East Renfrewshire COUNCIL

Taking control of our digital records

Name of Record	Taking control of our digital records
Author	SIIO
Owner	CXBM
Date	0.4
Review Date	ongoing

Version	Notes	Author	Date
0.1	First Draft	HJ	16/02/21
0.2	Sections provided for ERC review – 1.Introduction 2.Taking control of our digital records in shared drives and MS Team files 6. Digital preservation and taking control of our digital archives Partial sections of business systems and Hdrive/OneDrive	HJ	07/04/2021
0.3	Update to complete all sections as follows Existing sections updated in light of CMG review Added sections following CMG review 1.Intro - Where to store what table 3. Business systems – existing systems 4. Personal files in Hdrive/OneDrive Added 5. Email and MS Team comms for review	HJ	19/04/2021
0.4	Updated following CMG review	HJ	21/04/2021
0.5	Updated following CMG review	HJ	23/04/2021
0.6	Updated following final CMG review	HJ	25/04/2021
0.7	Minor amendments and restructure	SIIO	29/4/21

Introduction

PLEASE NOTE: this guidance contains a number of best practice tips but is subject to ongoing review as the broader information governance rules emerge.

Digital records fall into two categories:

- Structured, that is, data records held on business systems like GOSS and CareFirst
- Unstructured, that is every other type of digital record, like documents, emails, spreadsheets, etc.

Unlike paper files, where record keeping practice has been long established, the Council has little record keeping and records management rigour in place for its digital information and records, despite the fact that most records are now predominantly received, create, and managed in these media.

Our digital records are dispersed across business systems, network drives, and more recently within M365 Teams workspaces and linked file document libraries. This uncontrolled, silo culture makes it difficult to identify what records and information the Council holds. Legacy data (past its retention and disposal date) is often stored excessively and obsolescence is not dealt with. Council employees do not work in a vacuum – they collaborate and share information with others in their teams, services and across the Council.

The silo culture has impacts here too, with collaboration and sharing often carried out using emails – leading to further duplication of information and effort, and loss of integrity.

The following good practice guidance and tools:

- provide approaches and examples on how to improve the management and use of East Renfrewshire Council's digital records, in line with the Council's Records Management Framework
- will help you fulfil your records management responsibilities as documented in our Records Management Policy and help you work more efficiently and effectively, individually and in teams.

What does good digital records management look like?

Records and information are easier to find:

- Records are filed according to the type of Council work they support, in a controlled filing structure based on the Council's Business Classification Scheme and, in turn, an approved Records Retention Schedule
- Folders and files are appropriately and consistently named
- Records and information that are no longer required to support Council business are disposed of in line with the Council's Records Retention Schedule

Trust in information is increased and co-ordination improved:

- Final version records are clearly identified and are distinct from non-record drafts
- Controls are implemented to protect the trustworthiness of records and related metadata

Costs are better controlled:

- the growth of information and records storage is managed
- the migration of information and records to other systems is improved
- the identification of information or records to be deleted is improved

The guidance is split into the following sections:

General guidance

Taking control of our digital records in Shared Drives and MS Team Files

Taking control of our digital records in business systems

Taking control of our digital records in the "H" drive and OneDrive

Taking control of our digital records in Email and MS Team communications

Digital preservation and taking control of our digital archives

Taking control of our digital records in shared drives and MS Team files

Introduction

Unless otherwise stated, the following guidance applies to the management and use of documents and records in both Council shared drives and MS Teams.

The shared network drives and MS Teams Files (document libraries) collectively provide the main filing areas for staff who work for a specific Council service or team to store, retrieve and work on the digital documents and records they need to do their job.

When a Microsoft Team is created, a SharePoint site is also automatically created. Each channel within your team will correspond to a folder in the document library.

Individual MS Teams with their integrated Files libraries, now provide the Council's preferred active workspaces for business teams, meeting groups and project workgroups to communicate, information-share and collaborate to support current working. However the Council's network shared drives must continue to be used for the long-term storage of official records of council business that require retention beyond their immediate business use. These should continue to be stored in the appropriate area of the Council network drive or business system on line with the approved retention schedule. Any official records created within Teams as part of active work must be moved accordingly.

Roles and interaction between network shared drives and M365 Team Files

This inevitably means that files will need to be moved (or copied where appropriate) between shared drives and specific MS Teams through the course of normal working. Without effective, compliance and consistently applied rules, controls and procedures in place, this way of working can quickly increase the existing business risks we have in relation to unmanaged digital documents and records including file duplication, version integrity and over-retention.

The basic rules for controlling transfer of files between shared drives and File libraries in MS Teams is:

1. Move documents that only Team members need to access and work on from the network to the Team Files document library, making sure you delete the original document from the network drive.

2. Copy any documents uploaded from the network to Team Files for ease of reference to support team work, adding "copy" to the file name of the uploaded document.

3. Identify any finalised official council records that are being stored in Teams and move these back to the correct filing area in the shared drive - or other appropriate Council system - when active work is completed or as alternatively agreed with the MS Team owners.

Creation and capture

When creating and capturing records it is important to think about WHY we are doing this. The main reasons are:

- to enable you and others to find and use them to support current working
- to enable you and others to find and use them to support future work
- to provide evidence of compliance with Council policies and procedures
- to aid compliance with information related legislation and regulations such as Freedom of Information and Data Protection
- to provide evidence for external audits and inspection

For these reasons it is important that when documenting our work, we create and capture records that can be trusted as reliable, consistent, accurate, secure and accessible.

Failure to produce quality digital records leads to financial, reputational and operational risk with adverse impacts on the Council, its staff, the services we provide and the people we provide them to.

The good news is that by following the guidance in this section we can all reduce these risks and work more effectively and efficiently.

What records should we create and capture?

Records are a product of the work that we do. In order to understand which records need to be created and kept, we need to understand how work is being done and how information is being used. We need to be able to distinguish between the records we must keep and the records that can be deleted from e-mail inboxes and working folders on the network and in MS Team files

Business processes and procedures should document what records need to be created and captured and integrated with existing monitoring and audit processes to ensure that these records are being kept and that laws, policies, and procedures are being followed.

What format should records be saved in?

Working documents should be saved in the appropriate editing format e.g. MS Word, MS Excel, graphic application etc… The final, approved document should be saved to a format that all who need access to it can view it but can no longer edit it.

Any “convenience” digital copies that you and your team save because you can’t access the “master” copy should be appropriately destroyed when no longer needed for administrative use. If the master digital record is available to you e.g. on the shared drive, Council intranet, do not create your own copy.

Where should records be stored?

Files should be stored according to content and context– what they are about - and not their format – email, MS Word, paper, image etc…

When a document is ready to be saved, there should be one logical location for it, relevant to the business activity it supports or provides evidence of, in appropriately structured folders on the network shared drive directory or MS Team file library, with appropriate access permissions. Individual documents should only be filed in the very bottom/lowest level folder in the hierarchy.

Digital records and documents should not be stored on your “H” drive, OneDrive, personal email system or other locations which cannot be shared with those who require access to them.

Templates

Where standard letters and forms are required, the use of controlled master templates and forms ensures a consistent and professional format with appropriate branding and document properties, saves staff time and prevents loss, alteration or accidental disclosure of information. This is especially important for documents which are routinely released to the public. Templates should be named according to the rules described in this guidance, saved in template format.

