[2021]

Information & Records Management

The information and records of the GLA are its corporate memory and are necessary for good corporate governance; to be accountable and transparent; to comply with legal requirements; to provide evidence of decisions and actions; and to provide information for future decision-making.

The information on this page will help you manage your information and records more effectively, ensuring you can find the information you need when you need it; reduce waste and unnecessary storage costs; and meet your legislative and regulatory obligations, such as those under the Data Protection Act and Freedom of Information Act.

- Records Management Policy
- Records Retention Schedule
- Historical archive
- Off-site records storage
- Guidance
- Records Management for move to the Crystal

Records Management Policy

The GLA Records Management Policy establishes a framework for the creation, maintenance, storage, use and disposal of GLA records. The first version was approved by the Mayor and the Assembly in 2004 and the current version was agreed by the Governance Steering Group and approved by a Director's Decision in March 2016.

Records Retention Schedule

The GLA Retention and Disposal Schedule is designed to support the destruction of information that the GLA does not need to retain and to help identify specific records that need to be kept. This guidance was updated in March 2016 and now forms part of the Records Management Policy.

Subject to the specific conditions, record-classes and situations listed in the Retention and Disposal Schedule, **the majority of records held by the GLA need only be retained for the duration of the Mayoral Term in which they were created (i.e. the current Mayoral Term) and for the duration of the subsequent Mayoral Term.**

The Retention and Disposal Schedule also details the specific legislative requirements that determine when certain records and classes of information should be kept for other specific periods.

Historical archive

It may be suitable for some important and interesting records to be kept forever as a historical document of the GLA and its work. These records are transferred to London Metropolitan Archives (LMA) for safe and permanent preservation.

A Historical Archiving Policy was approved by the Governance Steering Group in March 2012 and incorporated as part of the Records Management Policy in March 2016.   It includes a selection policy outlining the categories of records that are suitable for transfer to LMA.

For further details on sending records to LMA for permanent preservation, please contact Ian Lister.

Off-site records storage

Current records that you need on a regular basis should be scanned / digitsed and stored on an appropriate area of the GLA network, such as your teams' shared drive.

Semi-current records that you only need occasionally (e.g. once a year to write an annual report) can be sent to the GLA's off-site records store provided by DeepStore and managed by the Facilities Management Team.

Non-current records that you no longer have any use for should be destroyed unless there is a legal, audit or business reason to keep the records for reference. Quick Guide 2 and the GLA Retention and

Disposal Schedule should assist you in deciding what kind of records need to be kept, and for how long.

All records submitted for off-site storage with DeepStore must be indexed and submitted with review-or-destroy date in accordance with the GLA Retention and Disposal Schedule.

Guidance

A series of quick guides have been produced to help GLA staff manage their information and records more effectively - see the Attached Files menu on the right. These 1-2 page guides provide essential information and practical tips on topics such as managing emails and using shared folders.

Guidance specific to Mayoral and Assembly Members' recordkeeping and general guidance on records management has now been included in the GLA Records Management Policy. Additional guidance can also be found on the Information Governance Guidance for the Mayor and London Assembly Members page.
Training on information and records management is available as part of the Information Governance induction course.

Email Guidance

Email Management Guidance

Staff are advised to take care in managing their email in-box and the filing of emails in sub-folders of their in-box.

Everyone with an email in-box is responsible for managing it in a sensible way, deleting irrelevant emails and filing emails that need to be kept as a record of GLA business.

Emails should be retained in accordance with the GLA's retention schedule that sets out how long records should be retained.

Individuals are expected to ensure their email boxes are managed so that requests for information can be responded to effectively as well as ensuring the overall size of the mailbox does not become too large. The GLA Technology Group monitors the size of mailboxes - contacting individuals whose mailboxes appear to be disproportionately large.

To aid in system housekeeping, there is automatic deletion of emails that have not been filed in a subfolder of the Inbox. Any email that is over 3 months old and held in the in-box, sent mailbox or deleted items mailbox will be automatically deleted.

Emails which have been filed in in-box sub-folders will be retained indefinitely, but should be managed in accordance with GLA retention schedule.

Email Policy

This email policy sets out the obligations that everyone in the GLA has when dealing with email messages. You can view the full email policy outline for more detailed information.
Email should be treated with the level of attention given to managing formal letters and memos. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received. There are guidelines available for writing business emails.

All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Email messages can result in legal action being taken against the Authority or individuals and can be used as evidence in legal proceedings.

Email policy

Introduction
Purpose of the policy
Using email
Managing email messages
Management of public and shared mailboxes
Identifying and managing email records
Appendix 1
Appendix 2

Introduction

This policy applies to everyone in the Greater London Authority (GLA). It is based on guidance issued by the National Archives (Guidelines on developing a policy for managing email, National Archives, 2004) and was developed in consultation with the GLA's IT Strategy Board.

Purpose of the policy

Email is increasingly becoming the primary business tool for both internal and external communication, and so should be treated with the same level of attention given to drafting and managing formal letters and memos. Email messages should not be treated as an extension of the spoken word because their written nature means they are treated with greater authority. As well as taking care over how email messages are written it is necessary to manage email messages appropriately after they have been sent or received.

All email messages are subject to Data Protection and Freedom of Information Legislation and can also form part of the corporate record. Email messages can result in legal action being taken against the Authority or individuals and can be used as evidence in legal proceedings.

This email policy sets out the obligations that everyone (staff and elected members) in the GLA has when dealing with email messages.

There are two main sections within the policy: the first concentrates on sending email messages and the second concentrates on managing email messages that have been sent or received. Staff should ensure that they are familiar with the content of the policy and use it as a point of reference when dealing with email messages. To ensure staff and members are familiar with the content of the policy the Authority will provide training on the policy and keep staff aware of any changes that are made.

back to top

Using email (or sending email messages)

When to use email
Writing business email messages
Dealing with sensitive subjects
Misuse and personal use

When to use email

Email is not always the best way to communicate information as email messages can often be misunderstood and the volume of email messages people receive can be prohibitive to receiving a meaningful reply because of email overload.

