

GREATER LONDON AUTHORITY

[REDACTED]
(By email)

Our Ref: MGLA180117-9950

23 January 2017

Dear [REDACTED]

Thank you for your further request for information which the GLA received on 18 January 2017. Your request has been dealt with under the Freedom of Information Act 2000.

Our response to your request is as follows:

1) Please provide a copy of the current records retention policy of the Greater London Authority.

Please find attached a copy of our current retention schedule, email policy and email guidance for staff.

2) Please state when it was adopted, and provide a copy of the previous records retention policy.

The current schedule (v3) was updated in March 2016. Please find attached a copy of the previous schedule (v2).

The deletion of emails after three months was authorised on 13 December 2004 under Mayoral Approval MA2021.

3) Minutes of the meeting at which it was decided to adopt the current policy.

The current RM policy and R&DS was approved via Director Decision 1482:

<https://www.london.gov.uk/decisions/dd1482-gla-records-management-policy>

Please find attached a copy of MA2021 in relation to the email policy. Please note that the former Mayor of London Ken Livingstone amended the policy from six months to three. He has annotated this next to his signature.

If you have any further questions relating to this matter, please contact me, quoting the reference at the top of this letter.

Yours sincerely

Paul Robinson
Information Governance Officer

If you are unhappy with the way the GLA has handled your request, you may complain using the GLA's FOI complaints and internal review procedure, available at:

<https://www.london.gov.uk/about-us/governance-and-spending/sharing-our-information/freedom-information>

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 mailbox 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 mailbox before being removed
- An indication of the length of time the folder will exist, where possible

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 inbox. The main points to consider when managing email records are:

- Identifying email records
- Who is responsible 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

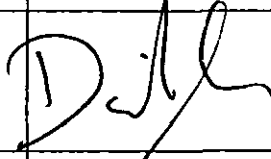
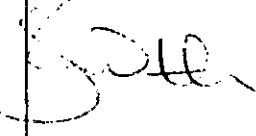
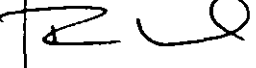
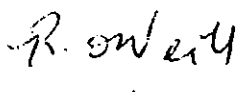
[back to top](#)

Request for Mayoral Approval – MA2021

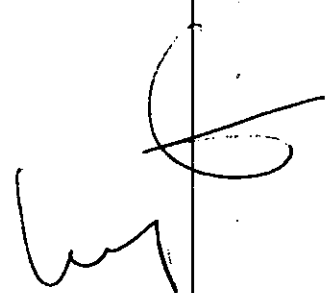
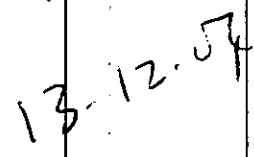
Decision Required:

The Mayor is asked to:

1. Approve the proposed Email Policy for the GLA

Name	Comment	Signature	Date
Originating Officer	Name: David Munn, Head of Technology Group Extension Number: 6531		12/11/04
Janet Worth Sponsoring Director	I have reviewed the request and am satisfied that • the details are correct • the proposal is consistent with the Mayor's vision and objectives and the business plan • the equalities issues/impact have been considered		12/11/04
Anne McMeel Executive Director of Finance & Performance	I have commented on the financial implications of the proposal		12/11/04
Howard Carter, Head of Law	I have commented on the legal implications of the proposal		12/11/04
Redmond O'Neill Policy Director or Mayoral Adviser	I have been consulted about the proposal and agree the recommendations		26 11 04
Mayor's Chief of Staff	I am satisfied that this is an appropriate request to be submitted to the Mayor Comments:		13/12/04

Email policy should cover use of emails is consistent with the Code of Conduct.

Ken Livingstone Mayor of London	The above request has my approval (NB, modify this section if you are setting out options) Comments: subject to the following amendment insert EIA E-Med Policy Page 10. 6.4, second paragraph, line 5 delete '6' insert '3'.		

Where this form is signed under delegated authority on behalf of the Mayor, please note the time of any discussion or correspondence with the Mayor:

--

Request for Mayoral Approval – MA2021

Supporting report

1. Purpose and decision required

The Mayor is asked to approve the proposed GLA email policy.

2. Detail of proposal (to include links with Business Plan)

2.1 This email policy sets out the obligations that everyone in the GLA has when dealing with email messages. The policy is due to go to BMAC on 1st December.

2.2 The policy applies to everyone in the Greater London Authority. 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 with contributions from the GLA Records Manager and Legal Services.

2.3 It has been produced to complement work that has been undertaken on records management (e.g. the GLA Records Management Policy and Retention Schedule – which provide guidance on what constitutes a record and how long they should be retained) and should assist the GLA in meeting its obligations under Freedom of Information (FOI) legislation.

2.4 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.

2.5 Guidance based on this policy will be produced and training will be provided as part of the work being undertaken on records management.

2.6 *Sending Email Messages includes:*

- It is the responsibility of the person sending an email message to decide whether email is the most appropriate method to communicate the information.
- When writing business email messages it is important that consideration is given to the way in which the message is being conveyed.
- Guidance is provided on dealing with sensitive subjects and writing business emails

2.7 *Managing Email Messages includes:*

- 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.

- 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 to appropriate email folders.
- Email messages are automatically deleted from the inbox and 'Sent Items' mailbox after 6 months.
- 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).
- Guidance is provided on the use of shared and public email folders

3. Equalities Implications

No implications are envisaged.

4. Health and sustainable development

No health and sustainable development implications are envisaged.

5. Consultation

The Policy was developed in consultation with the GLA's IT Strategy Board with contributions from the GLA Records Manager and Legal Services.

6. Strategy Implications

None

7. Legal Implications

- 7.1 Under S.34 of the Greater London Authority Act 1999 (the Act) the Authority acting by the Mayor or the Assembly may do anything which is calculated to facilitate or is conducive or incidental to the functions of the Authority. The provision of ICT equipment and services and policies and procedures governing the management and usage of those vices clearly facilitates the operation of the Authority.
- 7.2 The GLA allows staff personal use of it's ICT facilities as long as usage is not excessive and is undertaken without impact on work requirements. Policies and procedures governing the use of ICT for both work related and personal use are already in place and form part of the terms and conditions of employment of all staff. Breaches can therefore result in disciplinary action. Any changes to the process should be agreed with staff and representatives before implementation.

7.3 Regard also has to be had to the statutory requirements in respect of email usage in particular governing the interception and use of emails on an office system whether they are private or work related.

8. Financial Implications

With regard to the policy and its implementation, there are no direct financial implications arising from this report.

9. Supporting/background papers

Email Policy

Please ensure that you have included your name and contact number on the front of the form.

