Managing Shared Drives and Shared Mailboxes

This fact sheet provides guidance on managing shared resources such as network drives and generic Outlook mailboxes, and on digital records management best practice.

Why good records management is important

Regardless of our responsibilities or roles, good records management helps us work more efficiently – saving us time, improving our working practice, and generally making our working lives easier.

In addition, recent changes in legislation require the University to demonstrate a proactive approach to records management.

Core benefits

Core benefits to good management of shared storage include:

- Easy retrieval;
- Easily identified content;
- Anybody can locate records, regardless if they created them or not;
- Prevents repetition and duplication of work;
- Ensures the organisation complies with legislative requirements;
- Reduces storage burden (electronic records take up 'space' too!);
- Prevents accidental alteration or deletion;
- Minimises the risk of un-authorised access to records;
- Records are deleted appropriately when no longer required.

Note: We use the term **record** throughout this guide. What we mean by a record is any file, document, data or email. All these formats are records and should be managed the same way.

Managing Shared Outlook Mailboxes

For any organisation, a failure to manage email indicates a failing in records management generally. All mailboxes (shared or personal) should be appropriately managed and not used as a convenient storage location or permanent record of past actions. Email should be managed in the same manner as other digital or paper records.

Remember: If your email account is compromised, all the data within that mailbox may be accessible to unauthorised users.

Identifying what email to retain

- Identify what needs to be kept for business purposes;
- Mailboxes are intended for email that has a short life-span, not for permanent storage;
- If you need to retain an email message permanently or for a significant period of time, you should transfer it to an appropriate shared network drive or folder. See Toolkit's guide on archiving email for more information;

- If transferring an email message with attachments to a shared network drive, ensure all information and attachments remain usable. Do not use any system that changes an email or attachment's format into one that is no longer usable, e.g. a text file;
- The less you store in your mailbox the more effectively it can be used.

See Toolkit's Email resource for more comprehensive guidance on email practice.

Managing Shared Drives

Storing all records in a designated folder or subfolder within a clear file structure allows users to navigate, easily manage access, and apply disposal schedules.

File Structures

The top level file structure of the network drives and shared drives (Levels 1 and 2 in the example below) is allocated by IT Services.

Levels 3 and 4 are called classification folders and are created by each business area or team. Level 3 should reflect the core functions of a business area or team. Level 4 should then reflect the activities that are carried out to undertake that function.

This hierarchy of folders represents the relationship between records. Files should be structured logically and consistently to allow users to easily locate all the files which are related to each other or relating to the same activity in the same folder.

Basic layout of a file structure

In the example folder below titled: 'Records Management Policy', we see the progression of the policy from its initial consultation, draft, final and resources (automatically filed alphabetically).

Use of logical names for records and folders

To ensure all users can locate records and folders, use names that are clear and simple.

When naming records and folders:

- When naming individual records: decide on a logical name structure and use it consistently, for example: 'Folder_DocumentTitle_version', e.g. DP_SupplierAssessment_V1.2.docx;
- Create concise but relevant folder names;
- Never use personal or sensitive information in the name of the record or folder. This prevents personal or sensitive data being inferred by casual viewing of a record or folder title;
- Avoid using terms such as 'confidential' as this implies a level of sensitivity that could compromise the content of the record or folder by advertising this in the object's name.

Manage document life cycles

Remember: Electronic records, including email, are subject to the same retention periods as their paper counterparts.

- To find out how long to retain files, check the University's Records Retention Schedule;
- Create folders with common retention periods to assist managing destruction;
- Create a file plan or basic A-Z list of folders to aid content control.

The disposal of records should be undertaken after consulting the Guidelines for the Disposal of Records. This document is the University's formal process for the appropriate means of records disposal to agreed disposal schedules.

Ensure confidentiality and security of files

Folders should only be accessible by authorised members of staff. Folders and documents containing personal or sensitive personal data should be password protected or access restricted to a limited number of authorised staff.

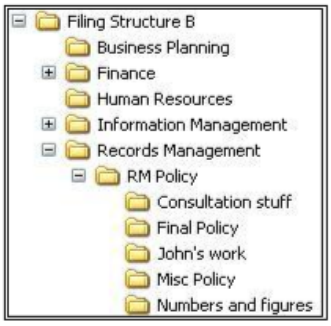
Access to shared folders should be updated when staff begin a role, move to a new role, or leave the organisation. Routinely review access permissions to shared resources to ensure that access is appropriate.

For further information on controlling access, please see Toolkit's File Permissions Management Tool guide.

Practices to avoid

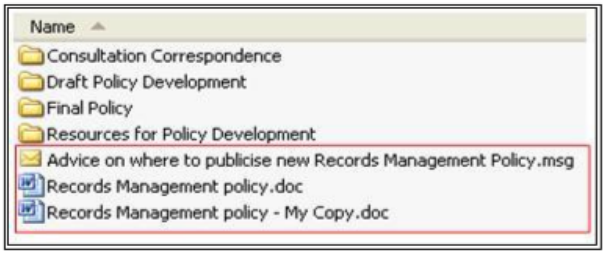
Staff create their own folders

Where there is no control over hierarchy of folders, staff members will have difficulty locating records and folders that they did not create. In the example below, the folder names do not make the content clear nor do they indicate a hierarchy. We should ensure that, even when we are working on a task individually, records can be easily located by colleagues.



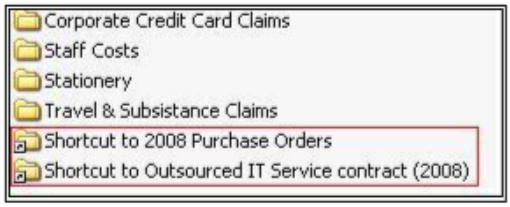
Storing records and files at the same level

Allowing folders and records to exist on the same level disrupts the file structure. In the example below, the relationship between the records and folders is unclear and provides no indication how they should be managed or disposed of.



Duplicated records in multiple locations

It is preferable to use shortcuts to folders rather than duplicate records in multiple locations. Shortcuts create an interactive link to a folder that resolves any conflicts in access, version control and disposal management. Decide what the primary location of the record or folder should be and place shortcuts in the secondary location.



Summary

- Always focus on making your file structure practical and usable.
- If a file structure is too complicated, users will not engage with it.
- No matter how good the file structure is, users can still file records in the wrong folder.
- The Information Governance Team can help and direct you to resources to assist you in creating a usable file structure.

Further information and help

If you require any further assistance, please contact the Information Governance Team