Permissions to create & edit templates need to be controlled but the templates themselves should be easily accessible to all relevant staff to prevent the creation and use of uncontrolled out-dated and inaccurate copies.

Standard file content

It is good practice to add some standard information within the content of the record itself. This helps to differentiate between the “master” set of records and uncontrolled copies as these lose context when printed or digitally stored in a separate location from the master.

Within the footer of each template or finalised document insert the autotext 'Filename and Path' and 'Page X of Y.

Documents must not have the date inserted as an 'Updated Field' or 'Autotext' as the date will change every time the document is opened and consequently the original date will be lost.

Where a document has to go through a review and approval stage, document history and version control information should be included within the document as well as the version number in the file title. Summary version control guidance for Shared Drives and MS Team Files is provided later in this document with more detailed instruction provided in Records Management Guidance Note - Document & Version Control. add link

Managing master records and duplicate copies

If at all possible it is best to avoid creating duplicate copies of the same record by ensuring that the master controlled copy of the digital record is identified and captured into a shared directory accessible to all who need it.

Once the final approved version of document has been completed, it should be locked down to prevent further editing. Either convert it to pdf/a format or change the access permissions to read only for all except designated system administrators.

In certain circumstances duplicate copies are unavoidable, for example, due to business system or file repository access restrictions. Where this is the case, these copies also need to be controlled.

The "master" record should be easily identified. This can be done by providing document control information within the text of the document indicating the location of the master record and that any other copies – digital or paper are uncontrolled and should be destroyed immediately after use.

File naming and indexing

The document should be captured with sufficient information – known as metadata - to indicate the context and content of the records and enable it to be retrieved, used and interpreted and to prove the record is reliable and has integrity. Some metadata e.g. creation date, who created it, what format it was created in, is captured automatically when it is saved. Records also need to indicate the Council function and activity it relates to, based on the Council's Business Classification Scheme. This will also be automatically captured in shared drives and Team Files so long as the folder structure, either in the Shared Drive or in MS Team Files, is based on the BCS. See Structuring shared drives and Team File Libraries below for more guidance on this. Other metadata needs to be created manually. The most important of these is the name of the file which, along with the folder you store the file in, should enable others to identify what the file is about without having to open it. When naming files, you should follow the Council's file naming conventions below.

Our Recordkeeping Metadata Standard add link provides more details on metadata requirements.

Scanning

Council records are now usually created, captured and held digitally. External parties should be encouraged to send records in digital rather than hard copy format. Where hard copies continue to be received, it may be appropriate for these to be scanned and saved to the appropriate filing area. Consideration needs to be given in relation to the legal or evidential integrity requirements of records.

More detailed procedures and guidance can be found in the Council's Scanning Guidance. add link.

Folder and file naming conventions for digital records

Using standard terms and following consistent rules for how we name individual files has a number of benefits for everyone:

- groups related records and documents together and in a logical order
- saves time naming files and searching and browsing for the information we need
- helps determine the relevance of documents without having to open them
- helps identify the most current version of a document
- helps identify obsolete, superseded and out-of-date documents

Naming convention provide a collection of consistent rules followed in naming documents, which should allow users to work effectively, ensure that files can be easily accessed by all who require access and to ensure that individuals are referring to and working on the correct document. The use of consistent naming conventions will improve efficiency by allowing staff to quickly identify the nature of the information contained within a document when searching for information in network drives and in MS Teams.

Provide short, meaningful titles

The title should be short and meaningful and contain, at a minimum, following elements:

- Subject – what the document is about e.g. the "subject" of this fact sheet is "naming conventions"
- Document type – e.g. minute, report, invoice , "fact sheet"

Depending on the content and context of the document, you should include additional information

e.g. for correspondence:

- Date – the date sent or received

e.g. for documents going through a review and approval process e.g. policies, reports, meeting minutes

- Status – e.g. draft, copy, final
- Version number – e.g. V0-1, V2-1

Use templates to embed naming conventions for consistency and efficiency.

Change titles of autogenerated file titling, incoming documents and emails

When saving items such as digital photographs and scanned images, the title should be changed from the system-generated number to a something meaningful. Similarly, provide more meaningful titles for emails that you are saving as records.

Avoid spaces when separating elements in the title

As a general best practice, use underscores "_" or dashes "-" between words in file names. For example: Recommended_File_Name.docx. When you use spaces in file names, all of the spaces will be converted to the characters "%20" in hyperlinks.

Only add dates in file names where you need them

Every document has a Created By and Modified By date in network shared drives and MS Team File libraries, so dates are usually not needed as part of the name of a document. Examples where they might be needed are for events, meetings and dates of sent or received correspondence.

If dates are used in folder or file names, order them in the format YYYYMMDD so they will be listed chronologically**.**

Numbers

When using numbers in titles, work out the highest number that will be required and use the following format so they are listed numerically –

Up to 10 – 01,02,03 ...10

Up to 100 – 001, 002, 003, ...033, 034, ..099, 100 etc..

Personal names

When it is appropriate to include a personal name in the file title (e.g. correspondence, appraisals) it should be given as surname first followed by initials as it is most likely that the record will be retrieved according to the surname of the individual.

Surname · Enter prefixes such as O' (without the apostrophe), Von, Van as part of the surname. · Enter Mc or Mac as they are spelt. · Enter surnames with hyphens as whole units, e.g Smithers-Brown becomes SmithersBrown

Forename(s) Enter only initials, unless the combination Surname+Initial already exists. In this case, enter the full forename.

Avoid the use special characters

Avoid non-alphanumeric characters, such as ? ; : / \ < > * & $ £ + = as they may not be recognised by the software and could prevent the document being saved. Even if Council systems allow you to save the file, if you send it to someone outside the Council, they may not be able to open it:

Hyphens and underscores can be used.

Dots/full stops should only be used to separate the file name from the file extension and not used within the title. Including dots within the title can cause problems when migrating the file into certain information management systems

Avoid unnecessary information

People often include information in the file title that is unnecessary or automatically captured elsewhere: Avoid repetition and redundancy: in particular, the title of a folder should not be repeated in the document title. This will aid efficient searching.

- avoid words that add no value to the title meaning e.g. “a”, “the”, “of”
- so long as the file remains in its current parent folder, do not repeat information already sign posted in the folder name.
- do not include creation or modified date as this information is automatically captured in the properties of the file.
- do not include the file type as this indicated in the file extension and icon

Order of elements and common words

Order the elements in a file name in the most appropriate way to retrieve the record, with the most important element first. Avoid unhelpful or common words at the start of file names, for example 'draft', 'letter', 'presentation', as these will appear altogether in search results.

Sensitivity and security

Do not mark files with their sensitivity or security in titles. Using terms such as ‘confidential’ could compromise content by publicising this in the name. Use access controls to prevent unauthorised access instead (See Information Security)

Abbreviations and acronyms

Avoid using unfamiliar abbreviations or acronyms, especially if the information or records might be widely shared. Only use commonly recognised acronyms or abbreviations. Ideally service areas should agree and document these in local rules, where appropriate. See below

Agree standard terms for consistency

Service teams should develop and apply locally applicable naming conventions to folders and files aligned with the best practice rules described above. This should also include lists of standard terms (including abbreviations and acronyms) to ensure consistent terminology is used for the names of committees, organisations, activities and subjects. These can be set up as controlled terms lists within SharePoint Online.