Greater London Authority Records Retention Schedule

- [Introductory Notes](#)
 - [What is a retention schedule?](#)
 - [Benefits of a retention schedule](#)
 - [Retention periods and organisational value](#)
 - [Understanding the GLA records retention schedule](#)
 - [Using the retention schedule](#)
- [GLA records retention schedule](#)

This records retention schedule should be read in conjunction with the GLA's Records Management Policy which states that all GLA staff will dispose of records not required for a specific legal, business, operational or historical purpose in a timely and efficient manner, in accordance with the GLA's retention schedule. Guidance on what type of records should be kept is in [Records Management Quick Guide 2 – Keeping records for corporate requirements](#).

What is a retention schedule?

A retention schedule is a set of rules identifying classes of records and specifying their retention periods and what should happen to them at the end of that period. 'Records class' is the term used for a set of records consisting of individual records which are similar in nature and result from the same activity, either in a particular business unit or throughout the GLA. Aggregating these records into records classes ensures consistency and cuts down on the time and resources needed to make and apply retention and disposal decisions.

Benefits of a retention schedule

- Records of continuing value are identified and can be managed appropriately
- Records which cease to have any value to the GLA can be disposed of efficiently
- Clear instructions on what happens to records when they are no longer needed to support GLA business
- Definitive periods of time for which records should be kept and remain accessible
- Consistency in retention of records across the GLA
- Evidence of compliance with legal and regulatory requirements for the retention of records
- Evidence of what records were created but subsequently destroyed.

Retention periods and organisational value

The retention periods in this schedule have been set according to organisational value and, if applicable, the historical value of the records.

Organisational value focuses on the GLA's needs and obligations and on the records as information assets. It is about value for accountability, legal or reference purposes, and

includes protection of the legal and other rights of the GLA and those with whom it deals, and compliance with whatever regulatory framework applies.

In determining organisational value, the following factors are considered:

- The importance of the function that the records support.
- Comments from business units about their requirements for continued access to the records, including the risks of not having this access.
- The importance of the records for protecting the interests and legal rights of the organisation and those with whom it deals.
- Any legal or regulatory requirements – even if they do not actually specify the length of time records must be kept, they may include relevant things like liability thresholds.
- The requirements of any body with a right to audit the GLA.
- Any accepted standards or best practice within the public sector.
- The relationship between the records and other related records and the data or evidence they provide.

Often information-rich, cumulative or summary records will be kept in the longer term while more detailed, bulky but ephemeral records can and should be destroyed earlier. For example, the quarterly accounting reports will be kept in the longer term while the weekly reports that contribute to them can be destroyed once the quarterly report has been compiled.

Using the retention schedule

The retention schedule has been developed to be used in the following ways:

When new records are created

The retention schedule should be used as a point of reference in the day-to-day management of records. The most effective point in the lifecycle of any record at which to decide how long it should be retained, and for what reason, is when that record is created.

When opening a new file, creating an electronic record or typing a letter, this retention schedule will act as a guide to the conditions under which that record should be managed, stored and ultimately disposed of.

When designing or implementing a new paper filing system

Any new office system intended to improve the efficiency of paper filing should be designed with a clear understanding of the legal and business requirement for record keeping, when they should eventually be destroyed and whether records should be transferred to the London Metropolitan Archives for permanent preservation.

When transferring files to off-site storage

Office space is at a premium at City Hall and it is rarely possible to retain files on-site for the length of time for which they have to be retained. The retention schedule should always be consulted when transferring files to the Crown off-site records store.

When destroying files

In order to protect itself and minimise risk, the GLA should not maintain records longer than it needs to; nor should it destroy records sooner than is required. The retention schedule provides consistent guidelines on the retention period of all of the GLA's records.

Understanding the GLA Records Retention Schedule

Code to facilitate cross-referencing with the Crown Records Management system (used to send records for off-site storage)

Functional area

Amount of time the record should be retained (retention period); event after which the retention period is applied (trigger); and action to be taken once record has exceeded its retention period

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-BF	Building and facilities management Management of City Hall and other GLA buildings, their facilities and equipment. Includes security, maintenance of GLA buildings and the environments within them, stock control and room booking				
1-BF-0001	Access control records	Key logs; key registers; security data logs	Destroy 2 years after end of year covered	Business requirement	
1-BF-0002	Activity and event records	Facilities management planning for specific events held within City Hall or other GLA facilities (includes events booked by external bodies such as charities); booking forms; function sheets; London's Living Room diary	Destroy 2 years after last action	Business requirement	
1-CM	Corporate Management Management and approval of corporate activities. Includes mechanisms for decision making, business planning and the development of corporate policies and procedures				
1-CM-0001	Audit reports		Destroy 6 years after report is published	Audit requirement	
1-CM-0002	Audit Working papers		Destroy 3 years after report is published	Business requirement	Audit reports will usually be submitted to the Assembly and will be preserved permanently as part of democracy/ Assembly, committee and scrutiny meetings records (final version)

Other relevant information such as related records

Title/description of the records – enables the entry in the schedule to be matched with the records

Legal/regulatory/ business need guiding retention

GLA RECORDS RETENTION SCHEDULE (Version 2 – 2012 edition)

1. Select the functional area that your record falls under
2. Identify the records class that describes your record, using the example column for assistance
3. Note the retention period and what to do once that period expires

Alternatively, you can search the schedule by pressing **Ctrl+F** on your keyboard and entering keywords relating to your records.

Functional areas:

- [Building and facilities management](#)
- [Corporate management](#)
- [Democracy](#)
- [Financial management](#)
- [Health and safety](#)
- [Human Resources](#)
- [ICT](#)
- [Information Management](#)
- [Legal](#)
- [Mayoral strategies](#)
- [Planning and building control](#)
- [Procurement activities](#)
- [Project management](#)
- [Public relations](#)
- [Risk management and insurance](#)
- [Strategic partnerships](#)

