## Annex A – Using appropriate filing structures

The following guidance set out the principles of setting up a structure of folders on a network shared drive to provide a clear and logical location for saving and finding information.

Using a meaningful filing structure will help your team identify and locate records and will help manage and protect sensitive information in compliance with legislation such as and Data Protection Act 2018.

The folder structures for electronic files should reflect the activities of your business area or team and allow staff to save and retrieve information efficiently.

The folder structure should:

- be easy to understand for those who add and use information within it;
- classify the information according to the activities of the business area;
- provide and preserve context within which the records were created (by sitting alongside relevant and related information; and
- provide appropriate levels of access to staff and security for sensitive information.

By considering where you will need to save sensitive information, such as personal data or information that needs restricted access, you can help ensure the GLA complies with data protection legislation and prevents any unauthorised or unlawful processing, damage, loss or destruction of personal data.

The folder structure you use should reflect your business activities and workflows by using a sensible and practical structure of folders that have meaningful titles and that contain appropriate and relevant files, documents and records.

If your folder structures are well designed, it will allow your team and colleagues to access more effectively and introduce measure (such as password permissions) that limit access to information which has a genuine need to be protected.

An appropriate folder structure might be modelled on the functions of your team. Alternatively, it could be based on particular subject areas or areas of policy work.

In either case, avoid using broad or vague terms or descriptions, and never use folders titled 'misc', or 'admin', or named after individual members of staff (e.g. 'Mary's folder'). These don't describe the content of the folder and can cause other problems such as:

- inhibit the sharing content and information across the organisation;
- create unnecessary duplication of records – people don't know where to store something;
- cause problems with routine disposal policies;
- create legacy folders with no clear ownership;
- reduced efficiency in terms of compliance with the Data Protection Act or Freedom of Information Act

These problems can be aggravated if users move to a different or leave the organisation.

There are many approaches to amending your filing structures. Irrespective of the method you use to create and effective filing structure, it must at the very least contain the following attributes:

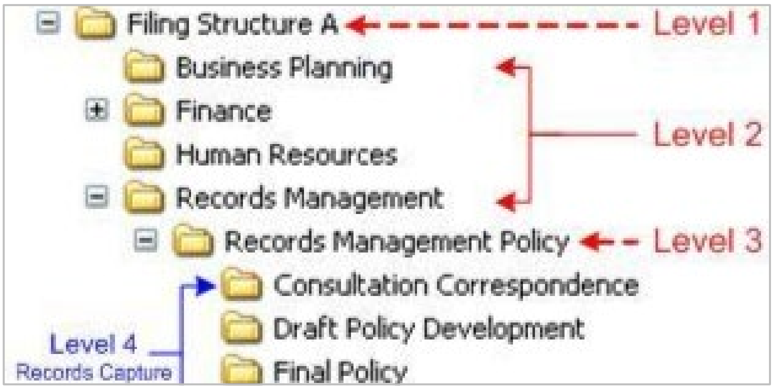
- Be a structure that can be easily interpreted and discourages users from placing records in inappropriate locations
- Use simple names that identify relevant and appropriate folders for saving information

Formal records-management orientated folder structures will typically have three levels (or layers) of folders that act as segregations for information. These levels represent the **functions**, **activities** and **transactions** of your team. The fourth and usually final layer sits beneath these and is where the records are to be captured and stored.

This example shows a basic layout of a filing structure on a shared-drive, but the same principles can apply in other situations and on other platforms

**Upper-level folders <u>should never contain files or records</u>.**

**Records are normally only expected to be captured in the lowest level of the filing structure.**




If you employed a temporary member of staff, would they be able to extract specific information from your records without any particular knowledge of your business area or the documents you hold?

In summary, the GLA does not dictate any one particular solution or structure that teams should use to organise their records. The folder structure that your team adopts and uses should be clear and relevant to the work of your team and directorate. If your colleagues don't know where to save information, it might need some attention.

For more information please visit the GLA's Records management Policy and Guide to managing shared folders. We have also produced guidance for keeping records for corporate requirements

If you need advice about organising the folder structures used by your teams, please contact the Information Governance team.

