The National Archives

Essential Records Management

(A guide to managing electronic records using existing infrastructures and resources)

Contents

Introduction

Purpose

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

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

- Improved business efficiency with increased accessibility to all records.
- Structured management of specific records retained for legal, regulatory and audit purposes.
- Support accurate capture and management of electronic records (irrespective of format) into the file system.
- Retention of a corporate memory of transactions, decisions and actions taken by, or on behalf of, the organisation
- Identifying records required for permanent preservation and archive.
- Help protect the rights and interests of the organisation and others who the organisation retains records about.
- Identify records potentially at risk from digital obsolescence so that they can be maintained under a programme of digital continuity

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

- Establish a records management policy.
- Creation and use of business rules.
- Development of a classification structure.
- Introduction of email management rules and version control.
- Establish user compliance / buy-in.

Without these an organisation is at risk of failing to manage records properly exposing them to risks ranging from reduction in business efficiency to potential legal action.

Throughout this guidance examples of best practice are provided using Microsoft Windows XP and Office 2007 (with Outlook). This guidance is not, however, limited to users of this platform and software applications which are used for demonstration purposes only.

This guidance replaces records management guidance previously published by the Historical Manuscripts Commission[1], and guidance on managing records in Office 97 published by the Public Record Office[2].

[1] Records Management Advice to smaller organisations wishing to introduce a management system

[2] Good practice in managing electronic documents using Office 97 on a local area network environment

Audience

This guidance is intended for use by 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 etc. The document is not aimed at a specific sector or industry.

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

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

This guidance is not restricted to any particular sector or industry. References to specific guidance (i.e. The Records Management Code of Practice) are chosen 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.

Scope

The focus of the 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 application that offer some form of informal document management (e.g. Microsoft Office Sharepoint) may be used but are not referred to in this guidance. Whilst such applications may support record management activities, an organisation still needs to develop and implement clear policies and management rules that will build an identifiable records management culture.

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 business rules, it requires the reader to translate the guidance into best practice in the most suitable manner for their organisation. Inevitably some technical discussion is required. 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.

Examples provided 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, website management tools.

In addition this guidance will not discuss the use of systems or applications used to manage physical records such as a tracking system or library system for the same reasons.

Definitions

This guidance will uses some terms in a specific way these are listed and explained in brief below.

Business Classification Scheme

An intellectual structure that categorises 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.

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.

Filing Structure

A hierarchical structure of folders within a file system that provide a coherent location in to which records can be captured.

The term “filing structure” is synonymous with the term fileplan, however, this term is not used in this guidance as it is typically used to characterise the business classification scheme of an Electronic Records management system.

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

Management Rules

The term “Management Rule” is synonymous with the term “Business Rule”. Within this guidance Management Rules is preferred explicitly for records management within a file system. Either term is, however, acceptable and can be used when producing a rule set for managing records.

Metadata

Data that describes the context, content and structure of all records and folders within a file system.

Operating System

An interface between computer hardware and a user that manages (and coordinates) use of computer applications on a computer with the available resources provided by the computer’s processor.

Record

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[3]

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 shared device (e.g. hard disk or server space) used by multiple users and accessed over either a local area network or a wider area network connection.

[3] International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001

Records Management Policy

What is a Records Management Policy

A Records Management Policy may be best 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 for an organisation from which to build its records management. Where the 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 15489 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.”[4]

Whilst the policy may not be a lengthy document it should not be so vague and broad that no ownership or authority can be attributed to it. As well as being signed off at the highest level possible (i.e. board level) 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 policy and how it aids compliance with specific standards and legal responsibilities applicable to the organisation.
- Detail of the relationship between the policy and other policies within the organisation (i.e. email management or data security policies).

The creation of a policy should be considered as first priority for an organisation looking to improve or consolidate its records management. It should be done in consultation with the business and must be endorsed and supported by senior management.

The policy should remain format neutral encompassing all records created and managed by the organisation irrespective of media. Discussion on specific paper or electronic records management should be provided as supporting guidance underneath the policy.

There should also be a regular review of the policy. The timeframe for review should be at least every 5 years, but with flexibility to review it if significant changes in the business of the organisation require it (i.e. a new business activity or introduction of a new business system).

[4] ISO 15489-1:2001 Information and documentation Records Management Part 1: General; 2001

How does the Policy aid Records Management?

While the policy by itself does not resolve records management problems, it provides an authoritative mandate for implementation across 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 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.

In larger organisations it is more likely that the policy will provide a broad instruction that can be referred to by record managers as their authority for promoting records management. If difficulties with records management operational difficulties cannot be resolved at a procedural level with business managers, reference to the policy can be of great assistance in resolving them,

Example:

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 (e.g. response to subject access requests under the Data Protection Act).

Using incremental implementation of the 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.

Example:

An organisation has not produced a defined records management policy. As a result staff do not have a clear understanding of what records should be kept.

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.

Limitations of a Policy

As necessary and important as the policy is, it will not actively manage records on its own. Indeed that is not its primary use. It exists to reinforce the importance of records management at a senior level and determine the direction of it within the organisation. In order to realise the benefits of the policy an organisation will need to undertake other activities and changes under it.

The process of implementation required to support the 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 governance rules for the use and management of the file systems.
- Establishing a system for monitoring the file systems to ensure records are being effectively managed as intended by the policy.

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

Example:

The organisation has no records management policy (and associated processes) leading to record creation and disposal becoming completely unmanaged and uncontrolled, with vital information not being captured within the file systems.

As a result the organisation is subject to serious legal action for failing in a duty of care with regard to another party's affairs; leading to long-term reputational damage to both the organisation and senior management, who were also forced to resign from their positions.

Where can I learn More?

There is a wealth of advice on records management for all types of organisations. There is, however very little specifically written on the development of Records Management Policies.