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-BF	Building and facilities management (including events and Squares management) Management of City Hall and other GLA buildings, their facilities and equipment. Includes security, maintenance of GLA buildings and the environments within them, stock control and room booking. Also organisation and promotion of events and ceremonies by the GLA and management of London Squares under the GLA's control.				
1-BF-0001	Access control records	Key logs; key registers; security data logs	Destroy 2 years after end of year covered	Business requirement	
1-BF-0002	Activity and event records	Facilities management planning for specific events held within City Hall or other GLA facilities (includes events booked by external bodies such as charities); booking forms; function sheets; London's Living Room diary	Destroy 2 years after last action	Business requirement	
1-BF-0003	BREEAM (Environmental Assessment Method) documentation		Destroy when superseded		
1-BF-0007	Lease management	Lease for City Hall; correspondence relating to lease	Destroy 6 years after lease is superseded or terminated	Statutory (Statute of Limitations)	
1-BF-0008	Lost property records	Lost property log	Destroy 1 year after last entry		
1-BF-0009	Maintenance records (of City Hall/other buildings/sites)	Cleaning; painting; fault reports	Destroy 7 years after last action	Statutory (Statute of Limitations)	
1-BF-0010	Maintenance records (of equipment)	Service records; plant files; fault reports	Destroy 7 years after disposal of equipment	Statutory (Statute of Limitations)	
1-BF-0011	Operational Log Book		Destroy 1 year after last entry		
1-BF-0012	Out of hours sign-in book		Destroy 1 year after last entry		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-BF-0013	Patrol records	Deister patrol database entries; incident reports	Destroy 1 year after last action		
1-BF-0014	Retained items records	Retained items forms; related correspondence	Destroy once item returned to owner		
1-BF-0015	Security pass records	Applications for security pass; correspondence regarding checks and other related issues	Destroy 1 year after end of year that member of staff/Mayor/Assembly Member leaves		
1-BF-0016	Temporary pass records	Temporary pass log	Destroy 1 year after end of year covered		
1-BF-0017	Theft reports and investigations	Theft reports; investigations into reported thefts; records of action taken	Destroy 6 years after last action		
1-BF-0018	Water treatment records	Records kept to comply with statutory duties	Destroy 6 years after last inspection	Statutory	
1-BF-0019	Conference management records	Planning of conference – correspondence; attendance lists	Destroy 2 years after end of conference		Previously 1-EM-0001 under version 1 of retention schedule (moved on request of FM)
1-BF-0020	Maintenance of Squares' infrastructure	Maintenance records	Destroy 12 years after last dated record	Statutory (Statute of Limitations)	Previously 1-EM-0004 under version 1 of retention schedule (moved on request of FM)
1-BF-0021	Organisation of event records	Event files/folders	Destroy 6 years after event		Previously 1-EM-0005 under version 1 of retention schedule (moved on request of FM)
1-BF-0022	Recording of ceremonial events and civic occasions	Visitors' books; audio-visual recordings; photographs	Transfer to London Metropolitan Archives after 2 years		Previously 1-EM-0006 under version 1 of retention schedule (moved on request of FM)
1-CM	Corporate Management Management and approval of corporate activities. Includes mechanisms for decision making, business planning and the development of corporate policies and procedures				
1-CM-0001	Audit reports		Destroy 6 years after report is published	Audit requirement	
1-CM-0002	Audit Working papers		Destroy 3 years after report is published	Business requirement	Audit reports will usually be submitted to the Assembly and will be preserved permanently as part of democracy/ Assembly, committee

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
					and scrutiny meetings records (final version)
1-CM-0005	Business Plan	Published with annual budget of GLA	One copy to be retained permanently by Finance and Performance; one copy to be transferred to LMA on publication		
1-CM-0006	Business Plan – drafting	Drafts; departmental submissions	Destroy once plan has been approved		
1-CM-0009	Contacts details	Name, address and telephone number; biographical notes; company/organisation	Destroy when new information supplied; when no longer available; when no longer required; on request by data subject	Statutory (Data Protection Act)	
1-CM-0010	Cross-directorate/strategic working groups and meetings records	Governance Steering Group	Convenors of group to destroy records 5 years after end of year in which meeting took place		
1-CM-0012	Directors' Decisions (DDs)		Corporate Management Team (CMT) to retain permanently. All other copies to be treated as duplicates. Treat significant drafts as Policies and Procedures (Corporate).		
1-CM-0017	Mayor's Annual Report	Mayor's Annual Report; Mayor's Annual Equalities Report	Treat as Public Relations/GLA Publication		
1-CM-0019	Mayoral Decisions (MDs)		Corporate Management Team (CMT) to retain		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
			permanently. All other copies to be treated as duplicates. Treat significant drafts as Policies and Procedures (Corporate)		
1-CM-0023	Policies and procedures – corporate	Equalities policies and toolkit; Records Management Policy; Data Protection Policy; Procurement Policy; Finance Manual; Retention schedule; complaints and comments procedure/policy; Health and Safety Policy; HR Handbook; code of ethics and standards for staff	Destroy master set (held by policy/procedure owners) 6 years after superseded; treat all others as duplicates. NB most significant policies and procedures will be retained as part of BMAC, MDs or DDs papers	Statutory for some	
1-DM	Democracy Management of democratic activities including elections, meetings of the London Assembly, its committees and scrutiny, and standards for elected members. Includes support of elected members and political groups				
1-DM-0001	Assembly, Committee and Scrutiny meetings records – drafts and working papers	Drafts of reports; corrections of evidence; published information collected as part of inquiries; proofs of evidence and reports; routine correspondence	Destroy 1 year after inquiry is completed/meeting has taken place NB: in the case of requests for information please see Public Relations		
1-DM-0002	Assembly, Committee and Scrutiny meetings records (final version)	Minutes; Agenda; Business Papers; Reports; Indexes; significant briefings; evidence given to	Master to be kept permanently by Secretariat; transfer copy of all papers to London Metropolitan		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		scrutiny and committees; Mayor's reports to London Assembly; non-routine correspondence leading to changes of procedure or major decisions	Archives annually		
1-DM-0003	Biographical records of elected Members	Biographies of elected Members; photographs	Destroy when Member leaves office		
1-DM-0004	Briefings (formal) regarding GLA policy and development of policy	Briefings to Mayor, Deputy Mayor, Assembly Members	Review for transfer to London Metropolitan Archives 2 years after last action		
1-DM-0005	Contact details/biographical information relating to witnesses and specialist advisers (committees and scrutiny)	Name, address and telephone number; biographical notes; expertise	Destroy when new information supplied; when no longer available; when no longer required; on request by data subject	Statutory (Data Protection Act)	
1-DM-0006	Elections - planning	Minutes of meetings; planning; reports	Destroy 12 months after close of poll		
1-DM-0007	Elections – ballot papers		Destroy 12 months after close of poll	Statutory (Representation of the Peoples Act)	Section 57 of Act
1-DM-0008	Elections – declaration of results	Consolidated returns of votes received	Destroy 6 months after close of poll	Statutory (Representation of the Peoples Act)	
1-DM-0009	Elections – expenses claimed by candidates		Destroy 12 months after end of financial year	Statutory (Representation of the Peoples Act)	
1-DM-0010	Elections – results		Retain permanently		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-DM-0011	Gifts given to visitors by elected Members	Orders; invoices	Destroy 6 years after end of financial year	Statutory (Audit)	
1-DM-0013	Mayor's Question Time	Agenda; recordings; minutes; notes	Transfer to London Metropolitan Archives annually		
1-DM-0014	Mayor's Question Time Database	Record of questions asked and answers received	Keep permanently in electronic form; available on GLA website		
1-DM-0015	Mayor's Question Time administration	Questions received; planning of MQT; related correspondence. Draft notes should be treated as ephemera.	Destroy 2 years after MQT		
1-DM-0016	Membership of committees/scrutiny	Lists of members; correspondence; minutes of meetings to decide on membership (where not part of committee/scrutiny meetings)	Destroy 5 years after last action		
1-DM-0017	Peoples' Question Time	Recordings; minutes; notes	Transfer to London Metropolitan Archives annually		PQT material is responsibility of External Affairs
1-DM-0018	Peoples' Question Time administration	Questions received; planning of PQT; related correspondence	Destroy 2 years after PQT		PQT material is responsibility of External Affairs
1-DM-0019	Registers of Interests	Register of interests for Mayor and Assembly Members; register of gifts and hospitality received by the Mayor and Members of the Assembly	Transfer to London Metropolitan Archives after end of session covered		
1-DM-0020	Standing Orders		Retain permanently		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-DM-0021	Webcasts	Assembly meetings and other public meetings	Retain permanently		
1-DM-0022	Members correspondence and related information	Constituency casework	Review or transfer to appropriate Member when Member leaves office		
1-FM	Financial Management Management of financial resources by the GLA				
1-FM-0001	Annual statement of accounts		Transfer to London Metropolitan Archives 6 years after end of financial year	Statutory (accounts need to be available for inspection at City Hall for 6 years)	
1-FM-0002	Approvals process records	Delegation of authority; arrangement for the provision of goods and services (for contracting, see Procurement)	Destroy 6 years after end of financial year	Statutory (Audit)	
1-FM-0003	Asset Register		Remove individual items 6 years after end of financial year in which they were disposed of	Statutory (Audit)	
1-FM-0004	Asset Register supporting documentation	Asset disposal records; asset purchase/acquisition records; valuation records	Destroy 6 years after end of financial year in which action was completed	Statutory (Audit)	
1-FM-0005	Borrowing records	Loan records	Destroy 6 years after end of financial year in which loan is repaid	Statutory (Audit)	
1-FM-0006	Budget development records	Unpublished draft budgets; departmental budgets; draft estimates	Destroy 2 years after end of financial year		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-FM-0007	Budget monitoring records	Monitoring of actual revenue and expenditure against budget predictions	Destroy 1 year after end of financial year		
1-FM-0008	Budgets	Draft, final draft and approved component budgets for the GLA and the four functional bodies; any written statement by the Mayor under paragraph 6(5) of Schedule 6 of the GLA Act 1999 as to why he may submit a final draft budget for approval which is not the draft consolidated budget as amended by the London Assembly; proposals and final substitute calculations under Schedule 7 of the GLA Act 1999	One copy of approved component and consolidated budgets and related documents to be retained permanently by Finance and Performance; one copy to be transferred to London Metropolitan Archives on publication; drafts to be destroyed 6 years after end of financial year they relate to	Statutory (budget needs to be available for inspection at City Hall for 6 years)	
1-FM-0009	Capital spending plan	Draft and final capital spending plan under section 123(1) and 123(3) of the GLA Act 1999	One copy to be retained permanently by Finance and Performance; one copy to be transferred to London Metropolitan Archives on publication	Statutory (needs to be available for inspection at City Hall for 6 years)	
1-FM-0010	Copies of transactional records (where original is held by F&P) – see also Transactional records	Invoices; purchase orders; claims; vouchers	Destroy 1 year after end of financial year		Retain in department until destruction
1-FM-0011	Council Tax precept	Calculation records;	Destroy 6 years after	Statutory	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
	records	setting of precept	end of financial year	(Audit)	
1-FM-0012	Employee pay records	Authority sheets; payroll deduction authorities; payroll disbursement; employee pay records; employee taxation records; overtime claims	Destroy 6 years after end of financial year	Statutory (Audit/Taxes Management Act)	
1-FM-0013	General ledger records	General Ledger	Destroy 6 years after end of financial year	Statutory (Audit)	
1-FM-0014	Internal recharging	Recharging records to other groups within the GLA; journal transfer requests	Destroy 6 years after end of financial year	Statutory (Audit)	
1-FM-0015	Periodic statements and reports	Monthly and quarterly reports; monthly and quarterly statements; working papers contributing to these; monthly accrual statements; cashflow statements; creditor listings and reports; debtor listings and reports	Destroy 2 years after end of financial year		
1-FM-0016	Reconciliation records	Reconciliations; summaries of accounts	Destroy 2 years after end of financial year		
1-FM-0017	Taxation records	Taxation records; motor vehicle logs; fringe benefits tax records; group certificates	Destroy 5 years after end of financial year	Statutory (various regulations and audit)	
1-FM-0018	Transactional records identifying receipt and expenditure of financial resources	Allowance claims; work orders; purchase orders; invoices; credit card statements; cash books; receipts; cheque	Destroy 6 years after end of financial year	Statutory (Audit)	Retain in department until day-to-day use has ceased; transfer to Crown until destruction