Version Control

Some records go through a number of versions, starting out as working drafts and then moving on to a review and approval process prior to release as a finalised record. It is important to be able to differentiate between these various drafts, using a consistent version numbering protocol at the end of the file name.

Here is an example of a simple protocol for version control:

- Draft documents - V0-1; V0-2; V0-3 …
- Approved document – V1-0

When an approved document then moves into a new review phase e.g. annual review of a policy,

- Documents under review: V1-1; V1-2; V1-3 …
- Approved updated document: V2-0

The document control history of more formal review processes should also be documented within the content of the document, ideally using a formatted document template (see section – Creating and Capturing Records for more info on templates)

Version control in M365

M365 automatically saves the changes you make to files stored in Team document libraries and stores the last 500 modified versions of the file. Old versions are not found during searches, but you can examine old versions of a document by viewing it within SharePoint Online and selecting View Version History.

This is excellent from a business continuity perspective and also provides an audit trail of changes. However it does not address situations where you need formal document version control. In these instances you should follow the version control advice provided above.

For more detailed guidance on version control see the Records Management Guidance Note - Document & Version Control. add link

Naming folders

The names given to folders should enable the viewer to instantly identify the contents within the folder.

The principles below must be followed when naming folders:

- Folders must be clearly named by a relevant and meaningful subject area
- You may have spaces between words but no dashes, commas, abbreviations or jargon.
- Only create folders with organisational or departmental names when the content is demonstrably team focused, for example, team meeting details, business continuity documents, work plans etc.
- Folder titles should not be repeated in the hierarchy. For example, if the top level is **Procurement**, the second level should read **Strategy**, rather than **Procurement Strategy**. The only exception to this rule is where a proper noun is concerned, e.g. where the second level reads **Procurement Strategy Committee (PSC)**, as that is the name of the committee itself.
- Use date subfolder folders to help manually manage retention and disposal of information and records in line with the Council's record retention schedule

The next section provides more detailed advice on structuring folders on shared drives and in MS Team file libraries.

Structuring shared drives and Team file libraries

Logically structure filing systems on the shared drives and in MS Teams will help you to identify and organise the digital records that you need to keep. The benefits of using agreed and controlled filing systems include:

- it provides a standard way to organise and save records across a department, service or work group
- related digital records can be organised consistently, whether on shared drives or Team file libraries
- similar records are kept together for easier filing, retrieval, retention, and disposal.

Developing folder structures to support digital records management

Council services and teams use network shared drives and MS Team Files to store a mixture of records, working files and reference material. In order to identify records, service areas should have folder structures that support easy identification and management of these three distinct groups:

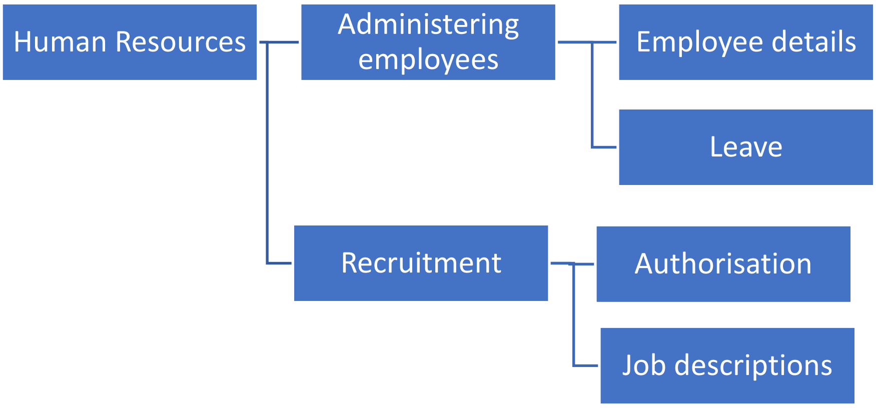
- a folder identifying finalised records to store and classify the final aggregated record of the completed business activity
- a folder structure to store and share non-record drafts, other working files and reference material to support the activity – where relevant
- a virtual library or knowledgebase for sharing reference material across the Service or organisation – clearly indicating which are internally created and which are third party resources

The benefits of segregating content are:

- allows staff to distinguish records from other content;
- helps staff and operational IG to delete working files;
- improved migration to more suitable systems.

Activity based folder structures

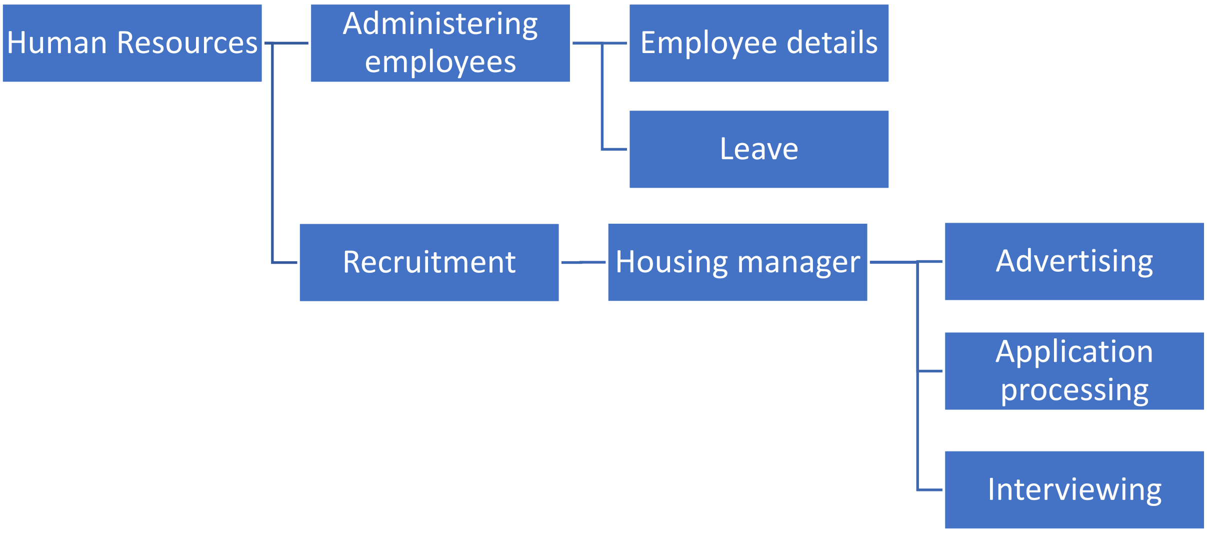
Documents and records should be stored in a hierarchical folder structure based on main business functions and associated activities and processes in line with the Council's business classification scheme. This has the advantage of organising information based on the way in which work is carried out. The following diagram illustrates a logical structure based on some activities related to the HR function.



Subject and case files

In some cases it will make sense to organise information by subject, e.g. regular meetings, general correspondence with an external agency, guidance material on a specific work area.

Case files should be used where records relate to a specific time-limited entity or event, e.g. recruitment for a new post, processing of a planning application, a client complaint investigation. In these cases the lower folders will identify the activities related to the process with a top level folder identifying the specific case, e.g. by case number and entity title. The following diagram is an example of a folder structure for organising records related to a recruitment campaign:



Developing the structure

The goal is to find a way to organise the information that makes sense to everyone who needs access to it. All staff need to be involved in this process and to receive awareness training on how to classify their documents using the system once it has been put in place.