Implementation Guidance

- Corporate policy on electronic records; The National Archives, 2000.
- This is a useful and instructive toolkit not only on the reasons for a policy, but also how to plan and develop it. Whilst written for public sector organisations looking to develop their electronic records management, much of the content is useful to anyone developing a Records Management Policy.
- The National Archives Records Management Guides: 2. Records Management Policy; The National Archives.
- This is a brief implementation guide developed to help public authorities achieve compliance with the Code of Practice issued by the Lord Chancellor under Section 46 of the Freedom of Information Act 2000. Again whilst initially aimed at the Public Sector its principles are is as applicable to anyone trying to establish a records management policy.

Examples of Policies

The following are examples of records management policies. They may provide useful text for a Policy, but the wholesale adoption of another organisation's records management Policy is not recommended.

- JISC Records Management Policy
  http://www.jisc.ac.uk/index.cfm?name=pres_rmps
- The Financial Services Authority Records Management Policy and Standards – RMPS
  http://www.fsa.gov.uk/pages/information/pdf/records_policy.pdf
- Record Management Toolkit for Schools – Record Management Policy
  http://www.rms-gb.org.uk/download/730
- NHS CFH MODEL Records Management Policy
  https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/NHS%20CFH%20MODEL%20Records%20Management%20Policy.doc

Filing Structures

What is a Filing Structure

In simple terms the filing structure reflects the relationship of business activities through careful structuring of folders (with meaningful titles) related to the records. In doing this the structure illustrates what the organisation's business is, and provides a means of managing its records

The purpose of a filing structure is to provide an environment where a common understanding of how records should be stored and retrieved can be presented. 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 also allow the organisation to control access more effectively ensuring those authorised to capture and retrieve records can do so effectively, but unauthorised users are not inadvertently granted access at the same time.

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 the use of names of business units (or individual users) should be avoided 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 and manage at a strategic level.
- Reduced efficiency in terms of compliance with the Data Protection Act or Freedom of Information Act.

These problems can be further exacerbated if users move, or leave and business units are created or closed.

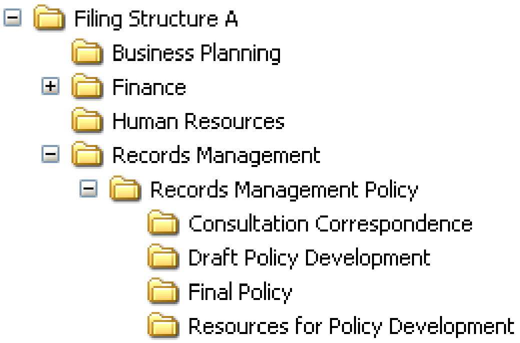
There are many approaches to creating a filing structure and even a number of commercially available tools available to aid organisations when designing (or even re-designing) one[5].

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 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.

[5] More information is available at the end of this chapter under "Where Can I Learn More"

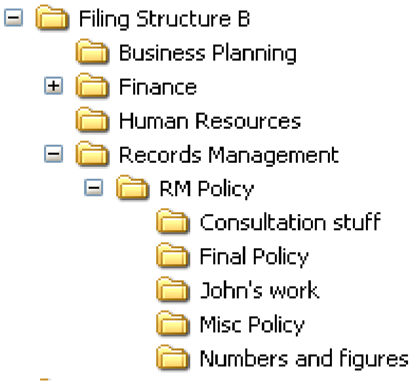
Example



- Filing Structure A
  - Business Planning
  - Finance
  - Human Resources
  - Records Management
    - Records Management Policy
      - Consultation Correspondence
      - Draft Policy Development
      - Final Policy
      - Resources for Policy Development

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

Example



- Filing Structure B
  - Business Planning
  - Finance
  - Human Resources
  - Records Management
    - RM Policy
      - Consultation stuff
      - Final Policy
      - John's work
      - Misc Policy
      - Numbers and figures

This is an example of a poorly designed and managed filing structure with no control over the hierarchy of folders leaving users confused as to where to capture records for any given function.

It is important to bear in mind that the visual representation of the folders is only for display purposes. The actual digital objects (records) are stored randomly and it is the operating system which displays them in a logical order using the folders as a prompt.

How does the Filing Structure aid Records Management?

Within a file system there is very little standard functionality that can be used to control the creation, deletion or movement of folders. In most file systems such options are limited to a simple “on” or “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 gone.

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

Filing structures, therefore, support records management by providing an understandable and accessible location for all records; thereby encouraging users to work within it. This helps an organisation reduce the risk of business critical information being lost within an uncontrolled file system or left in personal drives or email accounts (where it may be deleted without anyone knowing it existed).

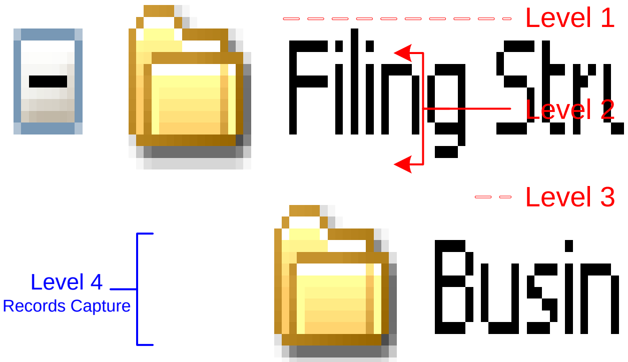
Constructing the filing structure

Designing a filing structure is often a time consuming task, particularly where there has never previously any formal order or agreed layout for records and folders. Whilst there are products that can help with reducing the time it takes to design the filing structure, it will still need to be done thoroughly and with the usability paramount to its ongoing success.

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.