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		counterfoils; bank statements; subsidiary ledgers; journals; vouchers; catering bookings			
1-FM-0019	Treasury management	Published Annual Strategy Report; half year and year end performance reports	Destroy 6 years after end of financial year	Statutory (Audit)	
1-FM-0020	Treasury management – investment records	Statements; correspondence	Destroy 6 years after end of financial year in which investment is terminated	Statutory (Audit)	
1-HS	Health and safety Management of measures to ensure a healthy and safe workplace				
1-HS-0001	Accident books/Accident Reports		Destroy 3 years after last entry	Statutory (The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995)	
1-HS-0002	Equipment inspection records		Destroy 6 years after destruction of the equipment	Statutory (Statute of Limitations)	
1-HS-0003	Inspection records	Directorate H&S inspection file	Destroy 1 year after last action		
1-HS-0004	Lifting operations inspection records		Destroy once superseded	Statutory (Lifting Operations Regulations 1998)	
1-HS-0005	Process monitoring	Monitoring results	Destroy 3 years after last action	Statutory (Lifting regulations and	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
				others)	
1-HS-0006	Risk assessments		Destroy 3 years after assessment is superseded	Statutory (Lifting regulations and others)	
1-HS-0007	Staff health care arrangements	BUPA health screenings; administration of free eye tests scheme	Destroy 3 years after last action		
1-HR	Human Resources Management of HR activities. Includes individual files on members of staff as well as records of recruitment campaigns, training and development and negotiation of terms and conditions				
1-HR-0001	Disciplinary – Final warning		Destroy record 2 years from date of disciplinary decision		See 1-HR-00024 for Disciplinary – Interview
1-HR-0003	Disciplinary – Warning involving children		Retain on employee file until file is destroyed		
1-HR-0004	Disciplinary – Written warning		Destroy record after 1 year of date of breach		
1-HR-0005	Employee records – health and sickness	Sickness absence records; health declaration/pre-employment health screening; self-certified medical certificates, doctor's certificates, statements of fitness to work, records of major injuries received in the workplace, medical referrals	Destroy 7 years after termination of employment	Statutory Sick Pay (General Regulations 1982 Reg 13) Reporting of injuries, diseases and dangerous occurrences Regs 1995 Reg 7	
1-HR-0006	Employee records (but see below for exceptions)	Contract; initial job application; job offer letter; references; CRB checks; proof of right to work; pre-employment	Destroy 7 years after termination of employment	Statutory (Statute of Limitations, s5) Finance Act	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		health screening; probationary period documentation; changes to terms and conditions; extensions to fixed term contracts; job descriptions of jobs held within GLA; exit interview forms; service termination documents; compromise agreements; application for season ticket loan/bike loan; childcare vouchers		1998 (for season ticket loan, bike loan, childcare vouchers etc)	
1-HR-0007	Employee records required for pension purposes	Annual assessment reports for last 5 years of service; death benefit nomination forms; copies of death/marriage certificates; personal payroll history; pension estimates and awards; summary record – full name and date of birth, NI number, pensionable pay at leaving, reckonable service, reason for leaving, new employer's name, amount and destination of any transfer value paid, amount of any refund of contributions; resignation, termination and/or retirement	Destroy when employee reaches age 72 or 12 years after their death, whichever is sooner	Statutory (Statute of Limitations)	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		letters; added years; AVCs; sick absence records; disciplinary action affecting terms and conditions			
1-HR-0008	Equal opportunities monitoring records	Monitoring forms	Destroy 3 years after end of year received		
1-HR-0009	Grievances records	Correspondence from staff member raising concern; responses; minutes of meetings; decisions; appeals	Destroy 7 years after closure of case	Sex Discrimination Act 1975 & 86; Race Relations Act 1976; Disability Discrimination Act 1995	See 1-HR-0026 for Employment Tribunal
1-HR-0010	Induction and probation records	Probation reports; extension of probationary period; induction courses attended; probationary period termination of employment	Destroy 7 years after termination of employment	Limitations Act 1980 s5	
1-HR-0011	Job descriptions	Job descriptions, evaluation documents	Destroy 7 years after termination of employment	Limitations Act 1980 s5	
1-HR-0012	Leave and attendance monitoring (non-statutory)	Jury service; study leave; special and personal leave (compassionate, study); attendance books; flexitime sheets/records; leave applications; annual leave; signing in books; daily diary sheets (FM); Open Weekend	Destroy 7 years after termination of employment	Limitations Act 1980 s5	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		workers database			
1-HR-0013	Performance monitoring records (official records submitted to and held by HR)	Performance reviews; training and development needs identification	Destroy 7 years after termination of employment	Sex Discrimination Acts 1975 & 1986; Race Relation Act 1976; Disability Discrimination Act 1995	
1-HR-0014	Personnel records held by line managers	Performance review notes; notes of one-to-one meetings	Destroy 2 years after last action (maximum – can be destroyed at any time before)		
1-HR-0015	Records of staff working with children		Destroy no sooner than 25 years after employment ceases	Statutory (Children's Act)	
1-HR-0016	Recruitment records	Advertisements; unsuccessful applications; shortlisting notes; interview reports; interview notes and schedules; unsuccessful applicants' details: rejection letters, feedback information, complaints from unsuccessful candidates (application, references and letter of appointment for successful candidate to be placed on employee file)	For external candidates destroy 2 years after recruitment has been finalised. For internal candidates destroy 7 years after termination of employment	Sex Discrimination Acts 1975 & 1986; Race Relation Act 1976; Disability Discrimination Act 1995	
1-HR-0017	Rotas	Rotas for covering GLA services	Destroy once superseded		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-HR-0018	Staff consultation	Planning; development; questionnaires; responses	Destroy 5 years from closure of file		
1-HR-0019	Statutory leave monitoring	Maternity leave; paternity leave; adoption leave authorisation and administration	Destroy 7 years after termination of employment	Limitations Act 1980 s5 and Finance Act 1998 (for statutory maternity pay claim form)	
1-HR-0020	Training – central record	Lists of attendees	Destroy 7 years after termination of employment. Destroy hard copy once logged on Cyborg	Limitations Act 1980 s5	
1-HR-0021	Training materials	Planning documents; presentations; training materials; notes	Destroy 1 year after course is superseded or 5 years after course given for last time		
1-HR-0022	Training – staff	Certificates; record of attendance; sponsorship details NB: may be kept on personnel file	Destroy 7 years after termination of employment. Destroy hard copy once logged on Cyborg	Limitations Act 1980 s5	
1-HR-0023	CRB check outcomes	Letter from the GLA's appointed agent notifying the outcome of a CRB check on those who will have frequent contact with young people and/or vulnerable adults (eg Peer Outreach Workers, Children and Young People's Unit)	Destroy 7 years after termination of employment	Limitations Act 1980 s5	
1-HR-0024	Disciplinary –	Notes of interview	Destroy 7 years from		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
	Interview		date of disciplinary decision		
1-HR-0025	Employee records relating to finance	Agreement to deduct from payroll; DSS queries; court orders; tax details; subscription details; details of payments	Destroy 7 years from tax year end	Finance Act 1998 Sch 18 Tax Management Act 1970	
1-HR-0026	Employment Tribunal	Case paperwork; minutes and actions; decision	Destroy 7 years after closure of case	Sex Discrimination Act 1975 & 86; Race relations Act 1976; Disability Discrimination Act 1995; Limitations Act 1980 s5	
1-IT	Information and Communications Technology Management of activities involved in providing ICT to the GLA				
1-IT-0001	Backup tapes		Destroy contents after 3 months		
1-IT-0002	Backups – Retrieval of data	Requests from staff or elected members for documents or data to be retrieved from the backups	Destroy 1 year after request has been completed		
1-IT-0003	Development and maintenance of systems records	Specifications; administration details; infrastructure information; testing records	Destroy 5 years after decommissioning of system		
1-IT-0004	Fault reporting and resolution records	ICT Helpdesk transaction records	Destroy 1 year after fault has been resolved		
1-IT-0005	IT Strategy	Development; implementation;	Destroy 5 years after superseded		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		planning; the Technology Framework (for IT Strategy Board papers, please see Corporate Management)			
1-IT-0006	Management information on TG Helpdesk	Statistics; customer satisfaction information	Destroy 4 years after end of financial year		
1-IT-0007	Management of systems development projects	ICT Project records: specifications; project briefs; PIDs; highlight reports; project plans; minutes; framework documents	Destroy 5 years after termination of project		
1-IT-0008	Monitoring and testing records (routine)		Destroy 1 year after end of financial year		
1-IT-0009	Records documenting licensing of software and systems by the GLA	Software licenses; inventories of software	Destroy 2 years after superseded/withdrawn	Statutory (licenses need to be retained to prove ownership until no longer used)	
1-IT-0010	Technical plans	Plans showing networks and connections in City Hall	Destroy when superseded		
1-IT-0011	The Technology Framework	Development; implementation; planning; the Framework itself	Destroy 5 years after superseded		
1-IT-0012	Equipment logging	Laptop and mobile phone booking out logs; security equipment handover signing forms	Destroy 1 year after end of year covered		Under 1-BF in version 1 of retention schedule
1-IM	Information Management Management of information resources, including records, databases, library materials, publications stock etc				