The top two levels of shared drive structures should map to the Council's Business Classification Scheme. Lower levels of shared drive structures must reflect the needs of the service or function. It is the responsibility of the owner of the parent folder to agree names for 'child' folders by reference to the Business Classification

Scheme and controlled subject/entity terms. This process should be managed in agreement with the users of potential 'child' folders.

Ideally, folder structures on shared drives and in Team files should not exceed four levels of subfolders to make it easier to file and find documents and to ensure that the file path of the document does not exceed the maximum allowed length of characters.

The filing system should be reviewed by relevant staff two or three times during the development process to ensure it makes sense to them and to find out if anything has been missed.

Access and security

Digital information must be protected from unauthorized access and use. An important task when developing the folder structure is to identify the records to which access should be limited. Decisions regarding access rights cannot be made in an ad hoc fashion. They should be based on an analysis of record content and user needs. They should be based on job categories, and not on individuals, so that all of the employees who are in a certain job category have the same rights to use these areas of the shared drive.

Appropriate access levels and read/write permissions to use shared drive folders should then be established so that users cannot view confidential or personal information that does not pertain to them or that they do not require to do their jobs.

In MS Teams, all team members have full read and write access to all folders and files within the default General channel folder via the Files tab as well as any and folders linked to additional standard channels in Files and that are created.

In M365 sensitivity labels are used to provide the relevant level of protection to information and documents, based on the Councils Information Security Classification Scheme. By default, all documents in MS Team Files have an Official label applied. On creating or uploading a new document that contains Official-sensitive information you must select the appropriate Official-sensitive label to that document. All members of the Team will still have full read and write access to these files if they are stored in a standard Team channel.

Private channels can be created where there is a business need to restrict access to files (and channel posts) to a select working group of Team members for reasons of sensitivity and confidentiality.

Managing folder structures

Controlling the folder structure

Once developed, agreed and built on the shared drive or MS Team library, a control process should be put in place to restrict the ability to add, delete or modify the filing system. If this doesn't happen the logical structure will soon give way to one of ad hoc chaos and individual rather than collective need. Required changes to the structure, including access rights, should be subject to a controlled change management process but should be designed so as not to impede end-user working, forcing them to "break the rules".

Managing "work in progress" files

By creating a "work in progress" subfolder within sections of the folder structure, you can separate draft from finalised records. This will help to identify the master record - the most complete record of an action, transaction or decision. It is this record that you rely on to take actions and make decisions. However it is very important that the use of "work in progress" folders is controlled to ensure that finalised versions are actually moved to the proper final filing location and obsolete working documents are deleted.

Housekeeping

It is good practice to carry out basic housekeeping tasks, enabling you to self-monitor and ensure that you are managing document and records in the best way to support your own working and that of your colleagues. Good housekeeping also enables you to meet the records management requirements of you, your team, your service, and the Council as a whole.

Even within a logically structured and controlled filing environment, you will still be creating and receiving documents and information that only need to be retained for a short period of time and can be destroyed as soon as they are no longer of immediate business use. These are often referred to as non-business records or transitory records.

In most cases the following types of records will have no significant operational, informational or evidential value requiring their retention. They may be destroyed as soon as they have served their immediate reference purpose. Files should be regularly reviewed and weeded of such material.

- files kept “just in case”
- convenience copies of policies, procedures, guidance
- files which have been created for temporary use and for one-off exercises e.g. to do calculations, data manipulations, labels, signs, posters etc
- information collected for complete projects where you were not the lead officer or where specific issues have been resolved
- files of a personal nature, eg. photos, social events, jokes etc. – these should never be saved on a shared drive or in MS Teams.

File clear-outs and rationalisation

A key step in moving to controlled filing environments in shared drives and MS Team, in line with Council RM policy including implementation of records retention rules, is to carry out file-rationalisation exercises to identify and action:

- Records supporting active work
- Records of completed work that have longer term retention requirements and must continue to be accessible, protected and properly maintained.
- Records that can be immediately deleted

The following table provides advice to help you and your team to identify which of your digital files need to be kept for business, legislative and historical reasons when no longer of active business use and what can be deleted, once no longer of active business use. As well as supporting clearance and rationalisation exercises in shared drives and MS Teams, it can also be used for initial clearance of email boxes, H drives and OneDrives.

Items marked “no” should be deleted as soon as possible, once no longer of active business use. Items marked “yes” should be retained in the appropriate area of the Council’s network drive. Refer to the Council’s records retention schedule and associated guidance to establish how long these identified records need to be retained.

How to identify a record	Is it a record?
Duplicate copies of records where the authority copy is held elsewhere	No
Early drafts and drafts for comment	No
Files which have been created for temporary use and for one-off exercises to do calculations, data manipulations, labels, signs, posters etc	No
Drafts reflecting significant changes in approach	Maybe - will require further review
Final versions	Yes
Final records of project: Initiation Documents Interim and final evaluation reports Project Proposals Project research, feasibility studies, plans, specifications Terms of reference, minutes, agendas, etc.	Yes
Records that may require transfer - High profile or innovative projects concerning changes to Council policy, planning and business	Yes – also offer/transfer to Council archive service
Outputs of interest to wider Council	Yes – also publish on Intranet
Outputs of project produced for other areas of business	Yes – transfer to business owner – may need to retain copy as part of project record

Don’t Allow Files to be Orphaned.

Files left behind by staff who no longer work at the Council or have transferred out of a department, or by a department which has moved to a new location, are called Orphaned Files.

There should be no files in any business unit whose current purpose, contents and owner cannot be identified. When there is no owner or person to take responsibility it is difficult to manage them. Staff do not feel empowered or comfortable disposing of them, since no one really knows what they contain. This can pose a problem, because if the contents are unknown the risk is then unknown.

Misfiling and misnaming

When we are in a rush it is easy to misfile information or name files in a way that, at a later date, makes no sense to ourselves or others. Also, when we can’t find a work folder to save a file to, it is tempting to create a new one, e.g. miscellaneous or general.

These are all sure-fire ways to lose information and to waste time trying to find and potentially recreate the information. When you come across digital files that have been misfiled, take the time to move them to the correct place. If you come across files that need be opened to find out what they are about then clearly the file name could be more meaningful. Again, take the time to rename the file to aid future retrieval. Team managers should monitor the use of folders and file naming conventions and organise staff training and clear-up sessions to ensure that effective and efficient file creation, filing and naming becomes part of normal working practice.

Retention and disposal of digital records

Retention and disposal of digital records should be managed in shared drives and in MS Team files order to:

- accountably dispose of records in a timely manner;
- reduce the volume of information and records stored;
- dispose of outdated, irrelevant or duplicate information or records; and,
- prepare for migration to another shared drive or more suitable system.

The Council's Records Retention schedule add link provide rules for the retention and destruction of records, and identifies records that have enduring historic value and should be transferred to the Council archive for permanent preservation.
All digital folders on network shared drives and MS Team files must be managed according to ERC's records retention schedules.

Folders that are in continuous use should be closed annually. For example, for agendas, minutes and background papers for meetings, 'archives' should be created annually so that efficient information management, including retention and disposal, and retrieval can be maintained.

A folder should also be closed if the work associated with it has ceased, for example a project or contract is completed or an employee leaves the Council.