## Annex B – File Naming Conventions

Naming conventions are rules which support thee titling of electronic files in a consistent and logical manner.

Naming files consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of data. A consistent approach to naming files will also ensure your files are stored in an appropriate order based on their name.

For example, Include dates in the format YYYYMMDD. They will be easy to find and appear chronologically.

We encourage teams to save information with consistent, appropriate, concise and relevant file names. Here are some helpful suggestions

i. Keep file names short, meaningful and easily understandable to others.

ii. Order the elements in a file name in the most appropriate way to retrieve the record.

iii. Avoid unnecessary repetition and redundancy in file names and paths

iv. Avoid obscure abbreviations and acronyms.

v. Avoid vague, unhelpful terms such as "miscellaneous" or "general" or "my files"

vi. For numbers 0-9, always use a minimum of two digit numbers to ensure correct numerical order (e.g. 01, 02, 03 etc.)

vii. If using a date in the file name always state the date 'back to front', and use four digit years, two digit months and two digit days: YYYYMMDD or YYYYMM or YYYY or YYYY-YYYY.

viii. When including a personal name give the family name first followed by initials, with no comma in between e.g. SmithAB

ix. Avoid using common words such as 'draft' or 'letter' at the start of file names

x. Use alphanumeric characters i.e. letters (A-Z) and numbers (0-9).

xi. Avoid using non-alphanumeric characters such as *? \/ : # % ~ { } in file names

xii. The file names of records relating to recurring events should include the date and a description of the event, except where the inclusion of these elements would be incompatible with rule 3

**Version control**

Version numbering helps to distinguish one version of a document from another. For some documents, you may decide that a simple numbering system consisting of consecutive whole numbers is sufficient to help you keep track of which version you are working on.

However, documents that go numerous stages of development before a final version is reached, and for those that are developed through input by multiple individuals, you may decide to adopt version numbers to keep track of both minor and major changes to that document.

*Minor Revisions*

Minor revisions are small changes made to a document such as spelling or grammar corrections, and other minor drafting or formatting amendments. Minor revisions to a document are reflected by making increments to the decimal number.

*Major Revisions*

Major revisions are changes to a document that require the document to be re-approved (either by an individual or a group). Major revisions are reflected by incrementing the whole number by 1.

Use the file name of the document to determine both the version and status alongside its name. Version and status details should always be at the end of the document title, for example:

- Records Management Policy Draft v0.1
- Records Management Policy Final v2.0

Once you have finalised a document, a decision should be made on whether the drafts now need to be kept or whether they can be deleted.

In the majority of cases it should be possible to delete drafts once the final version of a document has been agreed. This will help to reduce the confusion caused by the duplication of documents and means that there is less danger of earlier versions being accidentally used.

You should keep drafts if you think it is necessary to preserve a record of the process of developing the document. This may be, for example to maintain a record of why particular changes were made or to help when the document is redeveloped at some future date.

**Remember that draft versions of a document maybe subject to disclosure under the Freedom of Information Act.**

25 July 2022
Authored by
[redacted]

**<u>Email retention rules are changing - Action required</u>**

**Updating our email and record retention guidance**

**Changes to our policy will affect Outlook and MS Teams messages**

We have been reviewing how we use and retain emails and other messages as part of our work to update our policy and records retention guidance. We will be implementing an automatic retention and deletion rule that will be apply to all Outlook items and all MS Teams chat messages.

This rule will come into effect from the end of September.

**MS Teams:** the automatic retention period for Teams messages will now be 30 days instead of 90.

**Outlook:** All emails on the GLA network that are over eight years old will be automatically deleted. This will affect any members of staff who have either worked at the GLA for more than eight years, or who hold emails and other Outlook items that are more than eight years old. The majority of emails do not need to be retained for more than eight years.

This decision was approved by the Governance Steering Group earlier in July.