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-IM-0001	Bibliographic databases	Acompline; urbaline; Research Library catalogue	Delete entries when item no longer available		
1-IM-0002	Copyright declarations	Document delivery forms	Destroy 6 years after end of financial year	Statutory (Copyright Act)	
1-IM-0003	Database/system administration	User guides; problems	Destroy 5 years after system becomes obsolete		
1-IM-0004	Disposal records	Disposal certificates provided by contractors to demonstrate that records have been destroyed confidentially	Destroy 12 years after last action.	Statutory (Statute of Limitations)	
1-IM-0005	Document templates		Destroy once superseded		
1-IM-0006	Enquiries to information/research groups	Enquiry forms	Destroy 2 years after end of financial year (though see Public Relations for non-routine/FoI enquiries)		
1-IM-0007	Information about records held at the off-site store	Transmittal forms; entries on Off-site store database	Destroy/delete at end of financial year in which records destroyed or withdrawn from off-site store		
1-IM-0008	Information audits/records surveys		Destroy once superseded		
1-IM-0010	Reference records	Copies of information retained for reference purposes	Destroy when no longer required		Reference files should be weeded regularly to ensure that information that is obsolete is removed
1-IM-0011	Research data published by the GLA's information and research services	Current awareness bulletins; demography and statistics reports; briefings	Retain permanently		
1-IM-0012	Subscriptions to information services	Subscription forms; contact details for	Destroy 6 months after subscription lapses		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		subscribers			
1-LS	Legal Legal records. NB The GLA's legal service is provided by TfL Legal on a shared service basis. Some legal records should therefore be kept by TfL Legal in accordance with their retention schedule.				
1-LS-0001	Advice records	Correspondence; file notes; legal notes; instructions to counsel	Review 6 years after last action; if advice sets major precedent, consider offering to London Metropolitan Archives	Statutory (Statute of Limitations)	
1-LS-0002	Agreement records (not formal contracts)	Correspondence; concordat; agreement of terms; hire agreements; funding agreements; confidential decision forms	Destroy 6 years after agreement expires or is terminated	Statutory (Statute of Limitations)	
1-LS-0003	Byelaws		Retain permanently		
1-LS-0004	Conveyancing files		Destroy 12 years after closure.	Statutory (Statute of Limitations)	
1-LS-0005	Licenses		Destroy 1 year after expiry of licence	Statutory (need to demonstrate that GLA is licensed to carry out activity)	
1-LS-0006	Litigation files	Case correspondence	Destroy 7 years after last action; if case is high profile, review for transfer to Record Office	Statutory (Statute of Limitations)	
1-LS-0007	Real estate disposal records	Legal documents; particulars of sale; Board of Survey; tender documents; conditions	Retain until 15 years after all obligations/entitlements are concluded.	Statutory (Statute of Limitations)	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		of contracts			
1-LS-0008	Section 106 agreements		Retain until agreement is rescinded or replaced	Statutory (Town and Country Planning Act)	
1-MS	Mayoral Strategies Development and implementation of Mayoral strategies and policies. Includes development of policies included in the Mayor's manifesto and development of GLA Group policy. (See Corporate Management for GLA policies regarding internal management.)				
1-MS-0001	Consultation records	Consultation documents; replies; enquiries and objections made by the public; public inquiry documents	Review for possible transfer to London Metropolitan Archives 5 years after consultation is completed		
1-MS-0002	NOTIFY database	NOTIFY notifications database (Housing and Homelessness)	Destroy entries 2 years after households leave temporary accommodation	Statutory (Data Protection)	
1-MS-0004	Published Mayoral Strategies and related publications		See Public Relations/GLA Publications		
1-PB	Planning and Building Control Management of planning decisions referred to the Mayor; development and implementation of the Mayor's Spatial Development Strategy (SDS), also known as the London Plan				
1-PB-0001	Draft planning briefs and planning frameworks	Draft briefs referred to Mayor from boroughs; reports by case officers to the Mayor; the Mayor's decision on planning briefs	Destroy 3 years after superseded		
1-PB-0002	Mayor's SDS (London Plan) Frameworks – final	Development and implementation records	Destroy 3 years after superseded		
1-PB-0003	Mayor's SDS (London Plan) Consultation Responses	London Plan Database; PLU received responses; reference sets in Business	London Plan Database to be retained permanently; PLU responses to be		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		Support	transferred to London Metropolitan Archives when consultation on new plan begins; Business Support to retain one set of responses for reference permanently; other sets to be destroyed once immediate use has ceased		
1-PB-0004	Mayor's SDS development	Minutes of meetings; research; reports; key drafts	Review for transfer to London Metropolitan Archives after 5 years		
1-PB-0005	Mayor's SDS (London Plan) EIP Library		Transfer to London Metropolitan Archives when consultation on new plan begins		
1-PB-0006	Mayor's SDS (London Plan) Publications	The London Plan; the Draft London Plan; Towards the London Plan; guidance publications	See Public Relations/GLA Publications		
1-PB-0007	Mayor's SDS & Planning Meeting records	Minutes; agenda; records of decisions	Transfer to London Metropolitan Archives 5 years after meeting		
1-PB-0010	Planning Briefs		Destroy 3 years after superseded		
1-PB-0011	Stopping up orders	Orders; reports; decisions	Retain permanently		
1-PB-0012	Unitary Development Plan Responses	Submitted UDPs; case officers' reports to the Mayor; Mayor's decisions; records of related meetings	Destroy 5 years after last action		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
1-PB-0013	Urban Strategies implementation	Records of assistance given to major development projects in London	Review for transfer to London Metropolitan Archives 5 years after project is completed		
1-PB-0014	Planning decisions – reports to Mayor		Permanently	GLA practice	Retained electronically and published on website
1-PB-0015	Planning decisions files	All correspondence, plans, etc.	Destroy after 6 years	GLA practice based on planning permission for major schemes being given for 5 years + pre-application period	Transfer to off-site records store (Crown) once regular reference has ceased
1-PC	Procurement Activities involved in procuring goods and services for the GLA. Includes tendering and agreement of contracts NB The GLA's procurement function is provided by TfL Procurement on a shared service basis. Some procurement records should therefore be kept by TfL Procurement in accordance with their retention schedule.				
1-PC-0001	Contract management documents – contracts under seal	Service level agreements; compliance reports; performance reports; minutes and papers of meetings; variations and changes to requirements; extensions; complaints; disputes; quality assessments; quarterly review notes	Destroy 12 years after the terms of the contract have expired	Statutory (Statute of Limitations)	
1-PC-0002	Contract management documents – ordinary contracts over £50,000	Service level agreements; compliance reports; performance reports; minutes and papers of	Destroy 6 years after the terms of the contract have expired	Statutory (Statute of Limitations)/ GLA Contracts Code [amended]	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		meetings; variations and changes to requirements; extensions; complaints; disputes; quality assessments; quarterly review notes		22 October 2008]	
1-PC-0002a	Contract management documents – ordinary contracts under £50,000	Service level agreements; compliance reports; performance reports; minutes and papers of meetings; variations and changes to requirements; extensions; complaints; disputes; quality assessments; quarterly review notes	Destroy 2 years after the terms of the contract have expired	GLA Contracts Code [amended 22 October 2008]	
1-PC-0003	Drafts of specification		Destroy once specification is finalised		
1-PC-0004	Exception from financial thresholds		These are recorded by a Directorate or Mayoral Approval Form so will be retained as per instructions under Corporate Management.		
1-PC-0005	Expressions of interest	Calls for expressions of interest; expressions of interest	Destroy 2 years after contract let or not proceeded with		
1-PC-0006	Routine instructions to contractor/ supplier where cost is incurred	Correspondence (emails, letters); records of telephone conversations	Destroy after payment is approved		On major projects, records should be retained until the final payment has been made. If the instruction varies the work to be carried out under the original tender, the record of that instruction will become a contract management