Underneath these sits the fourth and final layer where the records are captured. This is to prevent users from creating sub-folder structures within a particular part of the filing structure that does not conform to the rules so that it becomes incomprehensible to anyone other than the user who created it

Example



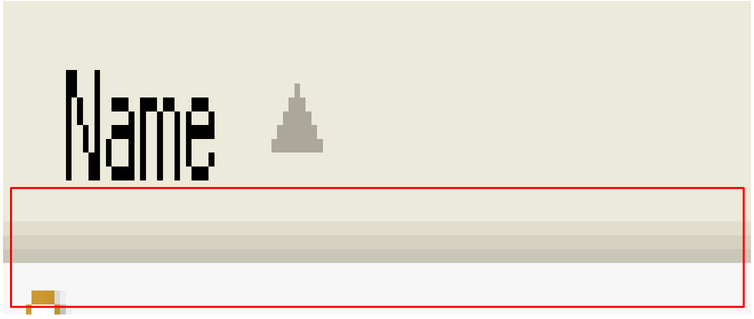
This example shows a basic layout in the MS Windows Environment. Other systems will use different icons and may display the filing structure slightly differently.

The upper folders or Classification Folders should never contain records and if the expertise is available they can even be given a different icon to that of a normal folder to provide a visual distinction to the user.

Creation, movement and deletion of these classification folders will need to be carefully controlled and restricted to a sub-set of users, or in smaller organisations only the records manager(s). This will ensure that any development of the structure is consistent and that inappropriate access or disposal of them does not occur. 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's functionality. This is particularly difficult where users have the 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 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 in relation to disposal because it is not clear if the record should be disposed of under different rules to the folders (and their content) or not.

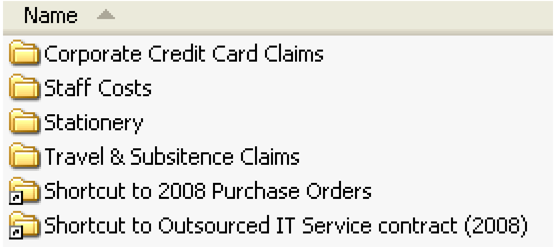
The management rules will need to be supported by frequent monitoring of the filing structure and errors corrected. With significant IT configuration, custom scripting may allow a greater level of functionality within the filing structure to prevent end users from adding records at inappropriate levels of the structure. This guidance does not cover these options as customisation is likely to be expensive in terms of resource and finance.

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.

Whilst this functionality does not exist in a file system, it is possible to achieve some of the benefits of pointers by using the "Shortcut" option in MS Windows.

Example



Name

- Corporate Credit Card Claims
- Staff Costs
- Stationery
- Travel & Subsitence Claims
- Shortcut to 2008 Purchase Orders
- Shortcut to Outsourced IT Service contract (2008)

In this example two folders (in the red box) needed to exist in two parts of the filing structure. Having decided the primary location for the folders a shortcuts were created and located in the secondary location.

This technique can significantly reduce the amount of duplication present in a filing structure; it will also help support organisations trying to respond to requests for information by ensuring only one copy of a record or location for records exists.

Shortcuts, whilst useful, must be used with caution. As they are simply 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 point to anything.
- Inconsistent disposal processing is possible as the record manager will not necessarily be able to locate all shortcuts.
- It presents 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 problems can be summarised as:

- The functionality of a file system (discussed above) present 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 cannot stop users from 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.

This 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 a records management function (either corporately or locally) can help ensure records management activities are being carried out inappropriately.

Where can I learn More?

Designing a Filing Structure / Business Classification Scheme

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

- Business classification scheme [File plan] design, 2003, The National Archives:
  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:
  http://www.rms-gb.org.uk/resources/92
- JISC Infonet HEI Business Classification Scheme, 2007:
  http://www.jiscinfonet.ac.uk/partnerships/records-retention-he/hei-bcs-user-guide
- NHS Purchasing and Supply Agency Business Classification Scheme:
  http://www.pasa.nhs.uk/PASAWeb/NHSprocurement/AboutNHSPASA/Electronicrecordsmanagement/Businessclassificationscheme.htm

Business Classification Tools

The following is not an endorsed list of software but examples that can be used to aid an assessment of a file system(s) to help build a filing structure, as well as address redundancy and duplication.

Other products may be available and each organisation will need to asses whether they need such a service at all.

- a.k.a.® available direct from the Australian developers or in the UK via Inform-Consult:
  http://www.a-k-a.com.au/ or http://inform-consult.co.uk
- One-2-One Classification Software for Records Management:
  http://www.acs121.com/html/one2one.html
- Active Navigation:
  http://www.activenavigation.com/

Management Rules

What are Management Rules?

Records management should be seen as an organisational activity and not software implementation exercise. Without management rules implementation of the records management policy will be very difficult within a file system. 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 that can only be managed by implementing effective management rules.

Within a file system records (i.e. a text document or email) can be moved and edited freely without the actions being thoroughly 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.

The rules provide direction on the conduct of a range of records management activities. These include, but are not limited to:

- Naming conventions for folders and records.
- Management of the file 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. There are, however, some basic principles that should be included in the development of management rules. They should:

- Reflect and reference the good practice presented in the Records Management Policy.
- Be written in natural language (i.e. non-technical).
- Be made available to all users (e.g. via an intranet or central guidance library).
- Indicate where specific records (e.g. 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 benefits 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 or rules that does not allow them to do their job.

Example:

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 operating the records management function discover that the proposed filing structure doesn't suit the way users need to capture records.

Adaptation of the filing structure and management rules through consultation ensures users feel that they have been included in the development process. As a result the organisation develops a good records management culture in which the users do not feel the management rules have been imposed, and are happy to help perpetuate good records management.

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 supportive routine monitoring, management rules build a culture of records management within the organisation.