If, in exceptional circumstances, you hold emails older than this and there is a legitimate and genuine need that the information in the email should be retained, you will be required to take steps to save that email in a suitable format, and in a suitable location, to ensure its preservation. The Information Governance team have prepared some guidance to help with this. If you have any questions regarding saving emails, please contact the Information Governance team via information-governance@london.gov.uk

Please note that this rule will only apply to Outlook items. There are no plans to automatically delete or remove documents that are over eight years old. These should continue to be saved, retained and destroyed in line with our existing retention and disposal guidance.

As part of changes to our approach to the retention and deletion of electronic information, deleted emails (which are currently only kept on the network for 30 days after deletion) will now retained on our “servers” and remain accessible (in limited circumstances) for 8 years. This will not affect:

- emails deleted before these changes come into effect at the end of September; or

- emails held by staff who leave the GLA – their accounts will be deleted in-line with existing processes.

**Email retention guidance**

In line with the new automatic email retention rules that are due to be implemented, action is required now to ensure that emails older than 8 years and required for longer preservation are stored appropriately.

Every email transaction falls into one of the following categories during its life-cycle:

| | | |
|---|---|---|
| Business critical | Has business, evidential or legal value | Keep until value expires* |
| Informational | Has information or reference value | Keep until value expires* |
| Redundant | Business, evidential, legal or reference value has expired | Delete promptly |
| Irrelevant | Spam, unsolicited messages of no value | Delete promptly |
| Personal | Not work-related and of no value | Delete promptly |

*Please review the GLA's retention schedule Information and records management | Intranet (london.gov.uk) (Appendix B of the Records Management Policy). This includes a list of statutory requirements for retaining information.

To save an email in your shared drive, simply click and drag the folder from outlook into your target folder location. Capturing emails from Outlook into your shared drives requires some attention to the file format the email will be captured in.

Dragging emails from Outlook into the desired location should automatically save the email in the correct format: *Outlook Message Format (*msg).* Do pay attention to this rule and make sure it does not save as: *Outlook Message Format – Unicode (*msg)* as the email file will lose its integrity and will no longer be retrievable.

When emails are captured from MS Outlook into a file system they are automatically named using the text in the 'Subject' field of the email. As a result, the prefixes 'RE:' for replies and 'FW:' for forwarded emails may be retained. Remove these to ensure that the title of the record is clear and replace with the date of the most recent email in the chain and retitle ensuring the purpose and content of the captured email, for example:

- '20220721 Copy of New Records Management Policy sent to Chief Officer'

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

- 'FW New Record Management Policy'

**Things to consider**

- Avoid duplication where possible. Is the information being stored elsewhere? (For example, within the Finance team)
- Avoid mass / unorganised migration of all your emails to a landing folder in your shared drive. This will make file naming more difficult, create duplication and make future retrieval of a particular email more difficult.
- Do not save all your emails into a folder on a shared drive bearing your name, for example 'John's emails'. Your emails should be saved in a structured format in a folder which matches the business purpose to which your email relates.
- Use the email filters and sort functions in Outlook before transferring emails to your shared folders. Where appropriate, use the subject field so you can select the most recent email in a particular chain and store this version to avoid duplication.
- Save email attachments that you require separately. Check that there's no alternative location to access an attached document before you save yet another copy.
- Whilst saving emails to shared folders, consider the 'Temp test': If you employed a temporary administrative assistant (a 'temp'), would they be able to extract specific email from your manual records without any knowledge of your type of work or the documents you hold?
- Contact Information Governance for help

Staff leaving the GLA, and Line managers will already be following these steps in line with the GLA's HR Leavers procedure: Leaving the GLA | Intranet (london.gov.uk).

The National Archives have produced a very helpful guide for managing electronic records - For more information on structured 'relevant filing systems' and file naming conventions please review the guidance at: Managing digital records without an EDRMS - The National Archives

06 September 2022
Authored by
[redacted]

**Email retention rules are changing - Action required**

**Updating our email and record retention guidance**

Please remember that from October the GLA will be applying a retention period of 8 years for all emails (including emails stored in sub-folders of the in-box), meaning that emails older than that will be deleted.

Please see my previous blog post on this for more details.