It is the responsibility of the person sending an email message to decide whether email is the most appropriate method to communicate the information. The decision to send an email should be based on a number of factors including:

- The subject of the message
- The recipient's availability
- The speed of transmission
- The speed of response
- The number of recipients

The subject – email messages can be used for different types of communication and can constitute a formal record of proceedings. The types of communication which email can be used for include general business discussions, disseminating information, agreement to proceed and confirmation of decisions made. Although email can be used for these types of communication, it may be necessary to consider whether the sensitivity of the information would be more appropriately communicated in a different way. Dealing with sensitive subjects in emails is addressed in more detail in section 3.3. It should also be noted that there are certain subjects that should be avoided in email messages as they could be construed as discriminatory; this is covered in more detail in the section on email misuse, section 3.4.

back to top

Recipient's availability – there are times when email might not be the most appropriate way of communicating with people, for example if a message needs to be passed onto a person in the same office speaking to them face to face might be more productive, particularly if they receive large volumes of email. If the person to whom the message is being delivered is not located in the office it might be better to phone them, depending on the subject or nature of the communication. When a message needs to be communicated to someone who is difficult to locate, for example they work in more than one office, then an email message should be sent in preference to speaking to them either face to face or via the phone.

Speed of transmission – email messages are a good way of transmitting information if the information is needed quickly and the recipient is expecting the information. Where information needs to be communicated as a matter of urgency it is better to use the telephone.

Speed of response – although email messages can be sent and delivered quickly there is no guarantee that the message will be read or acted upon immediately. One of the perceived advantages of using email is that it can be responded to at the recipient's convenience. However, where an immediate action or response is required it may be better to speak to the person directly and send email confirmation if it is deemed to be necessary.

Number of recipients – although email is often considered to be a good way of disseminating information to large groups it should be noted that there are some restrictions. The ability to send an email to everyone in the Authority is restricted to the Internal Communications Team, the Technology Group and senior management. If a message needs to be conveyed to everyone at the Authority the message should normally be placed on the Intranet. If the message is particularly important an email should be sent to the Internal Communications Team requesting that they send an email to everyone detailing the nature of the information and providing a link to the appropriate point on the Intranet. It should be noted that only email messages that are considered to be of immediate interest to the majority of staff at the Authority would be sent to everyone.

Writing business email messages

When writing business email messages it is important that consideration is given to the way in which the message is being conveyed. This includes thinking about the title, the text and the addressees. As a way of helping staff to draft emails in an appropriate fashion for business use, guidelines for drafting email messages have been developed. These guidelines are appended to this policy.

Dealing with sensitive subjects

The privacy and confidentiality of the messages sent via email cannot be guaranteed. It is the responsibility of all senders to exercise their judgement about the appropriateness of using email when dealing with sensitive subjects. All external emails have a disclaimer at the footer of the email to protect the Authority from information being disclosed to unauthorised personnel, however there is no guarantee that this will protect individuals from potential legal action if emails sent include unsupported allegations, sensitive or inappropriate information.

Sensitive information can include commercial information, information about specific individuals or groups and information covered by national security classification. All information of a sensitive nature that is sent via email must be treated with care in terms of drafting and addressing. Sensitive information sent via email that is incorrect might provide a case for initiating legal proceedings against the person sending the information and/or the Authority.

When sending email messages that contain sensitive information the following issues MUST be considered:

- Email messages containing information that is not intended for general distribution should be clearly marked either in the title or at the beginning of the message, for example an email message containing comments about the performance of a specific staff member or a group of staff. This should decrease the likelihood of the message being forwarded to unintended recipients.
- Email messages containing personal information are covered by the Data Protection Act and must be treated in line with the principles outlined in the Act. Under the Data Protection Act personal information includes opinions about an individual or the personal opinions of an individual. Email messages containing this type of information should only be used for the purpose for which the information was provided, be accurate and up to date, and must not be disclosed to third parties without the express permission of the individual concerned.
- Email messages that contain information that is not supported by fact should indicate that it is the sender’s opinion that is being expressed.

Misuse and personal use

There are types of email use that are expressly prohibited and could result in formal disciplinary proceedings. It should be noted that email messages can constitute a formal record and can be used as evidence in legal proceedings. For further information on managing email messages as records refer to section 4.

When writing email messages the following conditions must be met:

- Any behaviour or comments that are not permitted in the spoken or paper environment are also not permitted in email messages

- Care should be taken when composing email messages to ensure they are inoffensive and cannot be construed as harassment. Downloading and forwarding material of a pornographic, discriminatory or derogatory nature are all prohibited. Refer to the “GLA Policies on the use of IT” for further information about what constitutes this type of behaviour
- The impersonal nature of email messages can mean that it is easier to cause offence than when speaking. If you are annoyed or angry about something take time to ensure the message does not inflame the situation
- Email messages containing inaccurate information in the form of opinion or fact about an individual or organisation, may result in legal action being taken against the person sending the email message and anyone forwarding the email message on to others
- The forwarding of chain mail is not permitted
- The terms and conditions of the “GLA Policies on the use of IT” must be abided by
- Only authorised personnel (i.e. the owner of the email account or someone authorised by the owner) should access email accounts

A restricted level of personal use of the work email account is permitted provided the following conditions are met:

- The sending of email messages does not interfere with work commitments
- The email messages do not constitute misuse of email, as detailed above

To protect the email network email messages are routinely scanned to ensure they do not contain viruses. Incoming email messages that are suspected of containing viruses will be retained by the Technology Group. An email will be sent to the intended recipient informing them that the message has been held and giving them details of who sent the message. The email message and the attachment will be retained by the Technology Group for 2 weeks before being deleted.

The GLA reserves the right to monitor email messages where it is considered appropriate (for example if it appears that email may be being misused). However, the content of email messages is not currently routinely monitored. If no action is to be taken as a result of monitoring then all the data collected will be destroyed immediately. If action is taken the data will be stored in compliance with the time limits set out in the GLA retention schedule. Further details of email security can be found in Appendix 2.

back to top

Managing email messages

Reasons for organising your mailbox
Making your mailbox manageable

Reasons for organising your mailbox

It is everyone’s responsibility to manage their email messages appropriately. Doing so will mean that work can be conducted more effectively as it will help in locating all the information relating to specific areas of business. It will also aid compliance with the Freedom of Information and Data Protection Acts.

To manage email messages appropriately email messages that are records business activities need to be identified. It is important that email messages that are records are relocated from personal mailboxes (i.e. the inbox, where you receive emails which are addressed to yourself and the sent box, where email addressed from you are sent to other people) to appropriate email folders (see section 6). Ephemeral email messages should be managed within the mailbox and kept only for as long as required before being deleted.

Email messages are automatically deleted from their inbox and 'Sent Items' mailbox after 3 months. To prevent loss of information, email messages must be acted upon and moved to an appropriate location as quickly as possible.

The Technology Group store backup tapes of the GLA network for three months. It is therefore possible, in an emergency, to request the restoration of a deleted message for a period of three months following deletion.