The other benefits of management rules include:

- Assist users in the conduct of day to day business.
- Improve business efficiency by ensuring all users capture and manage records in a similar manner allowing the organisation to locate information quickly and accurately.
- Encourage better 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.
- Empower the records managers to challenge poor records management within the organisation.
- Provide evidence to external authorities that deliberate and controlled management of file systems is encouraged by use of management rules.
- Translate the record management policy into standardised procedures for staff to follow.

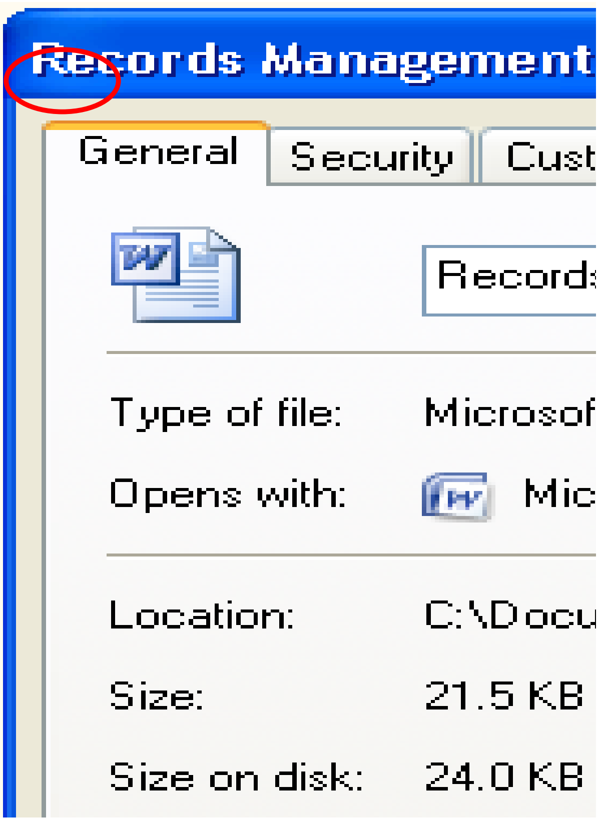
This is not an exhaustive list of benefits, but gives an idea of how significant an improvement management rules are to the use of file systems for records management.

Management of Metadata

Within the context of a formal electronic records management system, metadata is used to provide both informative and functional data about records and folders (i.e. details on how long a record should be kept for and access controls to enforce security).

Beyond controlling access and determining a user profiles, metadata within a file system is purely informative and cannot be used to control the records. As a result most records management functions rely on users carrying out records management tasks accurately and appropriately.

Example



Record

Type of file: Microsof

Opens with: Mic

Location: C:\Docu

Size: 21.5 KB

Size on disk: 24.0 KB

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 (i.e. the server clock is inaccurate) then 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).
- Only a limited set of metadata (i.e. a user access controls) is linked to, or enforceable by the Operating System, resulting in very little automated control to reduce human error.

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 management rules not be followed such as:

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

These are just examples and could be expanded to any extent or variation. Ultimately the rules rely on the good will of users to engage with them. This can be enhanced with a monitoring process by the records management function (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.

Even if well implemented, management rules cannot "do" records management. The users must be prepared to engage and work with the rules and the file system to achieve records management.

As well as being written in consultation with users, the management rules also need to be presented in accessible language (e.g. Plain English). They must also be available through the most practical means so that users can quickly find them for reference.

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 is not intended as a list of rules that can be directly applied, but areas where management rules will be required for **all** organisations using file systems.

Naming conventions

Naming conventions help bring together related records under common folders. They also enable users to distinguish between similar records to determine which is the record they require 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 the object every time.

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.

In addition organisations should consider carefully the use of sensitive information being used within the name of a record or folder such as people's names used in the titling of casework records and folders. This is to ensure that personal data is cannot be inferred by casual viewing of a folder name, but would require specific access being given to that record or folder to obtain any information.

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 it would compromise the content of the record or folder by advertising this in the object's name.

In practice certain records and folders will 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.

Format of Dates

It is very likely that users will want to manage some records, and the folders they are located in by date. Given the range of ways of writing the date, it is important that the organisation choose a standard format for all users to follow. This will note only aid the structuring of folders, but will significantly improve the ability to retrieve information when searching.

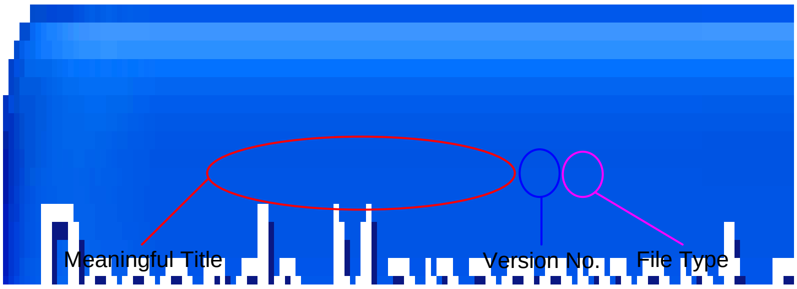
The most practical way of using dates is in the format Year-Month-Day or 2009-08-21. This is the standard format within most database systems as it allows for a much quicker sorting and searching. This is because in reality when searching for older records a user is more likely to know the year, and possibly the month, a record was created; whereas the exact date is not as likely.

Within the MS Windows Explorer view there is a further benefit for users as they can display the list of records (or folders) by date. If the format was Day-Month-Year the user would be presented with an out of sequence set of records as Explorer will only order the first set of digits.

Naming conventions for Record Versions

The means of indicating a current version of a record in any system is difficult. Management rules can aid this process 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.

The following example screen shots show how the addition of simple version suffixes can aid the identification and retrieval of the current version of a record, as well as giving a view of its development.

Example

This example illustrates the addition of a simple decimal system for indicating minor and major changes in the version. In this case 1.0 to 1.2 for draft edits and 2.0 is the version to be reviewed before publication.