Email retention rules are changing - Action required | Intranet (london.gov.uk)

This includes guidance on how to save any older email as a document if it needs to be preserved.

Some larger old emails with attachments may be partially held in an archive – which will mean that you will need assistance from the Technology Group to save them.

If you need save any of these emails please contact the Technology Group Service Desk

# Quick Guide

GREATER**LONDON**AUTHORITY

## Records Management Quick Guide 1 - Managing shared folders

This Records Management Quick Guide is focussed on how to manage shared folders on network drives (often referred to as team 'shared drives').

### What are shared folders?

- They are electronic storage areas on the GLA network for corporate information and records which we need to work on/share within a defined group. They are created on network drives (eg the GLA-wide N drive and your personal M drive).
- We use shared folders to store what is known as "unstructured data" (eg Word documents, Excel spreadsheets, emails, PowerPoint presentations, etc) where there are no corporate databases or systems available to store the information in a structured way.
- Each business unit or team is responsible for managing its own shared folders.

### Risks of poor management of shared folders

- Duplication of information within and between folders (a compliance and efficiency risk).
- No-one is sure which document in which folder is the correct/latest version (a significant compliance and reputational risk).
- Unauthorised access to confidential information is a constant danger (a compliance risk).
- No-one is sure when to delete obsolete, inaccurate or out-of-date information (a compliance, efficiency and financial risk).
- No-one takes responsibility for managing any of the above risks!

### Setting up a new shared folder on the network drives:

- Users wishing to set up a new shared folder should think carefully about whether the folder is needed or whether an existing folder will suffice.
- The person setting up the folder is responsible for managing both the folder and its contents in line with best practice (see page 2), for ensuring other team members follow best practice when adding new content and for deleting the folder and its contents once it is no longer needed so that they no longer appear on the shared drive.
- M drives should be used for personal or private material; as far as possible, GLA work should not be stored on this network drive.
- The N drive should be used for work that needs to be shared with staff in other directorates. All staff can access folders on the N drive and mage changes to documents stored there unless Technology Group has been asked to set up restrictions. Once projects are complete, you should either delete the related folders from the N drive or move them to your team shared drive where they can be managed.
- Where possible, the Intranet should be used to communicate policies, procedures and other information that needs to be shared GLA-wide.

## Managing folders

### Plan properly when setting up a folder

- What are the core objectives, functions and responsibilities of your team? You should base your shared folder structure on these functions and activities.
- Think about security. Be clear about who is to have access permissions; these considerations will also affect the folder structure.
- Discuss proposed changes with affected users and take into account their feedback.

### Take responsibility

- The shared folder will need a designated owner.
- Each owner should regularly review the folders' content and purpose to see whether they are still current or no longer needed (eg a folder relating to a completed project).
- Each owner should monitor any sub-folders which may be added to make sure they are relevant to the parent folder's purpose and are given meaningful titles.

### Keep it simple

- Give folders meaningful titles (ie names everyone will understand), which reflect clearly what the folder is about.
- Allow as few sub-folder layers as possible to enhance quick access and reduce length of file-paths.
- Store documents in the most relevant folder (ie the one covering the primary function to which the document relates).

### Dispose of obsolete information

- Delete as much redundant material as possible so that ephemeral documents are not stored unnecessarily (eg drafts, duplicates, obsolete versions and redundant reference material) – remember these can still be requested and may need to be disclosed under the Freedom of Information Act!
- Folder owners should regularly review the folder contents to check that it is still relevant to their team. If not, the folder should be deleted so that the documents no longer appear in the shared folder. This will reduce clutter and speed up the retrieval of business critical files/documents.
- Records of GLA business must be retained for at least the period specified in the **GLA Retention Schedule**.

## Managing files/documents within folders

### Use accurate, meaningful titles

- Don't use an individual's name as a folder or file/document title (eg 'Fred's procurement docs') – they don't reflect the folder's purpose and mean nothing to other colleagues.
- Avoid repetition – the folder name will be in the file-path so you don't need to repeat it in the document name – for example: Committee\Committee meetings\Committee agenda.doc
- Will there be several versions? If so, include the version number in the title (eg v1.0)
- Will you need to browse by date? Always include the date at the beginning of the title as follows: **YYYY-MM-DD** (eg 2009-06-30). Documents will then be listed in the correct chronological order.