Retention and disposal responsibilities

The functional area of the Council that owns the record is ultimately responsible for implementation of their section of the Records Retention Schedule, wherever it may apply across the Council, although operational practice may rest within other areas, requiring close collaboration, including ensuring that relevant managers are fully aware of their requirements of the Retention Schedule and apply accordingly.

Folder structure design to support retention and disposal

Retention can be complicated if records with different retention requirements are filed together. Services should consider retention periods when designing the records filing systems on shared drives and in MS Team File libraries to avoid this issue.

Where relevant, make subfolders for each year. This makes it easy to know how old the files are when it comes to retention and disposal. You can then review files folder by folder, instead of opening each folder to extract materials which have passed their retention periods.

Applying the retention schedule in shared drives

Retention can only be applied manually in shared drives; therefore roles and responsibilities must be assigned and followed. The Records Retention Schedule should be applied annually.

To identify time-expired and redundant information when applying a Records Retention Schedule, or during a clean-up, information and records can be sorted within folders by when they were last modified. File analysis tools can be used to speed up this process but must be used as part of file clearance strategies that ensure that any authority copies of records that represent high value or high risk to the Council are identified and appropriate action taken to ensure they are not inadvertently deleted.

Applying the retention schedule in MS Team File libraries

Retention and disposal of files in MS Team file libraries that need to be retained as the Council authority record beyond their active use, will not be managed within M365. As noted above, these records will be saved back to the appropriate Business System or area of the Shared Drive. Retention and disposal of the remaining files in

MS Team document libraries is applied automatically using M365 retention policies, configured based default rules agreed in line with the Council’s integrated business classification and retention schedule.

The Council’s M365 Information Governance Policy, once developed, will provide details of what these agreed default are.

Disposal of duplicate copies

It is very easy for multiple duplicate copies of digital information to exist so when disposing of digital records it is vital that all the various locations that a file could be stored have been considered.

Staff with access to digital records that are being deleted should ensure that any copies held anywhere in their email folders, files stores and recycle bin are also deleted to ensure completion. Items held in these locations are still held for the purposes of the Data Protection and Freedom of Information legislation. Deletion of a digital file removes the link to the file but it is possible that the file contents could still be retrieved using technical measures. Consequently, adequate security must continue to be applied to file locations and devices used to hold them until they have been fully erased.

System backups

System backups will continue to hold copies of deleted digital records until such time that the backup is deleted. Whereas the requirements of the Data Protection and Freedom of Information legislation technically still apply to such records, the Information Commissioner’s Office have taken a pragmatic approach to this type of content, recognising that it is possible to put it ‘beyond use’ while still held so rendering it out of scope. This will only apply if there is no intention to access or use it again, and it would require disproportionate effort to retrieve. However, such records could still need to be retrieved if subject to a court order.

Closing files to apply retention

One person in each team or service area can be given the task of reviewing digital records and applying retention schedules. This would involve “closing off” folders at appropriate times, e.g. end of the financial year, end of project, completion of transaction, close of case. These are typically indicated in retention schedules by the retention “trigger.” To close a folder, change the security restrictions on the folder to view only and rename the folder so that it is clear that it is closed.

Interpreting retention triggers

The trigger is the event that prompts the start of the retention period.

There are three common types of trigger:

- a defined point in the business process it supports (for example, termination of a contract or project, closure of a service user case file)
- on a calendar date, often the end of the current year to which the record relates. Where this is the end of the current financial or academic year, this is specified in the schedule based on what makes most sense operationally.
- when superseded or obsolete e.g. policies, procedures and guidance

As triggers are so tied into business processes, an important step in the implementation of the Retention Schedule for different Council areas will be to map the trigger to a specific business process step. For example, within the staff termination process, project closure process or approval of revised Council policy, procedure or guidance.

Calculating retention

If the record series is retained for the current year plus a number of years, calculate the retention period based on the example below:

trigger = current, retention period = 2 years:

- retain documents in this record series which are dated in the current year (2021) plus the next two years (2022 and 2023)
- destroy the records in 2024

If the record series is retained for a number years after an event occurs, for example termination of contract or termination of employment, calculate the retention based on the example below:

trigger = termination of contract, retention period = 5 years:

- retain documents in this record series which are dated in the current year (2021) plus the next 5 years (2022, 2023, 2024, 2025, 2026)
- destroy the records in 2027

Taking control of digital records in business systems

RM requirements for new systems

East Renfrewshire Council is committed to delivering a paper-less working environment and to using digital information systems as far as possible.

Central to the sustainable delivery of these goals is that good records management and information governance principles are built into the scoping, procurement, implementation and use of any new business systems which are deployed to ensure the proper management of both structured and unstructured data held and processed by the system.

While the specific requirements of any information system will depend on the particular need identified, there are a number of principles and requirements which should be considered as part of wider system specification.

For full Digital Document and Records Management systems, there is an international standard - ISO 15489 - and model compliance guidance has been issued by the DLM forum through their MoReq standard.

This guidance note makes some recommendations for consideration in relation to all digital records systems across the Council. It should be considered in conjunction with the further records management and information technology guidance noted at the end and with the advice of your IT Business Relationship Manager. Also, remember that any new system should be appropriately referenced in the Council's information asset register.

Perhaps the first consideration should be whether a new system is needed at all. Check with your Business Relationship Manager - the Council may already have a solution which will satisfy your requirements.

If the system is required, there are a number of options for the management of documents and records related to the Council function that the business system supports.

- Within the business system itself
- Within electronic document and records management system – e.g. M365 SharePoint Online - integrated with the business system

- Within digital document and records/content management system – ie M365 Sharepoint online – exported from system to M365

Clarity in strategic goals

Be clear what you need from the system. It has to be fit for purpose. Don't use a system which does not fulfil your requirements; don't pay over-the-odds for something with excessive redundant functionality.

Appropriate resourcing

All too often digital information systems fail to deliver not because of any problem with the system itself but because there is no proper commitment to the amount of ongoing support and resourcing required to properly utilise them. Consider what will be required for training, for ongoing administration and support and ensure that this is factored in to any assessment of the project. No information management system is simply "plug and play"

Functional and non-functional records management requirements

Not all of the following recommendations in the tables below will be necessary in all systems, but due regard should be given to each when specifying new business system requirements.

Functionality	Summary Requirement
Create/capture	Ability to capture and manage all required file types Automatically apply metadata to files on creation, import to the solution and when IG rules are being applied retrospectively. Set up templates so that as much required metadata as possible is automatically captured on creation including standard file naming
Edit document	Ability to edit draft documents Ability to redact, or annotate finalised documents while maintaining the original
Version control;	Automated version control

Document and process workflow;	Ability to create workflows that link business process with related document(s)/data e.g. sickness absence interview outcome letter and review/approval/email process
Desktop/online MS Office Suite apps integration	Decent integration including Outlook
Scanning;	Ability to scan hard copy docs direct to the solution
Security and privacy	The security of the information in a system will be largely dependent on the broader procedural and technical environment but consider whether any other measures are required. Access controls and audit functionality are important in protecting both the authenticity and integrity of the record. Also, consider whether a Privacy Impact Assessment should be undertaken if the system will be processing personal data and ensure that the Council's Information Security Schedule is included in any procurement exercise
Records declaration	Ability to finalise/declare information as a record - that is they should be able to hold information in an unchanging form when required. Once declared as a record, to establish its accuracy, authenticity and evidential integrity, the content and the relevant metadata should not be capable of being changed. Audit functionality should make clear when records were last accessed and amended, and by whom and how Ideally this should be automated or controlled manual process as part of workflow process. Should have ability to declare as record on capture where relevant eg a third party document or internally generated letter that has been sent.
Retention and disposal;	Business systems need to be able to delete records once they have reached the end of their retention. Make sure that any system you are considering has this functionality and that this is properly deployed in accordance with the Council's records retention schedule. Corporate retention and disposal rules for different types of records and information can be configured within the system Ability to dispose of finalised records in line with retention periods; permissions to do so should be restricted to authorised staff.

