need and the content of the email itself. The management rules should include:

- what type of email should be captured from a mailbox (for example, a decision or a formal request for information or assistance)
- which user is responsible for capturing a record (such as the sender who circulated meeting minutes)
- when an email should not be captured (as in the case of personal correspondence or general circulars or organisation wide memos)
- how emails should be titled when captured into the file system (renaming emails that contain 'RE:' in the title to indicate the content/purpose the response was captured)

- how to manage any attachments
- which file format for capturing emails, such as an .MSG not .PST (this can relate to managing attachments)
- responsibility for a shared mailbox, where used. This will depend largely on the number and use of shared mailboxes within an organisation

This is not an exhaustive list and other rules relating to management of casework processing or specific types of transaction management may also be needed.

It is not necessary to develop these management rules in isolation from those for other types of record. If the rules highlight any unique problems with email management (such which emails should be captured from a long exchange and by whom) they can be incorporated into the broader set of rules developed. This approach would help provide continuity for users in their understanding that records can be produced in many formats and are not restricted to a particular type of electronic record.

Guidance for email management

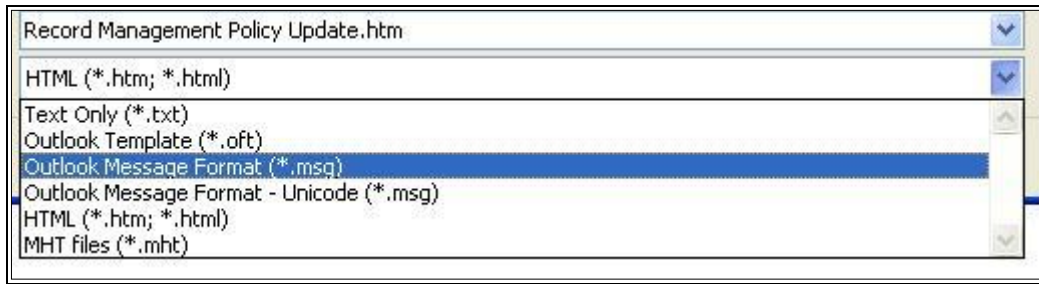
The rules for email management must be supported with guidance and training. The training should include:

- an explanation on the importance of capturing emails
- instructions on how to capture emails from the email client into the filing structure, including preferred file format for capture
- how to decide which emails should be kept and who should capture them
- an instruction on regular review of mailboxes to delete, unnecessary emails
- how to manage emails in a shared mailbox to ensure emails are captured into the filing structure

Email formats

Capturing emails from proprietary email clients into a file system requires some attention to the file format the email will be captured in. Depending on the email client the email may be presented in its own unique format to support the style and functionality of the email client.

Example:



In this example there are six possible formats which the file system will allow the email to be 'saved as' or captured. Not all of these formats will preserve the email in a way to ensure it retains its characteristics as an email and an authentic record.

For example '.html' will create a significantly smaller file of a captured email (as much as 50% in size). This reduces the storage used on servers but the usability, attachments (only a text header indicating their existence remains) and some metadata within the email are completely lost. The result is a version of an email record being captured that is unusable by the organisation and a potential loss of business critical information. Conversely the Outlook Message Format (*.msg), not only remains usable but the presentation of the format would demonstrate an accurate and authentic representation of the email as a record.

The organisation must also take in to account potential file format obsolescence if the email client were to be changed or updated significantly. Older or bespoke email formats are less likely to be supported by a newer email client. This could render the email unusable, or only viewable through a bespoke software application.

Where organisations use other email clients (other than MS Outlook), it cannot be assumed that emails can simply be captured within file systems without loss of information and functionality. The issue is ensuring the logical integrity of emails following their capture so that they remain accessible and fully usable within the designated location.

A very real concern is maintaining access to attachments. The most common are MS Outlook but Novell GroupWise and IBM LotusMail have a broad consumer base. There are many other email clients in use including CC Mail and Eudora. Generally, apart from MS Outlook, these other email clients do not support capture of an email, with its attachments, into a file system without some information loss.