There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office for an extended period, for example holiday. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act
- Freedom of Information request
- Evidence in legal proceedings
- Evidence in a criminal investigation
- Line of business enquiry
- Evidence in support of disciplinary or grievance action

In the event of absence an out of office message stating who should be contacted and the period of absence, must be set-up (this does not apply if working from home and accessing the email system remotely).

Where it is not possible to seek permission from the relevant individual, the procedure for gaining access to their email account is:

- Gain authorisation from the Head of Service (or Director)
- Submit a request to Technology Group Operations Manager
- Access is gained in the presence of the Line Manager
- A record is made of the reasons for accessing the mailbox together with the names of the people who were present.
- Inform the person whose mai box was accessed.

It is less likely that this procedure will need to be followed if email records are managed appropriately or mailbox access has been delegated to a trusted third party.

Making your mailbox manageable

Managing an email mailbox effectively can appear to be a difficult task, especially if the volume of email messages received is regularly of a large quantity.

There are a number of approaches that you should follow to aid the management of email messages. These include:

- Allocating sufficient time each day or week to read through and action email messages
- Prioritising which email messages need to be dealt with first
- Looking at the sender and the title to gauge the importance of the message
- Flagging where you have been 'cc'd' into email messages. These messages are often only for information purposes and do not require immediate/any action.
- Setting rules for incoming messages so they can automatically be put into folders
- Using folders to group email messages of a similar nature or subject together so they can be dealt with consecutively
- Identifying email messages that are records or need to be brought to other people's attention

- Keeping email messages in personal folders only for short-term personal information. Emails that are required for longer purpose should be managed as records
- Deleting email messages that are kept elsewhere as records
- Emptying deleted email messages from the “Deleted Items” folder
- Deleting email messages that are no longer required for reference purposes from the in and out box

back to top

Management of public and shared mailboxes

Overview of managing shared mailboxes and public folders
Public mailbox folders
Shared mailboxes
Levels of responsibility

Overview of managing shared mailboxes and public folders

In the case of shared mailboxes management is likely to be shared between everyone who has access. In the case of public mailbox folders management the folder owner should be responsible. The purpose of managing email messages, whether they are in shared mailboxes or in public folders is to identify emails that should be retained as a record of an activity and delete ephemeral messages.

When managing shared email mailboxes, there will also need to be some additional rules relating to when to delete an email message from the mailbox, how to identify an email message as having been answered and the types of email messages that should be treated as records. While it is the responsibility of the owner to ensure that there are specific rules relating to the management of shared mailboxes it is the responsibility of all everyone with access to shared mailboxes to abide by those rules.

When managing public mailbox folders the owner of the folder should provide some clear rules as to how the mailbox will be managed, this should include:

- The purpose of the folder
- How long messages will remain in the mai box before being removed
- An indication of the length of time the folder will exist, where poss ble

The owner of the folder must ensure that the messages remain in the folder no longer than the pre-agreed time period. After this time they should either be deleted or managed as records of the discussion. It is also the responsibility of the folder owner to delete the folder once it is no longer required and ensure that all non-ephemeral email messages are saved as records of the discussion.

It is important to remember that any email that made a significant contribution to the discussion of the business being conducted should be saved as a record and not just the final conclusions. The discussions that take place in the mailbox folder will represent the context within which the final decision was made and must be maintained as a record of the proceedings.

Public mailbox folders

The public mailbox is accessible by everyone in the Authority and is organised into folders. This should be used to discuss and share ideas relating to a particular area of work. Different folders should be used for discussing different topics. The public mailbox system works by someone placing email messages into the relevant folder and others replying to the email messages that already exist. Access to folders in the public mailbox is open to everyone, unless the person who is responsible for managing the folder makes a specific request to the contrary.

Shared mailboxes

Shared mailboxes should be used where there are a group of people responsible for the same area of work. This can be a way of ensuring that queries are answered quickly when members of the team are away from the office. Access to a shared mailbox is initially given by the Technology Group and can be granted by the person who owns the mailbox.

Levels of responsibility

Although the purpose of shared mailboxes and public mailbox folders is different there are some similarities in the way in which they should be organised. If a shared mailbox or a folder in the public mailbox is going to be used the following areas must be addressed so that the email messages contained do not become unmanageable and appropriate records are maintained:

- Identifying an owner
- The purpose
- Access
- Managing the contents of shared mailboxes and public folders

Identifying an owner – when a public folder or a shared mailbox is created one person must be identified who can take ownership of the folder or mailbox. For public mailboxes this person should be responsible for ensuring that the topics being discussed do not change too radically from the purpose for which the folder was created. In shared folders the owner should be responsible for developing rules governing how email messages are responded to and how this is communicated to other people using the shared mailbox.

The Technology Group has overall responsibility for maintaining shared mailboxes and public folder. If the owner has any specific problems with managing the shared mailbox or public folder these should be discussed with the Technology Group.

The purpose – the creation of a public folder or a shared mailbox should be done for a specific purpose, for example a public folder might be created to discuss a particular policy area and a shared mailbox might be created to answer queries on a particular subject. It is the responsibility of the owner of the shared mailbox or the public folder to ensure that the mailbox or public folder is used for the specified purpose. If the shared mailbox or public folder is not being used for the specified purpose the owner should take appropriate action. In the case of a shared mailbox this might be suggesting the sender a more appropriate place to send their enquiry. In the case of public folders the owner should act as a kind of virtual chairperson of the discussion and act as a mediator if the discussion is drifting from the original purpose.

Access – the level of access granted for shared mailboxes and public is likely to be different. For shared mailboxes access should only be granted to people who are able to answer the email enquiries that will be received. In shared mailboxes it might also be necessary for the owner to delegate some responsibility to other people who are granted access for managing the emails and ensuring the mailbox is used for its specified purpose. For people sending messages to the mailbox it will be necessary to ensure that a message is given to people who might want to send enquiries giving the email address and the purpose of the mailbox, this can be done on a website.

The default access for all public mailbox folders is that everyone in the organisation can view the contents of all the folders. When the folder is created everyone who might be interested in contributing to the discussion should be informed of its existence. As everyone in the Authority has access to the folder the owner needs to ensure that the email messages posted are relevant. Where the email messages are irrelevant the owner can delete the messages, having informed the sender why they are taking this action.

back to top

Identifying and managing email records

Essential principles
Identification and responsibilities
Managing email records with attachments
When and where to manage email records

Essential principles

Email messages can constitute part of the formal record of a transaction. Everyone is responsible for identifying and managing emails messages that constitute a record of their work. When an email is sent or received a decision needs to be made about whether the email needs to be saved as a record. Once an email message has been saved as a record it should be deleted from the email in-box. The main points to consider when managing email records are:

- Identifying email records
- Who is respons ble for capturing email records
- Email messages with attachments
- When to save email records
- Where to save email records

Identification and responsibilities

Identifying email records – a record is 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business'. When deciding whether an email message constitutes a record, the context and content of the email message needs to be considered. For detailed guidance on what constitutes a record please refer to the GLA Retention Schedule.