	system can flag/report on records due for review/deletion; where/if appropriate, system can carry out automatic deletion Ability to retain a deletion stub when a record is disposed of recording the details of when it was deleted and by whom – provides evidence of compliance with agreed retention rules should not prevent appropriate disposal of drafts, duplicates and working documents once a report or action has been completed and recorded, in line with agreed life cycle/weeding rules.
Recordkeeping Metadata	Ability to add as metadata, the required information about the documents/records and ensure that the system will properly maintain that. Metadata is an integral part of the record and the system should automatically record it, preserve it, and allow for its ultimate disposal or export. Where appropriate, ability for metadata to be inherited by individual documents within a series of related records The Council's Recordkeeping Metadata Guidelines sets out minimum metadata requirements for recordkeeping and includes a metadata template that can be used to map the recordkeeping metadata elements in the guideline to the equivalent field and tables in each database or business system that holds Council records.
Search, retrieval and view (render)	Good search and retrieval functionality based on combinations of attributes/metadata linked to the information Potential to save common searches (especially complex ones) so only the different parameters need to be entered
Taxonomy and structure	However good the search functionality is within the system, it will not be able to adequately fulfil its information governance role if the records within it are not stored or displayed within a clear and logical hierarchical structure – this can be enabled either by folders or by metadata associated with individual/groups of records
Backup	ability to be properly backed up and to be test restored. The responsibility for this and for ensuring the continued availability of the records needs to be

	clearly assigned.
Sys administrative functions;	Only authorised staff members should be able to carry out certain activities eg disposal of records at the end of the agreed retention period, changing of retention periods; adding, amending and deleting terms in pre-defined index lists
Hybrid file management	Ability to link data and files in the system to those held in other systems – digital and physical, This will enable the new system to be the single point of access for full staff record including active and closed
Digital preservation	Functionality to enable long term accessibility, integrity, confidentiality preserve integrity etc beyond life of system and ability to convert content into industry-standard long term preservation format – PDF/A
Import tools	Tools to bulk import documents and related metadata and ability to flag any missing mandatory metadata (assuming that you will be importing existing records/docs that need to be retained.)
Export tools and strategy	bulk export tools enabling the migration/transfer of electronic records including all metadata and audit trails in industry standard formats, to other parties/replacement systems Few digital records systems last more than a decade. It is likely that at least some of the information within them will be required beyond that timescale. Ensure that you are clear how you will facilitate that when it comes to moving on. Also, if there are data within the system which will need to be permanently retained as part of the Council's archival records, consideration needs to be given to their long-term management.
Ease of use	Any system has to be able to support the often-complex Council function that it is designed for; but it also has to be accessible to the staff who will be using it. When assessing different solutions against functional requirements, it is important to assess, not just if the solution has the required functionality, but how easy and effectively it achieves it.
Performance and scalability;	The solution must be scalable for future information growth and performance should be maintained as the amount of data increases.

Reporting	Reporting functionality to supply management information and KPI data from the system – or ability to integrate with a reporting tool that can
Interoperability, system interfaces and integration	Council systems should be able to relate to each other. Security is of course vital, but avoid bespoke systems which develop silos of data which cannot be reused for other appropriate purposes. M365 Secure file transfer/access for external parties Mobile/remote working Publishing to web Management reporting/dashboard Integration with line of business systems
audit trail/reporting of data processing	Audit trail/reporting to provide details of the following transactions: • Viewing documents, • Changing documents and metadata, • Deletion of content, • Permission levels, • Retention schedules, • Disposals • download and exports The audit trail should be easily accessible, and available on each individual record, to enable fast and accurate searches when they are required.

Implementing RM in existing Business Systems

The Council's existing corporate business systems like GOSS and Council service/function specific business systems like CareFirst also store and process digital information and records that need to be properly managed in line with Council Records Management Policy. This will be achieved by implementing minimum records management standards for each system.

The key steps that need to be taken to taken to achieve this are:

1. identifying the business functions/activities that the system supports and the related records held by the system

2. mapping these to the Council's integrated business classification scheme and retention schedule to identify the record keeping requirements of the system e.g. retention periods of records held,

3. assess the record keeping requirements of the system against these requirements

4. use the information gathered in steps 1 to 3 to select the most appropriate RM strategy for the system.

Many of our business systems may already have some or all required system functionality to meet the minimum RM standards for the digital records they hold.

For those that do not, a risk-based approach must be taken to identify what actions need to be taken to address this. The risk assessment should be based on:

- risks associated with the business function that is supported by the function or activity of the business area,
- the value of the records that are created and managed in the system (high value or low value records),
- the risk associated with records that are created and managed in the system.

Things that should be considered when assessing record and information risk should include:

- breaches to privacy due to over-retaining records,
- general security capabilities,
- loss of information (accidental or deliberate),
- unauthorised access,
- business continuity in disasters,

Strategies to address RM functionality gaps in existing business systems include:

- changing the configuration of the system, e.g. by turning on additional functionality or changing the data schema

- integrating the business system with an external recordkeeping system such as an EDRMS

- exporting records and saving the exported records into an external recordkeeping system such as an EDRMS

- business process re-engineering or introduction of new work processes
- implementing policies, procedures, business rules or guidelines to ensure the recordkeeping requirements are met.

Systems and requirements change as a normal part of business, and so recordkeeping strategies put in place for records of business systems should be routinely monitored to ensure they are continuing to meet the organisation's needs. Times when these strategies may be at risk include administrative change, process change or system upgrades or migrations.

Business Systems RM assessment tool

The Council has developed Business Systems RM assessment tool which can be used to:

- build functional RM specifications to support planning and procurement of new business systems and applied to existing systems.
- assess required functionality in existing business system to meet the minimum RM standards for the digital records they hold, taking a risk-based approach to identify what actions need to be taken to address identified gaps, focussing only on systems that hold records that represent high risk and/or high value to the Council

Add link

Taking control of our digital records in "H" drive and OneDrive

This section will need to be amended once final decisions have been made on Council IG rules related to OneDrive and migration of users from H drive to OneDrive including retention rules, non-business labels in OneDrive etc

The Council recognises that there are occasions when staff need to create and store information which does not form part of the Council's corporate records and which it is not appropriate to save to network shared drives, MS Teams or line of business systems. For this reason, all staff have access to a personal H:drive, and with the move to M365, the equivalent OneDrive.

These are private to each individual, but can be accessed for system management, monitoring and compliance purposes, subject to the Council IT and information governance controls organisational and technical controls.