There is a risk that emails will be kept in a format which is either wholly unusable or partially unusable. It is essential to undertake research at an early stage to determine the most appropriate method and storage format for maintaining emails within the filing system, while ensuring the emails remain usable and attachments accessible. For example, a decision is made to capture emails originating from an email client such as IBM's Lotus Mail in a text format (.txt). This particular product cannot provide a file format that retains the email with attachments present outside the email client. As a result the emails are readable but any attachments are lost. With emails used as carriers for single or multiple attachments, the adoption of such a format could result in the loss of information important to the organisation; the attachments are often of greater significance than the text of the email.

It is critically important that any decision to adopt an alternate format should be taken in full knowledge of the consequences. This decision should be preceded by appropriate tests, using emails both with and without attachments to confirm the functionality of the chosen format.

Retaining emails within the email client

Where there is not a suitable technical solution (or alternative file format) organisations should consider creating a mirror of the filing structure within the email client. This structure would consist of a set of shared folders and would be subject to the same naming conventions and access permissions applied to the main filing structure. Emails required for capture would be relocated into the appropriate mirrored folder within the email client. Users would need training to search both the filing structure and email folder to ensure they have found all the relevant records relating to a specific subject or activity.

Example:



Filing Structure



Email Mailbox Structure

This example shows the filing structure and the mailbox structure designed in tandem providing a means of relating emails, graphically in shared mailboxes, to other records in the file system

whilst held in the email client. Duplicating the filing structure in this manner constitutes an additional overhead as both structures will have to be maintained in tandem, but in some circumstances this may be the only viable option. Further sources on email management are provided in 'Where can I learn more?' at the end of this section.

Limitations of email management

There are a number of limitations to capturing emails into a filing structure. These limitations can be categorised under three broader issues. Each issue is expanded below, but all three are often tightly interlinked and dependent on one another.

Volume

Perhaps the most significant limitation caused by email is the ever increasing volume generated and received by an organisation. Depending on the organisation, and a given user's role, a mailbox could be subject to a significant amount of traffic. In such circumstances the decision of what to capture and what is simply ongoing correspondence becomes a difficult judgement to make.

Users might leave emails in a mailbox until it is either full to capacity (thus forcing them to address the issue in order to be able to receive and send emails again) or wait until they have time to resolve the problem. In either circumstance the result can be that email records are not captured into the filing structure with related records and are consequently unavailable to anyone searching the filing structure for all the information they require.

Time

The second limitation is time. The process of creating a draft record using a word processing application requires the action of 'saving' it. This is not a required process in creating an email so users can create and send emails with little time taken, unlike creating and saving other standard records on the file system. Capture of emails into the filing structure requires users to take time out to do this as a perceived extra action.

User convenience vs organisational risk

Storing emails in a personalised structure of an email client as opposed to capturing them within the filing structure provides users with an appealing level of autonomy; they can keep business

emails within their own mailbox where only they can see them. This can result in emails being treated as an individually owned asset within the user's mailbox rather than a corporate asset (which should be captured into a relevant location in the filing structure with record management controls applied and access shared).

The simplicity of automated functionality in email clients (automatically storing a sent copy of an email, for instance) removes the user's responsibility for ensuring an email is kept and is retrievable; the email client is seen as being responsible. Users tend to prefer to retain emails in the email client rather than invest in the effort of capturing emails into a filing structure.

A well designed filing structure, training and management rules can mitigate this attitude but each organisation must accept that a significant proportion of emails are likely to remain in a user's mailbox until the business has been concluded.

Some basic functionality can also help drive compliance and the capture of email. Many email clients allow limits to be placed on the size of a user's mailbox⁶, forcing users to address the problem or be unable to use their email until the backlog is cleared.

This could have a significant impact on daily work (such as processing transactions) and an alternative solution such as 'auto-deletion' after a set date (three months, for example) might be preferable. This approach makes users consider capturing emails into the filing structure more frequently. It also contributes to providing an organisation with a level of compliance with the fifth Data Protection Principle by ensuring that personal data is not retained unnecessarily (names, email address, or personal details listed in the email content).