Email messages that might constitute a record are likely to contain information relating to business transactions that have happened or are going to take place, decisions taken in relation to the business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a tender document for a particular service, background discussion about what this should and should not include might take place via email and should be saved as a record.

Who is responsible – as email messages can be sent to more than one recipient there are specific guidelines to indicate who is responsible for capturing an email as a record:

- For internal email messages, the sender of an email message, or initiator of an email dialogue that forms a string of email messages
- For messages sent externally, the sender of the email message
- For external messages received by one person, the recipient

- For external messages received by more than one person, the person responsible for the area of work relating to the message. If this is not clear it may be necessary to clarify who this is with the other people who have received the message.

Managing email records with attachments

Email messages with attachments – where an email message has an attachment a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a record depends on the context within which they were received. It is likely that in most circumstances the attachment should be saved as a record with the email message as the email message will provide the context within which the attachment was used.

There are instances where the email attachment might require further work, in which case it would be acceptable to save the email message and the attachment together as a record and keep a copy of the attachment in another location to be worked on. In these circumstances the copy attachment that was used for further work will become a completely separate record.

When and where to manage email records

When to save – email messages that can be considered to be records should be saved as soon as possible. Most email messages will form part of an email conversation string. Where an email string has formed as part of a discussion it is not necessary to save each new part of the conversation, i.e. every reply, separately. There is no need to wait until the end of the conversation before capturing the email string as several subjects might have been covered. Email strings should be saved as records at significant points during the conversation, rather than waiting to the end of the conversation because it might not be apparent when the conversation has finished.

Where to save – email messages that constitute records must be saved in an email folder. The GLA has a folder structure based on the records management classification scheme. This folder structure ensures that email messages saved as records are located with other records relating to the same business activity. Email messages that have not been saved within a folder will be automatically deleted after three months.

back to top

Appendix 1 - Guidelines for writing business email messages

Subject line

- Ensure the subject line gives a clear indication of the content of the message
- Indicate if the subject matter is sensitive
- Use flags to indicate whether the message is of high or low importance and the speed with which an action is required
- Indicate whether an action is required or whether the email is for information only if appropriate

Subject and tone

- Greet people by name at the beginning of an email message
- Identify yourself at the beginning of the message when contacting someone for the first time
- Ensure that the purpose and content of the email message is clearly explained
- Include a signature with your own contact details
- Ensure your signature is not unnecessarily long

- Ensure that the email is polite and courteous
- Tone of an email message should match the intended outcome
- Make a clear distinction between fact and opinion
- Proof read messages before they are sent to check for errors
- Try to limit email messages to one subject per message
- Include the original email message when sending a reply to provide a context
- Where the subject of a string of email messages has significantly changed start new email message, copying relevant sections from the previous string of email messages
- Ensure email messages are not unnecessarily long
- Ensure that attachments are not longer versions of emails
- Summarise the content of attachments in the main body of the email message

Structure and grammar

- Try to use plain English
- Check the spelling within the email message before sending
- Use paragraphs to structure information
- Use an appropriate font style and size
- Put important information at the beginning of the email message
- Avoid using abbreviations
- Avoid using CAPITALS
- Try not to over-use bold text

Addressing

- Distribute email message only to the people who need to know the information
- Using ‘reply all’ will send the reply to everyone included in the original email. Think carefully before using ‘reply all’ as it is unlikely that everyone included will need to know your reply.
- Use the ‘To’ field for people who are required to take further action and the ‘cc’ field for people who are included for information only.
- Think carefully about who should be included in the ‘cc’ field and keep the list as short as possible.
- Ensure the email message is correctly addressed

General

- Be aware that different computer systems will affect the layout of an email message
- Be aware that some computer systems might have difficulties with attachments
- Observe the restrictions on attachment size (attachments larger than 35Mb in size cannot be sent)

back to top

Appendix 2 – Email security policy

Email and virus scanning and content filtering products are located at the perimeter of the GLA network. The filtering products check all incoming and outgoing Email and Web traffic according to the GLA security policy.

Email security policy

The policy options for email security are split into the following categories:

Virus scanning incoming Email messages and attachments

All MS Office and known content types (130 types approximately) will be passed to a virus scanner for checking.
All attachments including Zip files and archive attachments will be unpacked for virus scanning before classing any content as unsafe and moving to a quarantined area. This is logged and the system administrator is notified.
All unknown Email content types including password protected and encrypted attachments will be quarantined. This is logged and the system administrator is notified.

Email containing a Virus will be blocked and sent to quarantine. This is logged and the system administrator is notified (keep for 14 days).
Email will NOT be automatically cleaned and allowed to pass through the email filter as this may corrupt the email or attachment.
There will be an e-Mail notification to administrator if a virus or unknown content is identified.
There will be an e-Mail notification to the originator of the e-Mail with any virus that their email will not be delivered.
All incoming virus scanning actions are recorded and written to log files

Virus scan outgoing Email messages and attachments

All MS Office and known content types (130 types approximately) will be passed to a virus scanner for checking.
All attachments including Zip files and archive attachments will be unpacked for virus scanning before classing any content as unsafe and moving to a quarantined area. This is logged and the system administrator is notified.
All unknown email content types including password protected and encrypted attachments will be quarantined. This is logged and the system administrator is notified.

Email containing a Virus will be blocked and sent to a quarantined area. This is logged and the system administrator is notified.
Email will NOT be automatically cleaned and allowed to pass through the email filter as this may corrupt the email or any attachments.
There will be an email notification to administrator if a virus or unknown content is identified.
There will be an email notification to the originator of the email with any virus that their email has not been sent.
All outgoing virus scanning actions written to log files.

Email legal Disclaimer for Outgoing Messages

A GLA legal disclaimer is inserted in all outgoing emails

ANTI-SPAM Protection – checking for incoming SPAM and GLA email filter Rules.

SPAM is Unsolicited "junk" email sent to large numbers of people to promote products or services. Sexually explicit unsolicited email is called "porn spam." This also refers to inappropriate promotional or commercial postings to discussion groups or bulletin boards.