Example

This example illustrates a further a suffix that requires the edition of a one word statement such as “draft” that reinforces version number and clearly identifies the records status. Where used, these terms must be very carefully controlled and monitored so that they are used consistently and not misleading. Any lists of controlled terms will need to be reviewed, and updated, at regular intervals.

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

Example

This example shows the consequence of having no management rules for naming versions of records. There is little coherent information and identifying versions and their relation to the others can only be achieved by opening each one and reviewing the content, a potentially laborious and expensive process. This could have a significant impact on records management activities such as disposal, and will also limit the ability to efficiently locate and retrieve the record.

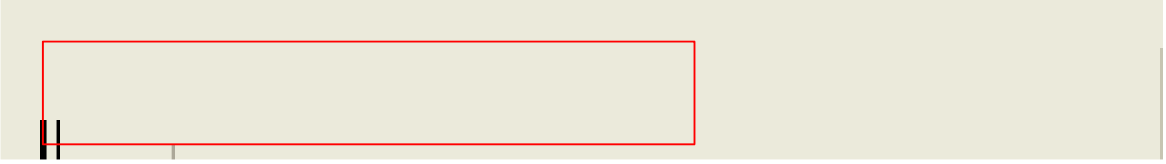
Naming Conventions for Emails

As well as ensuring that users save emails into the filing system there will need to be specific advice and guidance on the naming conventions for emails. When emails are captured from the email client (e.g. MS Outlook) into a file system they are automatically named using the text in the “Subject” of the email. As a result, users must be given guidance on removing the suffixes “RE:” for replies and “FW:” for forwarded emails.

The following examples illustrate the need for users to consider renaming emails when capturing them into the file system to ensure the context of each one is coherent.

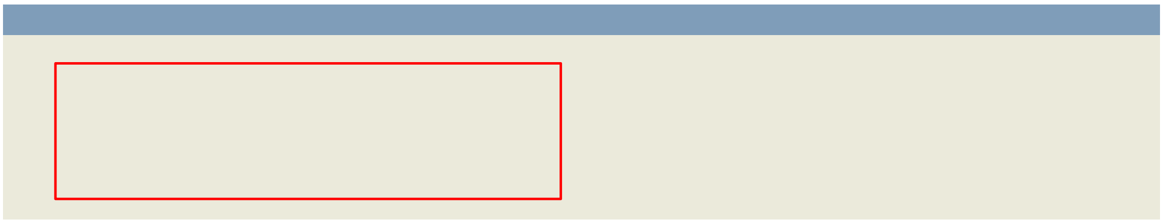
In practice this is likely to require more detailed guidance as there may be several emails captured as part of a record of a longer communication. If all these emails are captured and given the same name, the context and reason for capturing will remain unclear, like this:

Example



This example demonstrates the benefit of providing a meaningful title for each email. Whilst requiring an investment from the user, they now form a coherent set of emails with discernable content and relationship to other records within the file system.

Example



This example illustrates the problem when users do not actively rename captured emails. There is little understanding of what each email was created for, nor why it may have been captured as a result.

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:

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

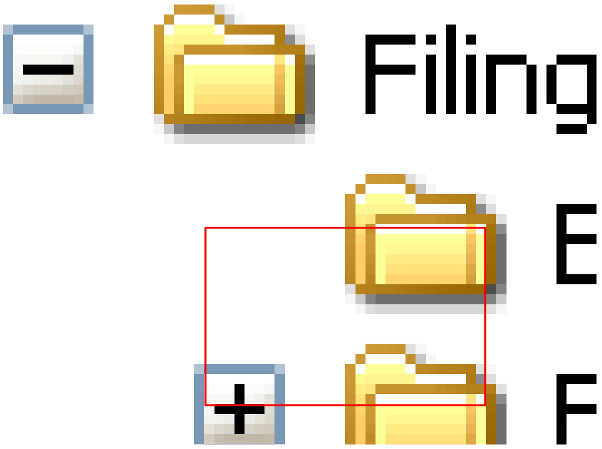
As with the naming conventions for records (including emails) there must be management rules for users to follow when naming folders. Unless this involves strict casework folders the rules do not need to be excessively prescriptive. They can be as simple as ensuring that the name of the folder reflects the intended content.

Example

This example illustrates 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) 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 of folders makes it very difficult to understand the whole structure and where to find specific records.

The folders for records (outlined) provide no means of identifying their content nor 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.

Where Can I Learn More?

For any organisation the process of developing management rules can be difficult. There is little available guidance specifically on management rules, their development and implementation. This is because the process is will be personal to each organisation dependant on size, sector and volumes of records to be managed.