### Enter essential 'metadata'

- Fill in the 'properties' field each time you create a document (select **MS Office** button, then **Prepare**, then **Properties**).
- Doing this will not only help everyone to find the document later but will enhance its authenticity and evidential value.

### Avoid duplication

- Don't file a document in more than one place. Use shortcuts if you think you won't find it easily later (right click on the document title, click 'create shortcut' and then move the shortcut to the relevant folder).
- When e-mailing information to other users with access to the same shared folder, send hyperlinks to documents whenever possible, NOT attachments.

### Don't forget about managing your e-mail!

- Important e-mails should be stored, like any other business record, in the shared storage area.
- Set up temporary storage folders in your Outlook mailbox which mirror the folders you use in the shared folder.
- Regularly review the contents of each folder and delete unimportant material.
- Move business critical e-mails out of mailbox folders and into the relevant shared folder as soon as the transaction is complete (save them using the Outlook message format '.msg'), then delete the original from your mailbox.

# Quick Guide

GREATER**LONDON**AUTHORITY

## Records Management Quick Guide 2 – Keeping records for corporate requirements

This Quick Guide explains your individual responsibility to ensure that activity is appropriately recorded. Unless consistent decisions are made about what records should be kept, the GLA is likely to either end up without the information it needs or to be overwhelmed by information it does not need. Both carry risks.

**Too much information means…**

- systems (such as SAP or the shared network drives) become clogged up with ephemeral information – searching is harder and takes longer, and it can be difficult to identify what is relevant to the business in hand;
- staff and other resources, including storage capacity, are wasted managing information that is not needed; and
- identifying the definitive version of a document can be difficult.

**The GLA's records should…**

- enable staff to do their work consistently, in full knowledge of the processes, decisions and actions that inform and drive the business;
- ensure the availability of credible and authoritative evidence to protect the rights of the GLA, its staff and anyone else affected by its activities;
- provide corporate memory so that lapse of time and change of personnel does not affect access to and availability of the corporate knowledge resource; and
- demonstrate accountability by providing the evidence and information required for any possible internal or external audit.

**Examples of records that should be kept**

- Minutes of senior management meetings at which key decisions are made. Accountability requires an agreed note of decisions that attributes and dates them.
- Details of accidents at work must be kept in an accident book under health and safety legislation.

**Too little information means…**

- the GLA has an inadequate corporate memory;
- records required to show accountability or for reference purposes are not there when needed;
- records providing evidence of rights and entitlements are not there when needed; and
- there are doubts as to the reliability of what is there.

**Examples of records that should not be kept**

- Personal copies of material that is in the GLA's records.
- Trivial or irrelevant emails and notes, eg confirming a meeting to be held.
- Early drafts of documents which are not shared with colleagues.

**Who should keep the records?**

To avoid duplication or lack of records, it should be agreed who in the GLA will save a record of an action, decision or other event. In most cases it will be obvious who is best placed to do this. For example, when drafting a policy, the originator should be responsible for keeping all versions including the final one. Similarly, internal emails discussing business should generally be kept by the sender, whilst the first recipient of incoming external emails or the sender of outgoing external emails should save the record if required.

**Related guidance**
For information on where and how to save records, see **Quick Guide 1 – Managing shared folders**

# Quick Guide

GREATER**LONDON**AUTHORITY

## Records Management Quick Guide 3 – Managing emails

It is the responsibility of all members of staff to manage their emails appropriately (see the GLA's email policy at http://intranet.london.gov.uk/pages/email-policy). It is important that emails are managed in order to comply with Data Protection and Freedom of Information legislation. Managing emails will also help you work more effectively and ensure the GLA's corporate records are appropriately captured.

Email messages are automatically deleted from the Inbox and Sent Items folders after **90 days** so to prevent loss of information, messages must be acted upon and moved to an appropriate location as quickly as possible.