Both of these approaches are not without limitations. Users may simply choose to drag and drop a large number of emails from a mailbox into a folder within the filing structure to circumnavigate storage limits or auto-deletion. This can only be controlled by management rules unless significant technical expertise is available to customise the file system that prevents such an action. In the event that either method is chosen, the organisation should conduct a risk assessment and develop a policy to support why it is doing this. This may form part of the records management policy or support it as a separate email management policy.

⁶ For MS Outlook the limits are actually controlled on the Exchange Server where each user's email profile is defined and stored

The policy should allow sufficient time to pass before the 'auto-deletion' removes the email. This gives users enough time to assess emails for capture before they are permanently deleted.

Alternative email storage

There are a range of means for storing email outside the filing structure. This section considers the bulk storage of emails in a near or offline email archive including their potential benefits and risks.

Bulk email archive storage

An attractive proposition for storing large volumes of email is to bulk archive them in a near-line or offline server with a search interface for retrieval using a commercial email archiving solution. These products provide organisations with a means of storing large volumes of email in a compressed form increasing the capacity available on a server. The benefits of bulk archiving options are:

- a reduction in IT support overheads trying to maintain a large volume of emails on a live email server
- a reduced cost for server storage (bulk archives are cheaper than expanding live email server)
- a single interface for searching all emails archived, accessible to all authorised users

Most commercially available email archive solutions used coded management rules within the applications that do not represent good records management as practised in the UK.

In particular the method of classifying emails within the archive is based on criteria such as automatically assigned keywords or date of last retrieval. Whilst potentially useful this information does not present the context or purpose of the email to a user when they are trying to retrieve specific emails from the archive. Further risks are:

- storing high email volumes which mean poor search returns from the search interface (insufficient search criteria are available from the archive solution)
- not enough detail known about the email to create an advanced search to narrow the possible returns when investigating the email archive

- record management rules cannot be applied within the archive solution
- access controls dependent on the design of the application which may not reflect the access controls as established within the filing structure, resulting in a potential security breach
- disposal management dependent on the design of the application which will not usually reflect that of the filing structure or organisations disposal policy
- complete aggregations of records cannot be confirmed until the archive has been thoroughly searched

A further issue with these types of archive is that the emails are usually bundled into a large compressed file which removes any relational context of that email to both other emails and records stored within the filing structure.

Bulk email archive file format

A further risk of bulk email archiving using MS Outlook email client is that the emails are often stored in .PST files. These are, effectively, a randomly bundled collection of the emails which is then compressed for storage savings. Other email clients will support a similar process. These bundled files are not stable even when stored in a designed email archive solution. Corruption of an email stored as a .PST file is significantly exaggerated as it is in a compressed form. This could cause irreversible loss of data, possibly without the knowledge of the organisation.

Organisations wishing to bulk archive emails must ensure that the system is sufficiently robust and coordinated so that these risks are either eliminated, or at a level they find acceptable. Irrespective of this decision, the organisation should still produce and endorse a policy of storing critical emails within the filing structure to ensure it is available.

Where can I learn more?

Email Management

- Guidelines on developing a policy for managing email:
nationalarchives.gov.uk/documents/information-management/managing-emails.pdf

Record Management Code of Practice reference

- [Guide 4: Keeping records to meet corporate requirements](#)

- Guide 6: Storage and maintenance of records
- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Integrating management of paper records

Most organisations using this guidance will probably have an existing paper records system. There is a temptation to replicate this system within a file system as it is familiar to the users, can be implemented quickly, and is potentially cheaper than starting from nothing. For some smaller organisations or discreet business units this can be a cost effective and efficient means of building all or part of a filing structure.

It is not always appropriate or meaningful to organise electronic records in the same way as paper records so consider any such initiative carefully. Before looking to replicate any part of a paper filing system in a filing structure the organisation must assess if it is fit for purpose in its current state.

Case Study:

The paper filing system is well maintained and has been developed over time to provide users with easy access to records by function or activity. The supporting finding aids are readily available and up to date. As a result any user could search for and retrieve paper records with minimal impact on efficiency.

Owing to the success of this approach it is deemed helpful that in outline the filing structure in a file system is designed along similar lines with a view to keeping as much information open as is both practical and sensible.

This case study identifies how a paper system could be used as a template for the filing structure in principle.