Access Control Management

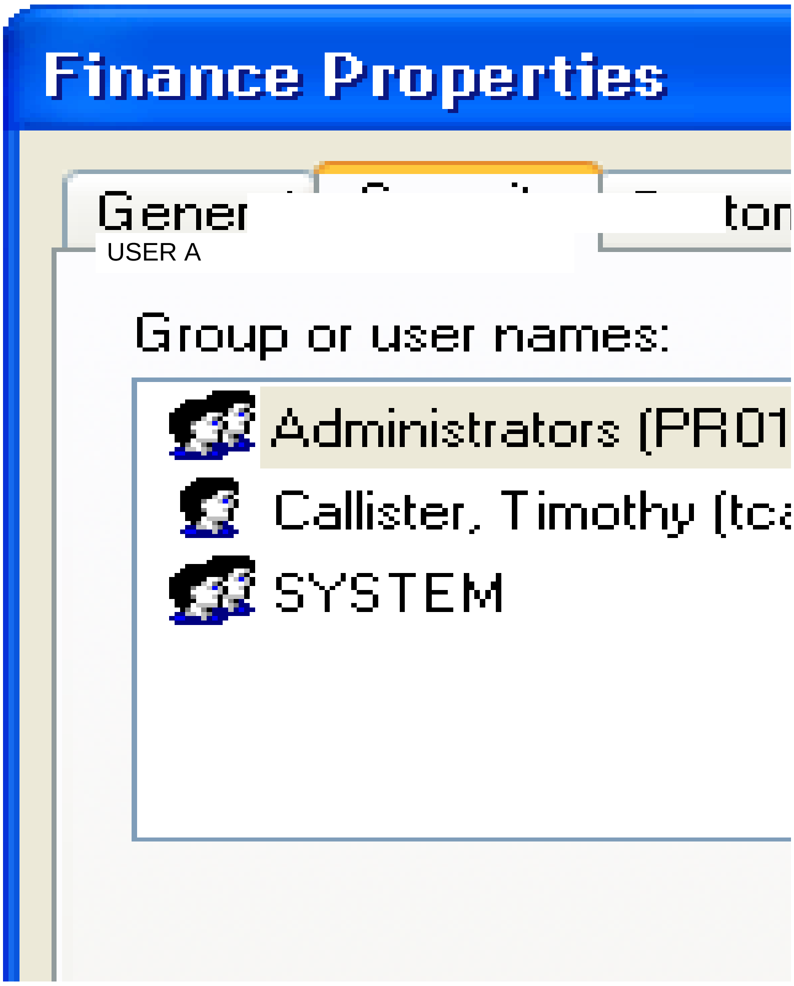
What Are Access Controls?

Access controls determine who can access and capture records as well as access and create new folders. The allocation of access controls allows an organisation to distribute responsibility for records and folders to the creators and managers of them. This accountability helps to ensure that records remain authentic and reliable and help retain their integrity and usability.

Some organisations may provide users with personal drives to store records such as copies of 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. Because these types of drive 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 access to the file system and an email account. 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



Finance Properties

Gener

USER A

Group or user names:

Administrators (PR01

Callister, Timothy (tc

SYSTEM

This example illustrates the “Security” window for a folder in a MS Windows File System. The list of “Groups” and “Users” indicate who has access to the folder. Those listed have the power to add or remove other users to control access as required. Additionally the Administrators can more finely granulate the “Permissions” to indicate what a user can do within this folder such as capture new records or create a new folder.

Using these basic controls an organisation can begin to form access controls across the filing structure that can be used to keep as much information as open as possible / 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 either drive, folder, or record level.

Allocating access controls by individual user would require substantial effort and be difficult to monitor or track. Development of access groups substantially reduces this overhead and can improve the controls placed on any part of the filing structure. This is potentially a very useful means of quickly applying access (or denying it) to a part of the filing structure by an administrator. It is, however, 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.

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. Specifically, a decision is made that the “Finance” folder (and lower folders) requires specific access controls. An access group called “Group A” is created and granted sole access within “Finance”.

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 (particularly where a large number of users are given access).

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. When only individual users require access, an administrator can provide a user with access to the required folder(s) or record(s) and deny access to all other users.

This should not be considered in normal access control allocation as it presents risks that the information will become lost and inaccessible to the organisation if that user leaves (temporarily or permanently), or moves to another business unit.

The success of access controls does not rely solely on the creation of appropriate groups. If the filing structure itself has not be 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 aid the records management function in controlling how and where information is created and accessed. This control 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.

Limitations of Access Controls

There are a number of factors that should be considered when implementing access controls within a file system. This is because 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

Access controls can very easily become complicated and difficult to track. In order to prevent this becoming a significant management overhead access controls should be kept as open as is practical (i.e. 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 so that they are reviewed and updated regularly.

Documenting this process is likely to be difficult as whilst 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 it to be reviewed 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 flinging 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 in an open file system. 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 (i.e. they can 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. The records management function will need to carefully monitor this type of behaviour. In practice this may be difficult to proactively monitor, and for this reason individual access controls should be avoided 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 that such changes are forwarded to records management function i so that they can update any affected access controls.

The same action would also be required when a user leaves the organisation and their IT profile must be deleted to prevent anyone from access 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 effectively prevents anyone other than the user from accessing the object, and circumvents the organisation's access controls. This functionality should either be switched off or actively discouraged. This is because passwords are either too simple to offer any actual security or 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 leaving relevant passwords there is a risk the organisation will not be able to change the passwords. Not only is immediate access an issue it also presents a challenge for digital preservation. Scaled preservation operations that convert records to another format can be significantly hampered if records require password cracking first.

Operational Limitations

A related non-records management issue is the actual 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 (e.g. a new user is added) there will need to be clear communication of the event between the IT and records management function 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. It is recommended 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.

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 schedules[6]. 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 separate and referred by the records management policy.

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 archive[7].. 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 should be based on the established disposal schedules and follow an agreed process for either destruction or transfer.

The disposal process should include reviewing records to understand their current context and content to decide whether it 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 (e.g. meeting minutes) could be disposed of, there must 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 (i.e. a casual email correspondence).
- It is an early draft that no longer reflects or aids the development of a final record.

[6] Sometimes referred to as retention schedules.

[7] Transfer to an archive is likely to be an issue for only a small proportion of an organisation's records.

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.

Supporting this process will be difficult in a file system, but can be significantly supported by:

- Grouping activities together to reduce the overhead in searching and reviewing types of record due for disposal (e.g. financial transactions).
- Using naming conventions (i.e. calling a contact a contract) to help readily identify types of records.
- Introducing of a custom metadata field in the folder or record “properties” 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 will have to be done manually including allocation of a disposal schedule, executing it and recording the event.
- Users may not consistently provide disposal information (where available) in a custom metadata field.
- Audit data is not readily available because actions that occur within the file system are recorded in one long, difficult to search list in server logs.
- A typical server log does not provide specific reports of record deletion without a bespoke PERL script and 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). This must be approached carefully 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 too rigorously configured users may disengage from it altogether leaving the organisation exposed to significant loss or mismanagement of information.