Block email from an unknown, un-trusted source or from an unqualified GLA Domain.
Block email containing SPAM, quarantine, log and notify administrator
Block virus hoax message, quarantine, log and notify administrator
Block chain letters, quarantine, log and notify administrator

Email content scanning incoming

Block emails larger than 35 MB
Block dangerous attachments types from dangerous file type list, quarantine, log and notify administrator
Block encrypted messages, quarantine, log and notify administrator.
Block password protected attachments, quarantine, log and notify administrator
Block dangerous scripts and code, quarantine, log and notify administrator
Block unknown attachments, quarantine, log and notify administrator
Block executable attachments except for Technology Group, quarantine, log and notify administrator
Log but pass through email containing Java script
Log but pass through email containing fragmented messages
Log but pass through offensive language
Log but pass through VIDEO files
Log but pass through IMAGE files
Log but pass through SOUND files

Content scanning outgoing

Block emails larger then 35 MB
Block dangerous attachments types from dangerous file type list, quarantine, log and notify administrator
Block encrypted messages, quarantine, log and notify administrator
Block password protected attachments, quarantine, log and notify administrator
Block dangerous scripts and code, quarantine, log and notify administrator
Block unknown attachments, quarantine, log and notify administrator
Block executable attachments except for Technology Group, quarantine, log and notify administrator
Log and pass through email containing Java script
Block spoofed and relay messages, quarantine, log and notify administrator.
Log but pass through offensive language
Log but pass through VIDEO files
Log but pass through IMAGE files
Log but pass through SOUND files

Offensive image security incoming

Log and notify administrator of offensive image but pass through

Offensive image security outgoing

Log and notify administrator of offensive image but pass through

back to top

GREATER**LONDON**AUTHORITY

GLA Records Management Guidance for moving to The Crystal

Date of approval and issue	March 2021
Version	1.0
Approved by	Governance Steering Group
Changes from previous version	
Review date	May 2021
Senior owner	Executive Director Strategy & Communications
Document owner	Information Governance Manager & Data Protection Officer

Contents

Introduction 2
Aim 3
Why do we need to do this? 3
What storage options will be available? 3
What do we mean by paper and physical files and documents? 4
How do we approach reviewing our information?...4
Step 1 - Review 6
Step 2 - Consider 8
Step 3 – Decide: Paper vs Electronic 10
Step 4 – Convert and Store..12
Approvals and amendments...15
Annex A – Using appropriate filing structures 16
Annex B – File Naming Conventions 18

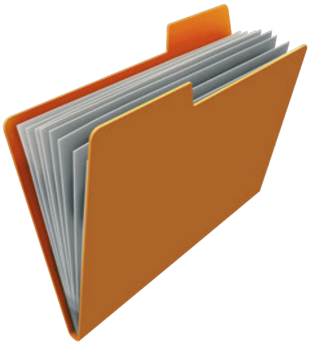
Introduction

The GLA is relocating City Hall to The Crystal at the Royal Docks and occupying two floors at the London Fire Brigade building on Union Street.

New working arrangements at The Crystal and Union Street will involve a significant reduction in the availability of storage for paper-based records

This guidance has been prepared for teams to assist in your plans for preparing to review and remove physical records held in the current City Hall and Union Street.

Over the past year, most GLA teams have successfully adapted to remote working arrangements and have developed new ways of managing the information we work with to carry-out our day-to-day functions, supported by the introduction of new IT hardware and software tools which we will carry forward into our new way of working.



Prior to March 2020, the GLA has become accustomed to storing information in hotboxes, cupboards and filing cabinets near our desks in the office.

Facilities for storing paper-based files and records will not be available at The Crystal and Union Street owing to strict restrictions on the space available.

The GLA therefore needs to take urgent steps to facilitate the destruction of all non-essential paper-based and physical records in City Hall and Union Street **by early June 2021.** This is a core element of the Transition Programme supporting the GLA's move to The Crystal and is critical step to allow the Facilities Management team to 'sign off' the return of the building to our current landlord.

The GLA will need to work with COVID-19 restrictions as we move forward in to 2021 as these may affect how and when staff can able to physically access the buildings. This is under constant review by the Transition Team and Corporate Management Team. However, this does not detract from the fact that the GLA must have 'cleared out' the records from City Hall by early June 2021.

The work required prepare for vacating City Hall ahead of the move to The Crystal requires immediate action and careful planning.

Aim

All staff are required to immediately start reviewing their paper and physical records, to destroy anything which does not need to be kept.

This guidance sets out practical steps to support staff in reviewing the physical records and files that are held in their office space, and to assess what records can be destroyed, digitised or achieved.

This guidance applies to all GLA employees, elected Members and Mayoral Appointees who are based at City Hall, Union Street or any other GLA premises who are affected by the relocation to The Crystal.

Why do we need to do this?

Filing cabinets, drawers and cupboards for physical files or media will not be available to staff working at Union Street or The Crystal for storing paperwork.

Staff working from Union Street and The Crystal will be based around anchor-points, rather than having fixed desks. Coupled with an increase in flexible and remote working, staff will no longer have pedestals and hot-boxes to store personal belongings or paperwork. They are not a practical solution for staff who might regularly work across both sites. It would not be a cost-effective use of the space available to us.

All paper files and all other physical media at City Hall need to be reviewed and either destroyed, digitised or archived before early June 2021.

What storage options will be available?

Staff will not have any personal storage (hotboxes or pedestals) available to them at either Union Street or the Crystal. Teams will not have dedicated filing cabinets, drawers or cupboards for storing any files, paperwork or other physical media.

Limited temporary storage will be made available at both sites to facilitate specific processes – e.g. the delivery of printed publications before distribution, or to receive and review boxes of archived information. Further information about any such arrangements will be made available by the Transformation Team in due course.

Most of the physical records and paper files held at City Hall and Union Street can probably simply be destroyed. The most appropriate methods for retaining the remaining information will be to scan or digitise paper records to be stored electronically on GLA shared drives.

Where there is a clear legal or valid business requirement for the file or document to be kept in a paper format, records can be archived and held in GLA's off-site records store managed by Deepstore. This is a costly option and should only be used as an exception for specific records, not as a general dumping ground for files which could either be digitised or otherwise destroyed.

Assembly Members' constituency casework and related documents should be managed and stored through the existing Caseworker system available to all Members. Please contact Ed Williams or Georgie Abbott to discuss this further where necessary.

What do we mean by paper and physical files and documents?

In a nutshell, anything which is not an electronic file, something saved digitally, or available on the GLA IT network, including the Intranet, shared-drives, GLA databases or online services. It therefore includes, but is not limited to, the following:

- All print-outs, photocopies, letters, invoices, statements etc
- All containers and boxes containing paper files or documents – ring binders, box files, cardboard folders, storage boxes etc
- Any notebooks, notepads or diaries;
- Printed publications, journals, books, pamphlets, books etc.