Case Study:

The paper filing system in an organisation has developed organically with little or no controls, users and business units are left to devise their own preferred ways of filing paper records with no corporate approach or requirement for current finding aids. As a result only users from within that part of the organisation could search for and retrieve paper records.

In a bid to reduce costs each part of the organisation 'copies' their paper filing structure into a filing structure on the file system. This leads to an impossible system whereby users are unable to locate or retrieve any electronic records where they do not have specific knowledge of that part of the filing structure.

This case study identifies how poor planning and management of paper records, copied into an electronic environment, will frustrate users trying to identify where to capture or retrieve records from. It will also lead to a failure in the filing structure as a whole.

In some circumstances an organisation may choose to use the filing structure to record details about related physical records using a simple text file as a place marker. Alternatively where a physical record tracking system is in place it may be beneficial for the organisation to align this with the filing structure (to mirror it) to present a consistent view of the organisations records irrespective of format.

Where can I learn more?

Storage of paper records

In addition to managing the alignment of paper and electronic records an organisation needs to consider how it stores the paper records. Specifically it should consider:

- identifying and categorising the records to ascertain their use, content and volume
- developing and managing a disposal policy concurrent with that of the electronic records held in the file system

- specifying and managing access to the paper records, including any offsite locations
- identifying the usage of the paper records to establish frequently accessed records which may need to be stored more centrally
- tracking and management of the custody of paper records when held in a file store or at a user's workstation
- assessing the most suitable means of storing the records to ensure they are accessible and not at risk from environmental or accidental damage
- development of auditing and reporting on the use, access and disposal of the paper records

These activities will help the organisation ensure its paper records are well maintained and managed to the same level as the electronic records within the file system. More information is available in guidance produced by The National Archives:

- Identifying and specifying requirements for offsite storage of physical records:
nationalarchives.gov.uk/recordsmanagement/requirements-offsite-store.htm

Record Management Code of Practice reference

- [Guide 4: Keeping records to meet corporate requirements](#)
- Guide 6: Storage and maintenance of records
- Guide 7: Security and access
- [Guide 8: Disposal of records](#)
- www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm

Further reading

General Records Management Guidance

- The National Archives Guidance on records management:
nationalarchives.gov.uk/recordsmanagement/advice/default.htm
- The National Archives Guidance on electronic records management:
nationalarchives.gov.uk/information-management/guidance/e.htm
- The National Archive Guidance on digital continuity:
nationalarchives.gov.uk/information-management/our-services/digital-continuity.htm
- Records Management Society guidance:
www.rms-gb.org.uk/resources
- Information Commissioner's guidance:
www.ico.gov.uk/tools_and_resources/document_library.aspx
- JISC guidance on records management:
www.jisc.ac.uk/publications/documents/pub_rmibp.aspx
- JISC Infonet infokit on records management:
www.jiscinfonet.ac.uk/InfoKits/records-management

Useful Publications

- Managing digital continuity:
nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf
- Jay Kennedy and Cheryl Schauder, Records management, a guide to corporate record keeping (second edition, 1998)
- Elizabeth Shepherd and Geoffrey Yeo, Managing records a handbook of principles and practice (2003)
- Effective records management. A management guide to the value of BS ISO 15489 (British Standards Institute, 2002) This is a four part guide
www.bsigroup.com/

Standards and Codes

- Revised Records Management Code of Practice (2009):
www.justice.gov.uk/guidance/freedom-and-rights/freedom-of-information/code-of-practice.htm
- ISO 15489-1: 2001 Information and documentation – Records management:
www.iso.org/iso/catalogue_detail?csnumber=31908
- ISO 23081-1: 2006 Information and documentation - Records management processes - Metadata for records:
www.iso.org/iso/catalogue_detail.htm?csnumber=40832

Legislation

- Data Protection Act 1998, Chapter 29:
www.ico.gov.uk/for_organisations/data_protection_guide.aspx
- Freedom of Information Act 2000, Chapter 36:
www.legislation.gov.uk/ukpga/2000/36/contents
The Environmental Information Regulations 2004, SI No. 339:
www.legislation.gov.uk/uksi/2004/3391/contents/made
- Public Records Act 1958 Chapter 51:
nationalarchives.gov.uk/policy/act/default.htm