Where Can I Learn More

- The National Archives advice on Retention and Disposal http://www.nationalarchives.gov.uk/recordsmanagement/advice/schedules.htm
- The ICSA Guide to Document Retention; Andrew C Hamer. http://www.icsabookshop.co.uk/disp.php?ID=633

Email Management

Email is now the primary means of communicating business information between organisations. For any organisation therefore, 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 deciding on protocols for responding to emails, sharing mailboxes or other functionality provided by email clients such as MS Outlook. This section will cover 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.

An email is often perceived differently from other formats of electronic record (e.g. 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.

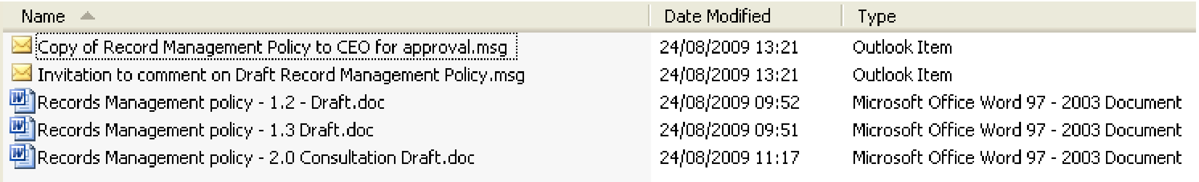
Organisations will need to train users how to identify emails that need to be captured for business purposes from the ephemeral communications. The difficulty of this task will vary depending on the volume, content and type of email an organisation or individual receives and produces.

How does Email management aid Records Management?

The ease of composition and transmission of email means that a large numbers of emails can be created very quickly. Left unchecked this volume becomes unmanageable at a significant risk to the organisation.

Capturing emails out of an email client in to a filing structure helps to place this volume of information in context with the rest of the organisation's 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 it can also see how and when related communications were sent 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 and which emails should be captured out of individual (or group) mailboxes into the filing structure.
- Training 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 will be dependant 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 etc.
- Management of email strings (separate emails for separate subjects).
- Titling the email "subject" field to ensure the reason for communication is clear.
- Acceptable circulation methods of emails (only include those who need to know)

Emails left in individual 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 by the records management function.

Whilst training and technical responses to this problem are a requirement, an organisation must also document a preferred formal process for email management. This does not need to be a lengthy detailed document but a short list of "do's" and "don'ts" in terms of capturing and managing emails.

Whilst the 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 (e.g. a strategic decision or a formal request for information or assistance).
- Which user is responsible for capturing a record (e.g. the sender circulated meeting minutes).
- When an email should **not** be captured (e.g. personal correspondence or general circulars or organisation wide memos).
- How emails should be named when captured into the file system (i.e. renaming emails that contain "RE:" in the title to indicate the content / purpose the response was captured).
- What file format emails should be captured in (e.g. an .MSG not .PST).
- 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 required.

It is not necessary to develop these management rules in isolation from those for other types of record. Providing the rules clearly 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

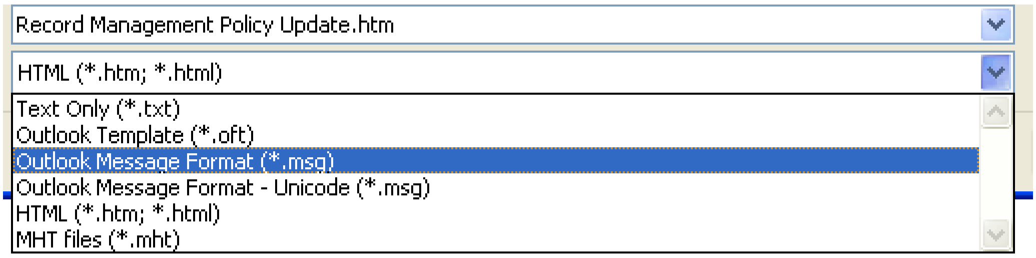
The rules for email management must be supported with guidance and training. For example the training should include:

- 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



Record Management Policy Update.htm

HTML (*.htm; *.html)

Text Only (*.txt)
Outlook Template (*.oft)
Outlook Message Format (*.msg)
Outlook Message Format - Unicode (*.msg)
HTML (*.htm; *.html)
MHT files (*.mht)

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 if the “Text Only (*.txt) format” is selected the user will save only a plain text version of the email. Not only would this format be unusable by the email client, any attachments in the original email would be lost with only a text header indicating their previous existence. The result is an ineffective version of an email record being captured that is of little use to the organisation.

Conversely if the user chose the “Outlook Message Format (*.msg), not only would it remain usable by the email client (and so the organisation) but the presentation of the format would demonstrate an accurate and authentic representation of the email as an email record.

When looking at a preferred file format, the organisation will also need to take in to account potential obsolescence were the email client to be changed or significantly updated. 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.

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 of emails 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.

As a result users may choose to simply 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 is email records not captured into the filing structure with related records and being unavailable to anyone searching the filing structure for all the information they are looking for.

Time

This leads to a second limitation which is one of time. The process of creating a draft record using a word processing application requires the action of "saving" it. As this is not a required process in creating an email users can quickly create and send emails with little time taken unlike the creation of other standard records where the saving action has to be carried out at some point in order to retain it on the file system. Capture of email records record into the filing structure requires users to take time out to do this perceived extra action.

Convenience

Storing emails in a personalised structure of an email client compared outside the filing structure provides users with an appealing level of autonomy. This often results in the mailbox being treated as an individually owned asset rather than a location for the business records managed at an individual level.