How do we approach reviewing our information?

Each team is responsible for reviewing their information.

If you do not review your paper files before the GLA is required to have cleared City Hall, they will be removed by FM and destroyed.

Your team will remain accountable for the loss of any critical information from this action, not FM and not the Information Governance Team.

You may wish to refer to the GLA Records Management Policy which sets out the GLAs approach to records management in support of this guidance. This includes specific guidance on **Mayoral and Assembly Member Recordkeeping.**

The approach to reviewing our information needs to **methodical and thorough**.

The GLA's records are its corporate memory, and are necessary for good corporate governance, to be accountable, to comply with legal requirements, to provide evidence of decisions and actions, and to provide information for future decision-making.

We acknowledge that many teams will have a large quantity of information that they will need to review, in a limited amount of time, with finite resources, and at a time when access to City Hall and Union Street might be restricted due to COVID19 restrictions.

The practicalities of our situation therefore require us to also be **ruthless and decisive** in our decisions to dispose of information which does not need to be held and is superfluous to our current ways of working.

Our approach should always focus on the appropriate disposal of redundant, out of date, or superfluous information. You should only retain information where there is a genuine, valid and legal need to do so. You should therefore follow these four steps:

- **Review** – At the outset, identify files that are no longer required, or might now be redundant, out of date, or otherwise superfluous that can be destroyed.
- **Consider** – Consider whether that file or document is a duplicate of an existing record, a printout of an electronic file, or if it is held elsewhere.
- **Decide** – If there isn't a legal obligation or a clear business need for the information to be kept in a paper format, scan it and save it electronically.
- **Convert & Store** – Ensure newly scanned or converted files are saved appropriately, and any remaining files are prepared to be stored in GLA off-site archives.

The table below highlights some of the key questions that should be considered for each of these steps, and these are covered in greater detail in the following sections of this guidance.

Review

- Does the file or document need to be kept?
- Can it be destroyed?
- Can you clearly identify why you need to keep it?

Consider

- Is it a printout of a file or document that is held digitally?
- Is the file or document unique or do other copies exist?
- Was the file or document produced by another GLA team?

Decide

- Is there a clear legal or legitimate business requirement for the file or document to be kept in a paper format?
- Is the information suitable for scanning or archiving?

Convert and Store

- Have you collated relevant records together?
- Where are you going to save your scanned / digitised information?
- Have you correctly prepared the relevant documents for archiving?

Step 1 - Review

The aim of this first step is to quickly dispose of anything that does not need to be kept.

- **The GLA cannot afford to keep large volumes of superfluous, redundant or inconsequential paper-based files.**

- **The bulk of the paper files and documents stored at City Hall or Union Street either do not need to be kept in a paper format, or do not need to be kept at all.**

- **You will need to be pragmatic and decisive. Be honest with yourself when asking if there is a *genuine* need for information to be retained, either as a paper file or electronically.**

- **The decisions taken at this step have the greatest impact; reducing the amount of information to consider moving forward, significantly reducing the cost and time taken to preserve information later on.**

- **If you don't need it, either shred it, put it in a confidential waste bin or a paper recycling bin depending on its sensitivity. FM will be able to provide dedicated bins for large quantities of documents.**

- **If you think something needs to be kept, put it to one side and come back to it in Step 2 once you've have cleared out everything that can be disposed of.**

It is important to emphasise that the GLA does not need to retain its information forever.

It is a common misconception that retaining information indefinitely mitigates risk. Retaining specific information for a defined period of time does promote accountability and transparency of our actions and decisions, but that same information can become a risk if it is retained for too long.

Out-of-date and inaccurate information becomes a risk as it might incorrectly be relied on or referred to.

Another common myth is that information needs to be kept in case we receive a Freedom of Information Act request. This is not the case.

FoIA covers information held at the time a request is received, and the Act actively encourages effective records management and the disposal of information in accordance with an established records management policy. Information which is held longer than necessary is still subject to a FoIA request. This makes them more time consuming to answer and can create complications in adding context to out-of-date information.

The GLA Records Management Policy contains our **Retention and Disposal Schedule (RDS)** which sets our clear retention periods for specific classes of information where we have an obligation to retain information, either to adhere to a specific legal requirement or a because of an agreed organisation need to retain that information.

Please read the RDS carefully to identify records which might need to be retained.

Civil servants have a habit of keeping information "just in case".

Files, emails and notes are squirreled away "just in case" they might be needed to justify actions or how a decision was made.These "personal stashes" often duplicate formal records that were designed to provide an authentic and auditable account of decision making, resulting in large quantities of duplicate unstructured information.

But in most cases, they serve very little purpose.

We then tend to forget where we stored that information because it either wasn't stored centrally or wasn't named properly. So, on the rare occasion when the "just in case" situations comes to pass, we have forgotten where that information was stored or can no longer find it. It has then ceased to have had a purpose.

If a formal record of a decision or action needs to be kept, make sure it is stored in an accessible location with a meaningful name.

Review your information by considering the following questions in order. If the answer to all of these questions is *'no'*, the information can probably be destroyed. If the answer is *'yes'*, put that information to one side, and come back to it in Step 2

1. **Is there a legal or regulatory obligation or requirement to retain the information?**
   If the information is covered by one of the specific legislative or regulatory requirements listed in the RDS, information should be kept for the specified period.

2. **Is the information likely to be relevant to any claim against the GLA, potential litigation or regulatory investigation?**
   Records should not be destroyed if there is ongoing or existing litigation or regulatory investigation. Records that might be required to support the GLA's position in the event of any such claim should be retained in line with the provisions of the Limitations Act 1980 set out in the RDS.

3. **Does the information relate to work on GLA policies, proposals, strategies and projects; or matters relating to corporate governance and management of the authority?**
   These records should be retained for the duration of the Mayoral Term in which they were created (i.e. the current Mayoral Term) and for the duration of the subsequent Mayoral Term. For the purposes of this guidance, a 'Mayoral Term' lasts from the 1st April directly before a mayoral election until the 31st March before the next election. For example:

   - 1st April 2012 to 31st March 2016;
   - 1st April 2016 to 31st March 2021.

4. **Does the information have significant historical value?**
   This will only apply to a very limited number of records, but these can be transferred to the London Metropolitan Archives for permanent preservation. Please see the Historical Archiving Policy in the GLA Records Management Policy.

Each team is responsible for reviewing their information.
If you do not review your paper files before the GLA is required to have cleared City Hall, they will be removed by FM and destroyed.
Your team will remain accountable for the loss of any critical information from this action, not FM or the Information Governance Team.