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
					document
1-PC-0007	Specification and contract development – contracts under seal	Tender specification; signed contracts; evaluation criteria; successful tender documents; quotations	Destroy 12 years after the terms of the contract have expired	Statutory (Statute of Limitations)	
1-PC-0008	Specification and contract development – ordinary contracts over £50,000	Tender specification; signed contracts; evaluation criteria; successful tender documents; quotations	Destroy 6 years after the terms of the contract have expired	Statutory (Statute of Limitations)	
1-PC-0008a	Specification and contract development – ordinary contracts under £50,000	Tender specification; signed contracts; evaluation criteria; successful tender documents; quotations	Destroy 2 years after the terms of the contract have expired	GLA Contracts Code [amended 22 October 2008]	
1-PC-0009	Tender evaluation records (contracts over £50,000)	Form listing tender prices; records of comments made on submitted tenders	Destroy 6 years after the terms of the contract have expired	Statutory (Statute of Limitations)	
1-PC-0009a	Tender evaluation records (contracts under £50,000)	Form listing tender prices; records of comments made on submitted tenders	Destroy 2 years after the terms of the contract have expired	GLA Contracts Code [amended 22 October 2008]	
1-PC-0010	Tender issuing and return	Opening notice; tender envelope	Destroy 1 year after start of contract		
1-PC-0011	Unsuccessful tender documents	Tender documents; quotations	Destroy 1 year after start of contract		Retain only one copy of each tender submission
1-PM	Project Management Activities involved in managing projects. (For IT projects see Information and Communications Technology.)				
1-PM-0001	Documents relating to projects	Project planning; Project Initiation Documents; risk register and issues log; minutes of working groups and steering	Destroy 6 years after project is terminated		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		groups; reports			
1-PM-0002	European Programmes (ERDF and ESF) management records	Operational Programmes; correspondence with DWP/ DCLG/EC, Programme Committee papers, project applications, project claims, monitoring information, publicity	Retain until 31 December 2025, unless otherwise advised	Statutory (EU Regulations)	
1-PM-0003	European Programmes (ERDF and ESF) management records	Operational Programmes; correspondence with DWP/ DCLG/EC, Programme Committee papers, project applications, project claims, monitoring information, publicity	Retain until 31 December 2014, unless otherwise advised	Statutory (EU Regulations)	
1-PR	Public Relations Management of relations with the public. Includes media relations, marketing, publications, promotion of London, public liaison activities and public consultation. (For consultation on Mayoral strategies, use Mayoral Strategies or Planning and Building Control.)				
1-PR-0001	Campaign/ marketing material	Posters; leaflets; web pages	Review for transfer to London Metropolitan Archives after 2 years		
1-PR-0002	Complaints records	Correspondence; reports	Destroy 6 years after final action	Statutory (Statute of Limitations)	
1-PR-0003	Consultation records	Planning; development; questionnaires; responses; stakeholder consultation records	Review 5 years after last entry		
1-PR-0004	Correspondence on WriteON (including Freedom of Information requests)	WriteON correspondence	Destroy 2 years after final action		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
	and responses)				
1-PR-0005	Original correspondence that has been loaded into WriteON system for correspondence handling	Paper or electronic records of correspondence that is also on WriteON system	Destroy 1 year after loading onto WriteON (in cases where the scanned letter is not clear, paper originals may be retained for longer)		
1-PR-0006	Factsheets	Factsheets not formally published	Destroy once superseded/withdrawn		
1-PR-0007	FoI and information access management information	Statistics; summaries of requests; anonymised data	Destroy 10 years after last action		
1-PR-0008	FoI Publication Scheme development		Destroy 5 years after completion of scheme/revisions		
1-PR-0009	GLA Publications	Mayoral Strategies; Information about the GLA; Consultation Drafts	Four copies from each print run should go directly to the Research Library; one copy should be sent to the British Library; and one copy should be sent to London Metropolitan Archives; for publications with an ISBN number, 6 other copies will be sent out to various copyright libraries; all others to be destroyed once reference ceases		
1-PR-0010	GLA Publications development	Correspondence; preparation; drafts	Destroy 1 year after finalisation of publication		
1-PR-0011	GLA Publications	Publications database;	Destroy when	Statutory (Data	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
	management	publications list; information about GLA publications	superseded/ remove information that is no longer relevant	Protection Act requires personal data to be deleted when no longer required)	
1-PR-0012	Media cuttings	Press cuttings; media reports	Destroy 2 years after end of year collected		
1-PR-0013	Presentations	Presentation slides; notes	Destroy 1 year after superseded or 5 years after last presentation		
1-PR-0014	Press releases		Database to be retained permanently (searchable via web)		
1-PR-0015	Speeches	Speeches made by Mayor or Deputy Mayor on GLA policy; preparatory notes; key drafts	Review for transfer to London Metropolitan Archives five years after speech made (material relating to speeches that were never made should be destroyed)		
1-PR-0016	Surveys	Survey of Londoners – unpublished survey data and analysis	Destroy 5 years after survey took place (summary of results to be treated as GLA Publication)		
1-PR-0017	Translations	Translations of GLA publications and other documents made routinely or by request	Destroy when original document is no longer available		
1-PR-0018	Petitions	Petitions sent in by the public or campaigners in support of or against Mayoral policies and/or Assembly Member	Destroy 6 years after receipt	Statutory (Statute of Limitations)	