There are several risks which arise from storing files in your H and OneDrive:

- Colleagues may not have access to necessary up-to-date information should you be unavailable - on holiday, on sick leave – or when you leave the Council.
- Records are not stored appropriately in line with the Council's business classification scheme and metadata standards.
- Version control, destruction of records and retention schedule rules cannot be adhered to
- Records could be inadvertently missed as part of a search in response to an information request.
- Personal copies of Council procedures, guidance or templates may not be the current version which risks you carrying out work based on obsolete instruction

For these reasons, work-related information and records must not be saved to your H or OneDrive, except for specific approved business reasons. Any early working/scratch documents which have reached the status of draft must be saved to the appropriate formal Council system and continue to be worked on from there.

Examples of types of information which can be saved to your H and OneDrives include:

- A document being used for research
- A sample of a document being used for reference
- A picture which will be used in a document
- Notes you have made which you will use to assist in delivering a presentation

You are responsible for managing the contents of your H:Drive and OneDrive on an ongoing basis to ensure they are kept to a minimum and that they are being used only when it is not appropriate to save these documents to Council systems as described above.

H:drive clear-out and migration to OneDrive

1. Sort out the content:

- Create 2 folders in your H Drive – MyFiles and WorkFiles
- Go through your folders identifying folders/files that are personal to you and move these to your new MyFiles folder.
- Go through your folders identifying any folders/files that support current or past council working and put it in the WorkFiles folder.
- Get rid of any rubbish or duplicates from within your H:drive folders, or anything that is a duplicate of material held in network drives, MS Teams or other Council business systems.

2. Move the content

- Move the content of your MyFiles folder into your OneDrive when you are advised to do so.
- Move your WorkFiles folder to the appropriate area of the shared drive when you are advised to do so.

3. Ongoing OneDrive housekeeping

Get into the habit of regularly checking and clearing your OneDrive folders, deleting files saved for information only as soon as you have finished with them and moving any working documents that have gone beyond the “scratch working” status into the appropriate Council system.

Taking control of our digital records in Email and MS Team communications

For many years email has been the preferred method for information sharing and collaboration within the Council and with external parties. With the adoption of MS Team digital workspaces, which provide integrated tools for instant messaging, collaboration, information sharing and online meetings, the Council now has a very powerful communication and collaboration platform that has the potential to truly transform the way that we work.

Inevitably a key part of digital communication and collaboration is the creation of information. Any information created or stored in Email or MS Team apps is a

Council record when it is evidence of business activities such as decisions, actions or delivery of services.

Without appropriate governance controls, rules and guidance in place to ensure the proper management of these records and realise the transformational potential of M365 collaboration and communication tools, including Outlook and Teams, the Council will be exposed to levels and types of risks far greater than those already experienced through long-term ungoverned and inappropriate email working practices. These risks include:

- adverse impact on individual and team productivity
- stockpiling of temporary information that very quickly becomes obsolete
- isolation and loss of valuable business records
- file duplication and lack of clarity on the which is the most current version

This section of guidance is focussed specifically on good practice management and use of email and MS Teams in relation to digital records management. It should be read in conjunction with related Council policy and guidance as listed and linked below:

- M365 Information Governance Policy
- RM-focussed Email Guidance

- an email and internet good practice guidance(intranet) covering related issues;
- guidelines (intranet) for using email as a communication tool with clients, citizens or Service users;
- information related to spam and phishing emails (intranet) and what you need to be aware of.

Add links

Identifying email and post content that needs to be retained as a record

As mentioned in the introduction to this section, a key part of digital communication and collaboration is the creation of information. Any information created or stored in Email or MS Team apps is a Council record when it is evidence of business activities such as decisions, actions or delivery of services. It is key is that you do not use these tools to store these records. Save key drafts, finalised documents and important decisions in the business system or shared drive where associated council records are stored.

It is the responsibility of MS Team Owners, or a delegated administrator, to ensure that this is done. Within personal MS Outlook mailboxes, the responsibility lies with the individual.

Use following list to help you and your team be aware of the types of information recorded in emails and MS Teams channel posts and private chat that may be a Council record will need to be retained and managed appropriately in the relevant Shared drive, MS Team or business system.

- Content that contributes to policy or decision-making process
- Content that reflects contributes to an action taken or decision made
- Content that contributes to a change to organisational policy or procedure
- Content with financial or legal implications (e.g. a contract, a grievance case)
- Content needed to support and help the running of Council business (e.g. team budgets, purchase orders of IT systems, business continuity management)
- Content that needs to be approved by, or reported to, another individual or internal or external body (e.g. Council committee, senior management, approved by spending team)
- Content that sets a precedent or contain something unique of historical interest (e.g. an intranet snapshot, audio clip or video file)

The following guidance provides best practice use of email and MS Team for collaboration and communication.

The purpose of MS Team Channels and Chat is for collaboration and communication to support active work e.g. projects and working groups. Because their main form of written communication is persistent chat, it is a replacement, in many instances, for email exchanged between those work-related teams. Effective use of MS Teams will therefore eliminate problems caused by collaborating via email – these problems are impacting the business and also the users/employees and include

- Multiple email conversations about the same topic with different audiences
- Multiple copies of the same email in individual sender and recipient mailboxes
- Losing important emails in amongst the dross
- Not including the right people in the email
- Including the wrong people in the email – especially when including others half way through conversations, or discluding those who have been included up to a certain point
- Duplicate files created through attachments – keeping track of different versions of a file

The following good practice tips will help you understand when to use email and when (and how best) to use MS Teams for communicating and collaborating with Council colleagues and external parties.

- Use email for more formal communications and communications where the audience is wider than MS Team membership
- Use MS Teams as your default communication and collaboration tool with other MS Team members.
- Your activity feed provides you with a range of notifications. These include a colleague 'liking' something you posted or replying to a thread you started in a channel that you are following.
- Use @notifications of individual members or whole team membership in channel posts, private chat and within individual documents stored in Team files to alert them to your post, message or query.
- Add links to existing Team documents within Channel posts and private chat.
- If you are uploading a file to the Team and want to alert other members about this, upload it via a Channel post as the document will be stored in the related Channel folder.

Access, security and compliance

It is critical to maintain the confidentiality, integrity and availability of council information in communications created in Teams and Email to ensure data is protected whilst meeting regulatory, legal and contractual obligations.

While of availability to content is an issue when individual mailboxes are used for ongoing storage of email content and attachments, you must be aware that any posts made in Team channels are recorded, stored and accessible by all members of the Team, except for private channels. It is your responsibility to ensure that your post content is appropriate etc

The conversation trail(s) in Outlook and in Teams, including those in ‘chat’, are disclosable under Freedom of Information (FoI) requests, Subject Access Requests (SAR’s) and other compliance, records management and data privacy requests. You must therefore employ extreme care in what you say, type and send when using these communication and collaboration tools.

Any instant messages you receive while offline will be available next time you come online. Conversation history and chats are persistent – that is, your conversations stay around even after closing the application. Make sure you do not share sensitive information that you do not want all invited participants to a chat to see. They will be able to read the chat even if they do not join the meeting or have already disconnected.

Retention and disposal

Users can and should remove emails once they have been actioned, either by deleting them, if they are of no further business value, or by moving them to the appropriate business system or file repository, if they need to be retained as part of a wider record of current or completed work.

Formal retention and disposal of information in MS channel posts and private chat is applied automatically using M365 retention policies and labels, configured based default rules agreed in line with the Council’s integrated business classification and retention schedule. Mailbox content of current employees and leavers will also be subject to Council-wide default retention and disposal policies which will also be applied automatically.