The simplicity of automated functionality in email clients (e.g. automatically storing a sent copy of an email) removes the user's responsibility for ensuring an email is kept and is retrievable; as the email client is seen as being responsible. As a result 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, however, 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 such as MS Outlook allow limits to be placed on the size of a user's mailbox[8], effectively 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 (e.g. the processing of transactions) and an alternative solution such as "auto-deletion" after a set date (e.g. 3 months) may be preferred. This approach makes users consider capturing emails in to the filing structure more frequently. It also contributes to providing an organisation with a level of compliance with the 5th Data Protection Principle by ensuring that personal data is not retained unnecessarily (i.e. names, email address, or personal details listed in the email content).

Both of these approaches are not without limitations however, as 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 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. The policy should allow sufficient time to pass before the "auto-deletion" removes the email. This is to give users enough time to assess emails for capture before they are permanently deleted.

Alternative Email Storage

Currently there are is range of ways for storing email outside the filing structure. This section briefly considers these approaches and provides their potential benefits and risks.

Bulk Email Archives

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. With MS Outlook email client the emails are often stored in .PST files that are effectively a bundled collection of the emails which is then compressed for storage savings. Other email clients will support a similar process.

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.

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

Whilst these are attractive benefits, in practice large bulk email archives are very problematic, both technically and from a records management point of view. These risks are:

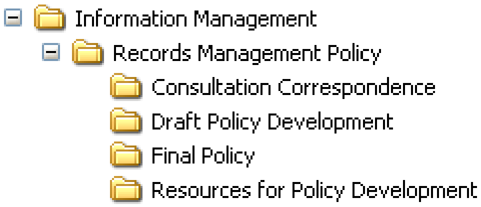
- High email volumes resulting in poor search returns from the search interface insufficient detail known about the email(s).
- Management rules are harder to apply within user mailboxes where it is not possible (or reasonable) to expect a records manager to access and review content.
- The archive software cannot readily indicate the relationships of emails to each other where their name or content is not very similar or the same.
- Context with other records is lost as emails are held in bulk outside the filing structure.
- Mass archive files such as ".PST" files can be unreliable and easily corrupted leading to partial or total loss of data.

Organisations wishing to bulk archive emails need to ensure that the system is sufficiently robust and coordinated that the above risks are either eliminated, or at a level of risk 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.

Retaining emails within the email client

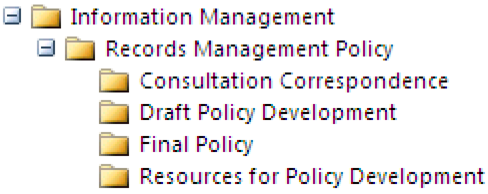
Dependant on the size of an organisation, and potentially the frequency of email correspondence it is possible that the organisation decides not store any (or only very specific) emails within the filing structure. This is likely to be suited more to group mailboxes with a subset of folders that can be designed to reflect part or all of the filing structure.

Example



- Information Management
  - Records Management Policy
    - Consultation Correspondence
    - Draft Policy Development
    - Final Policy
    - Resources for Policy Development

Filing Structure



- Information Management
  - Records Management Policy
    - Consultation Correspondence
    - Draft Policy Development
    - Final Policy
    - Resources for Policy Development

Email Mailbox Structure

This example shows the filing structure and the mailbox structure designed in tandem providing a means of allowing emails held in shared mailboxes to be retrievable by authorised users whilst they remain in the email client.

In practice this should only ever be short-term storage for emails because:

- Shared mailboxes are still only accessible to a small number of authorised users.
- The mailbox structure has to be manually built for every user every time at significant effort and expense
- Changes made in the filing structure would have to be manually updated in every mailbox location in order to retain a consistent approach and structure between the parallel systems.

Where Can I Learn More

Email Management

There is a range of guidance available on email management:

- Guidelines on developing a policy for managing email: http://www.nationalarchives.gov.uk/documents/managing_emails.pdf

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 quickly implemented, and is potentially cheaper than starting from nothing. For some smaller organisations or discreet business units this may be a cost effective and efficient means of building all or part of a filing structure.

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 (i.e. mirror it) to present a consistent view of the organisations records irrespective of format.

Any such initiative must be carefully considered as it is not always appropriate or meaningful to organise electronic records in the same way as paper records. 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.

Example:

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 example indicates how a paper system could be used as a template for the filing structure in principle.

Example:

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 ever find could search for and retrieve paper records.

In a bid to reduce costs it is deemed helpful that each part of the organisation “copy” 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 example shows how poor planning and management of paper records, copied into an electronic environment will not only frustrate users trying to identify where to capture or retrieve records from, but inevitably lead to a failure in the filing structure as a whole.

Bibliography

General Records Management Guidance

- The National Archives Guidance on Records Management: http://www.nationalarchives.gov.uk/recordsmanagement/advice/default.htm
- The National Archives Guidance on Electronic Records Management: http://www.nationalarchives.gov.uk/electronicrecords/default.htm?source=ddmenu_services2
- Records Management Society guidance: http://www.rms-gb.org.uk/resources
- Information Commissioner’s guidance: http://www.ico.gov.uk/tools_and_resources/document_library.aspx
- JISC guidance on records management: http://www.jisc.ac.uk/publications/documents/pub_rmibp.aspx

Useful Publications

- Records Management, a guide to corporate record keeping (2nd Edition); Jay Kennedy & Cheryl Schauder; 1998.
- Managing Records a handbook of principles and practice; Elizabeth Shepard & Geoffrey Yeo; 2003.

Standards and Codes

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

Legislation

- Data Protection Act 1998, Chapter 29: http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx
- Freedom of Information Act 2000, Chapter 36: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1
- The Environmental Information Regulations 2004, S.I. No. 339: http://www.ico.gov.uk/what_we_cover/environmental_information_regulation/legislation_in_full.aspx
- Public Records Act 1958 Chapter 51: http://www.nationalarchives.gov.uk/policy/act/default.htm