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		campaigns			
1-PR-0019	Recordings of telephone calls from the public for monitoring purposes	Recordings of telephone calls made to the Public Liaison Unit	Destroy 3 months after the call was received	Statutory (Data Protection Act)	
1-RM	Risk Management and Insurance Activities involved in establishing, planning for and responding to risks to London and the GLA. Includes disaster recovery planning and management of insurance policies				
1-RM-0001	Claims files	Correspondence regarding claim	Destroy 7 years after claim settled	Statutory	
1-RM-0004	Fire alarm/emergency lighting inspections		Destroy all except last two certificates		
1-RM-0005	Fire risk assessment		Destroy once superseded	Statutory (Fire regulations)	
1-RM-0006	Insurance policies	Insurance policies; correspondence; insurance inspections	Destroy 6 years after terms of policy have expired	Statutory (Statute of Limitations)	
1-RM-0007	Reports on major incidents		Transfer to London Metropolitan Archives 10 years after incident took place		
1-RM-0008	Reports on minor incidents		Destroy 7 years after closure		
1-RM-0009	Risk register		Destroy when superseded		
1-RM-0010	Tests of emergency plan	Correspondence; minutes of meetings	Destroy when superseded		
1-SP	Strategic Partnerships Activities involved in forming strategic partnerships with other organisations or individuals. Includes liaison with London boroughs and partnerships with other world cities				
1-SP-0001	Appointments to other bodies	Decisions to appoint chairs of functional bodies; correspondence; briefings, etc. regarding such decisions; though	Destroy 5 years after final action		