The Council’s M365 Information Governance Policy add link provides details of what these agreed default are.

Personal mailbox clear-out

As part of improvement practice, it is recommended that you take time to clear out your personal mailbox, following the steps below

- Sort out the content:
- Create 2 folders – MyData and WorkData
- Go through your folders identifying data that is personal to you and put document/folder in the MyData folder.
- Go through your folders identifying any data that supports council working and put it in the WorkData folder.
- Get rid of any rubbish or duplicates from within your Emails
    - Any emails that are transient and do not contain information of ongoing value to the Council should be deleted as soon as it has been actioned
- The emails that you save into MyData folder that are personal to you should be either be deleted as soon as it had been actioned, or moved to your H Drive or OneDrive, if it you will need to refer to it in the future
- The emails that you put in WorkData folder, because they contain information relevant to the running of the Council, and therefore may need to be retained as a record, should be moved to the appropriate business system, shared drive area of MS Team once actioned. If they have no further value, once actioned, they should be deleted

Digital preservation and taking control of our digital archives

Digital preservation

Many of the documents we create need only be kept for immediate business use after which they can be destroyed. Others have a longer term informational and evidential value and will have to be retained as records for many years. Records of historic archival value must be kept permanently.

Throughout their retention period, we must be able to:

- find the records
- view the records
- maintain their integrity and authenticity - and be able to prove this.

The process to enable us to achieve this is known as preservation. The preservation challenges and activities for paper records are different from those of digital records, though the principles are the same. This section will help you understand what digital preservation is about. It will also show you how to help ensure that digital records are managed over time so that they continue to meet the needs of the Council and its services effectively and efficiently, and in compliance with the relevant legislation.

Risk-based approach

Digital preservation can be a costly business in terms of time, effort and expense. It can be a daunting process knowing where to start. A good first step is to carry out a risk assessment to identify the value of the records for which your service is responsible and the reasons they have to be retained.

Preservation actions can then be developed that are appropriate in terms of need, value and risk to the Council. In this way preservation investment will be priority based and proportionate to the outcomes of that investment.

The Council's record retention schedule is a key tool here as it clearly identifies those records that will need to be kept for long periods of time and therefore require special management to meet the preservation principles outlined above.

Add link to Performance Risk and Compliance Framework

Preserving digital records

Preservation of digital records is a far more complex business than that of paper. Without the proper controls in place it is far easier to inadvertently or deliberately change, duplicate and delete digital records bringing into question the integrity, authenticity and security of those records. In order to access and view the files over time you will need appropriate software, hardware, and migration processes (to remove the risks posed by obsolete technology). These can maintain the integrity and authenticity of records – and provide evidence of this.

The preservation implications of digital records should be considered as early as possible and preferably at creation. This should be underpinned by a life-cycle management approach to the maintenance of technology and it is advisable that services involve IT throughout the preservation process.

With the transition towards e-government, more and more records will be "born digital," that is, will not have a paper equivalent. It is vital that any initiatives to move from paper-based to digital working takes account of this and ensures that the transition from paper-based to digital record keeping only occurs once a preservation strategy has been tested and implemented.

Addressing the backlog

As well as putting in place a robust process for the preservation of all future digital records, you will have to address the preservation of existing files. A potentially very costly exercise, this is again best undertaken following a risk-based approach. This allows you to focus only on those records of greatest need, value and risk to the Council as outlined earlier in this guidance.

The difference between back-up and preservation

Contrary to popular belief, backing up is not the same as preservation! Backing up of digital files is used for short-term data recovery following loss or corruption and is not an appropriate solution for the long-term preservation of digital records.

Practical tips

However there are still some practical steps you can take to support the longer term preservation of digital records.

Once finalised, a digital document that needs to be kept as part of a Council record should be closed down to further changes. This will maintain its integrity, reliability and authenticity. Convert finalised records of high informational and evidential value to Adobe PDF/A format to meet these requirements or apply read only permissions at document or folder level.

If you have files in old formats or media, e.g. floppy disks, microfilm, microfiche, identify any that need to be kept and contact IT to help convert these to the appropriate format and destroy the rest. The same applies to records stored on CD, videos etc. as these deteriorate over time and will become corrupted or unreadable within a few years of creation.

Ensure that you provide sufficient information about the file in the content of the document and in its file properties. This metadata is a part of the record, providing context and aiding future retrieval. When working on a document avoid the “Insert date” and other automatically generated text unless you can be sure that these will not be automatically updated each time they are opened.

Link to Recordkeeping metadata guidelines

Digital records of archival value

Some of the Council's records need to be retained permanently because they have long term evidential or historical value. The Council's Records Retention Schedule helps to identify records that have archival value and provides two different disposal actions for these records.

Retain for business or historical value: under this disposal action the full record must be transferred to the Council archive service for permanent preservation.

Review for business or historical value: under this disposal action, a review process must be undertaken in consultation with the Council's Senior Information and Improvement Officer to decide what subset of the full record needs is worthy of permanent preservation in the Council's Archive. This is likely to be either a random sample or selected examples of particular significance or interest.

The Council does not yet have a digital archive for maintaining and providing access to those digital records of enduring value that need to be preserved permanently. However, as the majority of Council records are now digital rather than physical, it is important that we ensure that we are identifying and retaining digital records of archival value appropriately, in preparation for when the Council has a digital archive repository. This will also meet our obligations under the Public Records (Scotland) Act 2011 Model Records Management Plan, Element 7: Archiving and Transfer Arrangements.

The Council's records retention schedule identifies records that should either be retained or reviewed for enduring business and archival value.

The table below provides provides a summary that can be used as an initial checklist by Services to identify digital records of potential archival value, especially when rationalising shared network drives that may contain the authority copies of Council records for which your service or team is responsible.

Further advice will be provided on maintaining these until a digital archive system is available for their transfer.

1. History, Procedures and Functions	Records relating to the origins and history of the Council and predecessor bodies; its organisation and procedures; functions and dissolution
2. Annual Reports and other publications	Copies of annual and other major Council reports and publications, including published research
3. Policy	Principal policy documents together with drafts which evidence policy development
4. Decision making Policy Interpretation / Implementation:	Records relating to the implementation and interpretation of policy and to changes in policy; Record sets of minutes and circulated papers of Council, statutory Committee and senior management meetings
5. Organisation Activities	Records relating to Council accomplishments, or to obsolete activities or investigations, or aborted schemes initiated by the Department;
6. Statutory Work	Evidence of statutory rights or obligations, title to property, claims for compensation not subject to a time limit, and formal instruments such as awards, schemes, orders and sanctions;
7. Legislative Requirements	Records which must be permanently preserved in compliance with legislative requirements
8. Records of significant local, national or international interest	Documents relating to significant public events, people (e.g. Council and Executive Group members), major incidents which give rise to interest or controversy at local or national level
9. Statistics	Records relating to trends or developments in Council service delivery and improvement, particularly where they contain unpublished statistical or financial data covering a long period of time or wide area;

10. National Research and Development	Documents relating to the more important aspects of Council services scrutiny and improvement research and development, particularly where these had a wider application and affected the political, cultural, social, economic or other aspects of Scottish or Council area life;
11. Statistical Research for Decision Making:	Statistical and quantitative research either undertaken or sponsored by the Council sponsored or undertaken by outside bodies, where its findings affect Council decision-making and the research reflects on the history of local government