Very old messages (over one year old) may have been automatically archived into a separate archive vault (they will have a vault icon next to them). To delete archived messages from your mailbox *and* the vault, ensure you select the delete vault email icon (otherwise you will just be deleting the shortcut from your mailbox and the message will remain in the vault). For assistance contact the IT service desk.

- Manage your emails as part of normal day-to-day practice; don't let emails build up until they become a significant task in themselves.
- Try not to send documents as attachments, as they clog up the server and create duplication – where possible, send a link to the document (either in a network shared drive, the GLA Intranet or the Internet).
- For one-way communications, such as project updates or GLA-wide announcements, consider using the Intranet instead of email. You can post news items, blogs, videos, and create invite-only forums.
- Follow Microsoft's 'Four Ds' model for deciding what to do with email messages, on a daily basis:

**Delete it** – Delete messages not relating to something you're working on; information you can find elsewhere; information you won't refer to in the next six months; and information you're not required to keep.

**Do it** – If you can't delete the email message, can you complete any necessary action in less than two minutes? If so, just do it: respond to the message or make a phone call. You can probably handle a significant amount of your email messages in less than two minutes.

**Delegate it** – If you can't delete it or do it in less than two minutes, can you forward the email to an appropriate team member who can take care of the task? If you can delegate it, do so right away. After you have forwarded the message, delete the original message or move it into your relevant reference folder.

**Defer it** – If you can't delete it, do it in less than two minutes or delegate it, the action required is something that only you can accomplish and will take more than two minutes. You need to defer it and deal with it after you have finished processing your emails.

<table>
<tr><th colspan="2">Managing your emails: knowing what to keep, where to keep it and how long to keep it for</th></tr>
<tr><th>Trivial emails</th><th>Emails that are corporate records</th></tr>
<tr><td>Many emails should not be retained, for example:<ul><li>Private, non-work related messages</li><li>Social communications such as lunch dates</li><li>Messages received from discussion lists</li><li>Spam – unsolicited messages of no value</li></ul>These should be deleted promptly or forwarded to personal email accounts if relevant.</td><td rowspan="5">A small proportion of emails will need to be kept for longer as corporate records, where they are the primary source of information and have business, evidential or legal value, for example:<ul><li>Emails that will be used to justify or explain a course of action or decision</li><li>Emails that will be used as a basis for future decisions</li><li>Emails that will be used to provide evidence of a business activity or transaction</li><li>Emails that detail any liabilities or responsibilities of the GLA</li><li>Emails that approve formal policy or set precedents</li><li>External business correspondence</li></ul>The retention period for emails that are corporate records should be in accordance with the corresponding records class in the GLA records retention schedule. They should be filed alongside other documents in their business context and then deleted from your mailbox.<br><br>Therefore, if the main file is paper based, then relevant emails should be printed and added to it (ensuring details of the sender of the email, recipients and date and time sent/received is printed without alteration).<br><br>If the main file is on a shared network drive, emails should be saved in message format (.msg) to the relevant folder; this preserves essential metadata about the message and enhances its evidential value.</td></tr>
<tr><th>Ephemeral emails</th></tr>
<tr><td>Some emails should only be kept for a short while. Whilst they affect GLA business, they do not need to be retained for business purposes in the longer term and can be deleted as soon as reference or value expires, for example:<ul><li>Emails for information – annual leave dates, meeting invites and arrangements</li><li>Copies of reports</li><li>Copies of newsletters</li><li>Delegated tasks from colleagues</li><li>Internal email messages received as cc or bcc messages (it is the responsibility of the sender or main recipient to retain emails)</li></ul>These should be deleted once initial action has been taken, reference has ceased or value as expired.</td></tr>
<tr><th>Reference emails</th></tr>
<tr><td>You may have some emails that you wish to keep for reference but would not consider as GLA records or information worth sharing.<br><br>These should be stored in folders under your inbox with suitable retention periods for each folder.</td></tr>
</table>

**Related guidance**

Quick Guide 1 – Managing shared folders
Quick Guide 2 – Keeping records for corporate requirements