Remember, the aim here is to quickly and effectively identify what can be destroyed so that you only need to consider relevant information that needs to be kept.

Step 2 - Consider

The aim of this step is to further reduce the amount of information that you will either need to scan or archive.

In Step 1, you identified information that could be destroyed from information which should be retained. You will now need to consider whether paper records and files you still have are a duplicate of existing records held elsewhere. If information is held elsewhere, do you really need to keep or save another copy?

Saving duplicate documents not only increases the amount of work that will be required to scan and save each file but will also increases the amount of storage used on GLA IT systems. The same applies if you create your own copy of a document elsewhere. You should also remember that if you are relying on a copy of the original document, your version could become out-of-date or inaccurate.

THERE IS NO NEED TO KEEP A PAPER PRINTOUT OF AN ELECTRONIC FILE.

- If you have a print-out of an electronic file that your team created or that is otherwise still available electronically, you don't need a paper copy. **Shred it or put it in a recycling or confidential waste bin.**

- If you have a printout of a document created by another GLA team, if the document needs to be retained, that team is responsible for keeping it. Check with them if you are unsure, but otherwise **shred it or put it in a recycling or confidential waste bin.**

- If no one in your team knows why you hold a paper file or document, or what it relates, to, **shred it or put it in a recycling or confidential waste bin.**

THERE IS RARELY A LEGITIMATE BUSINESS NEED TO HOLD DUPLICATE COPIES OF THE SAME INFORMATION.

- If you have a printout of a document created by another GLA team, if the document needs to be retained, that team is responsible for keeping it. Check with them if you are unsure, but otherwise **shred it or put it in a recycling or confidential waste bin**.

- If you have printed copies of GLA policies or guidance, up-to-date copies are on the intranet or london.gov.uk. **Shred it or put it in a recycling or confidential waste bin.**

- If you have paper copies of meeting agendas, minutes or papers, the team responsible for the meetings are responsible for keeping them. **Shred it or put it in a recycling or confidential waste bin.**

- If you have paper copies of documents relating to MQTs, Mayoral Decisions (including delegated decisions) or Committee papers, formal copies of these are kept by the appropriate teams. Check with them if you are unsure, but otherwise, **shred it or put it in a recycling or confidential waste bin.**

By the end of these first two steps, you should have disposed of the majority of paper documents and files that you hold.

All the paper files you still hold will either need to be scanned and saved or archived.

- **Scanning is time-consuming and resource-intensive.**

- **Archiving requires a lot of preparation and is costly.**

Make sure you now only hold information you genuinely need to keep.

Step 3 – Decide: Paper vs Electronic

You should now only have information which clearly has to be retained AND that you are confident is not already held elsewhere.

The aim of this step is to identify what information needs to be scanned and saved on the GLA IT network, and what information needs to be submitted to archives.

There two key questions that you now need to consider:

IS THERE A CLEAR LEGAL OR LEGITIMATE BUSINESS REQUIREMENT FOR THE FILE OR DOCUMENT TO BE KEPT IN A PAPER FORMAT?

There are very few legal or regulatory requirements, or legitimate business needs, for retaining information as a hard copy. Most files and documents can therefore be scanned and stored electronically with little or no detriment to the purpose why they need to be retained.

- An example of where paper copies must be kept would be documents 'under seal' – i.e. those contracts, deeds, or other legally binding documents which contain or feature a wax seal, a seal 'embossed' onto the document by a special stamp.

In most cases, legal documents, including some deeds, can be executed without wet ink signatures (or a seal). The Governance team has produced guidance to help you determine if a wet ink signature is strictly required.

https://intranet.london.gov.uk/sites/default/files/intranetfiles/executing_formal_docs_electronically_-_v1.3_jul_20.pdf

It is no longer practical for the GLA to retain paper copies of files documents with a clear rationale for doing so.

- An exception to this rule would be large format drawings or plans, which cannot readily be converted into an electronic format without specialised scanning equipment.

If the rationale for keeping paper copies is, *'We have always done it this way'* or '*I thought we were told we had to keep paper copies'*, you will need to investigate what purpose this is supposed to serve, and why an electronic copy would not suffice.

We do not necessarily have to keep paper or hard-copy documents solely for the purposes of internal audit or assurance, or because they might be required to support a legal case or claim.

The GLA has prepared specific guidance to support scanning to protect the legal admissibility of electronic records and documents. This should only be required in a limited number of circumstances and is summarised in Step 4 of this guidance.

If you have questions, please consult the Information Governance Team.

In the absence of clear business purpose, or other legal / regulatory obligation, for doing so, our advice would be to convert paper files to electronic files.

IS ARCHIVING A PAPER RECORD PRACTICAL OR APPROPRIATE?

The only option for retaining paper files is for them to be stored off-site in the archives managed under contract with DeepStore. In many cases archiving will not be a practical option for the paper files you hold.

1. Archiving is costly; the GLA is charged for each box that is held. The GLA has a limited central budget for GLA archiving. Directorates submitting large volumes of information to the archives will need meet the costs of doing so.

2. Archived information is not held on-site; it is not even held in London. Most of our archives are in an old salt mine in Cheshire. The archives are intended for long-term storage and is not a practical option for information that you need frequent or urgent access to. We are charged for withdrawals and re-submissions.

3. The contents of all boxes sent for archiving need to be fully itemised and indexed and have a clearly defined return or destruction date. The documents in storage will be of no use if we can't find what we need when we need it. You will therefore need to ensure this work is complete before any information is sent off-site.

Information should therefore only be sent to archives if:

a) It has to be kept as a hard copy;

b) It cannot be easily scanned or digitised due to its format; and

c) It is not information you are going to rely on, or require, on a regular basis.

Remember that the off-site archives are a repository for the long-term retention of information. It is not a dumping ground for miscellaneous or ephemeral information, or a quick-fix solution for information that hasn't been properly reviewed and catalogued.

Step 4 – Convert and Store

This final step summarises the processes to either scan your remaining paper files and documents to be stored electronically, or to prepare information to be archived.

After this step, you should have no paper files or records left. Your outstanding paper files will either be ready to be transferred to archives, or where they have been scanned and digitised, you will be able to delete those last remaining paper copies.

OFF-SITE ARCHIVING WITH DEEPSTORE

The GLA off-site archiving service is contracted to DeepStore and is overseen by FM and the Information Governance Team. Detailed guidance on how to use this service is published on the intranet - https://intranet.london.gov.uk/pages/site-archiving

Off-site archiving requests must be processed via the online DeepStore System. Advice on how to use the system can be found in a dedicated User Guide published on the intranet.

Access to this online system is only available for registered users, and each team should have at least one registered user. If you don't know who the registered user is for your team, please email the FM Helpdesk ([redacted]london.gov.uk). Requests to register a new user should be made to the FM Helpdesk through your Head of Unit or AD.

To obtain archive boxes, barcodes and tags, you will need to contact FM Helpdesk. Boxes must only be used for items that will be sent to the off-site storage facility; one barcode label and two tags will be supplied with each box requested.

PREPARING DOCUMENTS FOR ARCHIVING

- The standard box size is 38cm long, 28cm wide and 25cm high (i.e. for A4 paper). A3-sized boxes are available but incur additional handling and storage costs.

- Only keep information in lever arch folders, ring binders and box files if it helps group relevant documents together and keep them in the correct order.

- Each box should either contain the same type or class of information, the same piece of policy work, and/or information with the same retention period. For example:
    - Files concerning Planning Application X (2019) – *information relates to the same piece of work and has the same retention period.*

- You should ensure you have a detailed record of the contents of each box. This doesn't need to list every single document in each box but should be sufficiently detailed to be able to identify the right box if you needed to recall the information in the future.

- Each box must be submitted with a specific retention period. You must also specify whether the box should be returned to the GLA or destroyed after this period. Contact the Information Governance Team if you have any questions about retention periods.

- The Facilities Management Team have the right to refuse to accept boxes into the archives if the relevant criteria are not met.

ARCHIVING COSTS

The Head of Facilities Management is responsible for the budget for off-site archiving. Limited one-off additional funds have been allocated to cover processing essential relocation archiving.

- **This will not cover excessive submissions to the archives**, for example, where information is being "dumped" into the archive rather than being properly reviewed.

- In some cases, the costs associated with large deposits may need to be met from the relevant Directorate Budgets, rather than FM. The Head of FM has the final say on whether the central archiving budget will cover any submission to the archives.

SCANNING DOCUMENTS

Most paper files, documents and records will need to be scanned using the Multi-Function Printer (MFP) devices at City Hall and Union Street. Guidance on using the MFPs for scanning is available on the intranet via the links below:

- https://intranet.london.gov.uk/sites/default/files/intranetfiles/using_gla_mfds_booklet_march_2014.pdf

- Video guidance - https://intranet.london.gov.uk/node/6756

Each scanned file will be individually emailed to your email account by the MFP device and will be given the same file name –
'Scanned from a Xerox Multifunction Printer.pdf'

To be effective, scanning using MFP devices requires **planning and preparation**. We recommend you following the following steps.

i. Organise the documents and files you are going to be scanning into a logical order. Group documents based on the work, project or policy that they cover, and/or by date. This will make the following steps considerably easier.

ii. Scan documents in sensible bundles, maybe 5 to 10 documents in one go. Each scanned file will be sent to you as an email with the same file name, and you will need to save each of these files (see below), so it will be easier to tackle these in reasonable chunks.

iii. Before you start scanning, you will need to identify where the information is going to be stored. These documents should not be held in your email account indefinitely and should be saved to an appropriate location on a GLA network 'shared drives'. It should be saved alongside related information where it can be accessed by your team. More information about managing folder structures can be found in Annex A below.

iv. You also need have thought about name the saved file name. Make sure files are saved within consistent and meaningful titles, particularly where they are part of a large series or collection of records. Some examples and suggestions can be found in Annex B.

v. When you scan each document, make sure the MFP device is set up to correctly scan that document. For example, is the document single or double sided? All documents should be scanned in black and white, unless where capturing colour is necessary.

vi. Always check to ensure the scanned version is readable and complete before you destroy and paper copies, and that it is been named and saved appropriately.

Please contact the TG Service Desk ([redacted]london.gov.uk) if you have any questions about using the MFP devices.

In exceptional cases, the GLA might be able to engage third-party contractors to digitise a large series of organised and clearly indexed series of records. This will only be possible for files of a consistent nature and type in situations where we can provide a contractor with detailed information to allow them to save and name the resultant files with appropriate levels of detail.

If you have a series of files that might need to be scanned, please contact the Information Governance team in the first instance. The cost of any external scanning might need to be met from Directorate budgets. The Transformation Board has the final say on whether funding is available.

Scanning published material

There are copyright rules about scanning and storing published material, just as there are with photocopying. A limited account of scanning is allowed under 'Fair Dealing', but this applies strictly to private study or research of a non-commercial nature and must not involve dissemination of any kind.

For commercial purposes, material can only be scanned if: (i) the copyright holder has granted permission or (ii) there is a Copyright Licensing Agency scanning licence in place.

Legal Admissibility

Certain signed documents and legal agreements such as deeds or contracts must be scanned to legal admissibility standards found under British Standard (BS10008:2008). This should only be required in a limited number of circumstances if you want to guarantee that your scanned documents are legally admissible in the event of a challenge – i.e. where it is paramount that electronic files possess the following characteristics:

- **Authenticity:** trustworthiness of origin and evidential content.
- **Integrity:** retention of the evidential content of the information.
- **Availability:** accessibility of the information as required.

The Information Governance Team has prepared specific guidance to support scanning to BS10008:2008. If you believe this is an appropriate course of action for your records, please contact the Information Governance Team.

Approvals and amendments

This policy was approved by the GLA Governance Steering Group in February 2021

This policy will be subject to periodic review as considered appropriate by GLA Information Governance Manager, Head of Facilities Management and Governance Steering Group.

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:

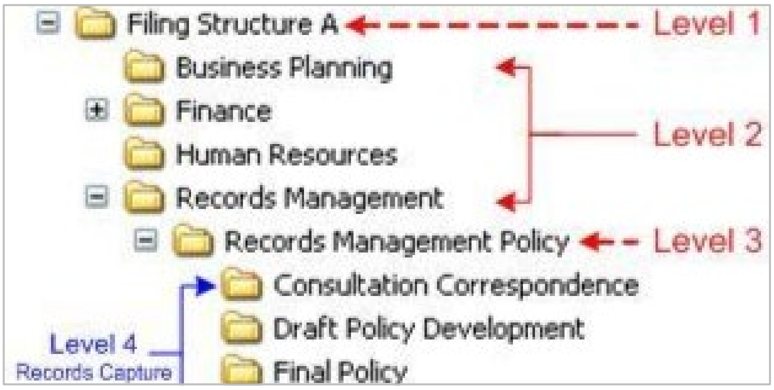
- Be a structure that can be easily interpreted and discourages users from placing records in inappropriate locations
- Use simple names that identify relevant and appropriate folders for saving information

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.