Retention code	Records class	Examples	Retention period, trigger and action	Authority	Notes
		see Mayoral Strategies for records relating to policy development of and towards functional bodies			
1-SP-0003	Partnership and Friendship City Agreements		Retain permanently		
1-SP-0004	London Partnerships Register		Retain permanently		Previously 1-EM-0002 under version 1 of retention schedule (moved on request of FM)

Greater London Authority

Records Management Policy

March 2016

1 Purpose

The purpose of the Greater London Authority's (GLA) Records Management Policy is to establish a framework for the creation, maintenance, storage, use and disposal of GLA records, so as to support strong corporate governance processes and to facilitate the Authority's compliance with the Freedom of Information Act 2000, the Data Protection Act 1998 and other relevant pieces of legislation.

2 Scope

This policy applies to the whole Authority – the Mayor, Assembly Members and staff. It also applies to consultants engaged in GLA work. The policy covers all records created in the course of GLA business and activities. A record is recorded information in any form created or received by the GLA. It may be either in an electronic or a paper form.

3 Policy statement

The records of the GLA 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. All records created during the course of GLA work are the property of the GLA. Managing and using records effectively will ensure that the GLA gains the maximum benefit from them.

The GLA recognises the importance of this essential resource and undertakes to:

- 3.1 Manage records within a single corporate framework, according to agreed procedures
- 3.2 Comply with legal obligations that apply to its records (see appendix B)
- 3.3 Exercise best practice in the management of records, as outlined in relevant standards
- 3.4 Encourage effective access to and use of records as a corporate source of information
- 3.5 Keep records electronically where appropriate
- 3.6 Store records efficiently, utilising appropriate storage methods at all points in their lifecycle (pedestals, filing cabinets, off-site records store), and disposing of them when they are no longer required (securely destroying or preserving them as part of the GLA's historical archive)
- 3.7 Provide appropriate protection for records from unwanted environmental (fire, flood, infestation) or human (alteration, defacement, theft) impact
- 3.8 Safeguard records necessary for the continuity and regeneration of the GLA in the event of a disastrous occurrence
- 3.9 Identify and make provision for the preservation of records of historical value

4 Roles and Responsibilities

- 4.1 The Head of Governance and the Information Governance Manager are responsible for developing corporate records management policy, procedures and guidance and communicating them to staff.
- 4.2 All GLA staff are responsible for documenting their work and keeping records in line with GLA policies and procedures.
- 4.3 Facilities Management (FM) is responsible for the coordination of off-site storage for non-current records.

5 Implementation Methods

- 5.1 Off-site storage will be used for records that are no longer required on a constant basis but are not yet ready for disposal.
- 5.2 Vital records will be identified and steps taken to ensure their survival in the event of a disastrous occurrence.
- 5.3 Records of historical value will be identified as early as possible and transferred to London Metropolitan Archive when GLA use has ended. Records not required for historical purposes will be destroyed in line with the GLA's retention schedule.

6 Policy Review

The *Records Management Policy* and association documentation will be reviewed by the Governance Steering Group to ensure that it continues to fulfil the needs of the GLA.

7 Appendices

- Appendix A – Definitions
- Appendix B – GLA Retention & Disposal Schedule
- Appendix C – Historical Archiving Policy
- Appendix D – Guidance on Mayoral and Assembly Member Recordkeeping

1. Appendix A: Definitions

What is a record?

A record is recorded information, in any form, created or received by the GLA or individual members of staff to support and show evidence of GLA activities. It is important to differentiate between a record and a document. All records are documents, but not all documents are records. In effect, a document becomes a record when it forms part of a business activity.

An example of a document would be a blank form. If somebody completes and submits the form, it becomes a record, because it has participated in a business activity. Some documents will never (and should never) become records, due to their ephemeral nature. Examples include promotional literature received (unless it is relevant to a particular project or initiative ongoing or planned), junk mail (e-mail or otherwise) and other items of no more than passing significance.

Records need to be authentic, reliable, have integrity (be complete or unaltered, except under controlled conditions) and be useable. Records therefore need to be subject to controls that ensure these features are maintained.

What is records management?

The international standard on records management describes it as:

*"[The] Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and [disposal] of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records"*¹

Effectively, it is about applying the necessary controls to the GLA's records to ensure authenticity, reliability, integrity and usability.

What is a Retention and Disposal Schedule?

This is a policy statement setting out what records the GLA holds and how long they will be retained before disposal. It can also be used to set out what needs to happen to records at different stages of their lifecycle to ensure that they are stored efficiently. This guidance reflects the GLA's own corporate requirements for records keeping, and incorporates the applicable legislative and regulatory requirements for record keeping and disposal.

More information about the legislative and regulatory provisions that apply to the records held by the GLA can be found in the *GLA Retention & Disposal Schedule* at Appendix B

What are vital records?

These are records without which the GLA could not function or be reconstructed in the event of a disaster.

¹ BS ISO 15489-1: 2001 Information and documentation – Records Management

Appendix B

Greater London Authority Records Retention Schedule v2.0 March 2016

All GLA staff will dispose of records not required for a specific legal, business, operational or historical purpose in a timely and efficient manner, and in accordance with the GLA's retention schedule.

What is a retention schedule?

A retention schedule is a set of rules identifying classes of records and specifying their retention periods and what should happen to them at the end of that period. 'Records class' is the term used for a set of records consisting of individual records which are similar in nature and result from the same activity, either in a particular business unit or throughout the GLA. Aggregating these records into records classes ensures consistency and cuts down on the time and resources needed to make and apply retention and disposal decisions.

Benefits of a retention schedule

- Records of continuing value are identified and can be managed appropriately
- Records which cease to have any value to the GLA can be disposed of efficiently
- Clear instructions on what happens to records when they are no longer needed to support GLA business
- Definitive periods of time for which records should be kept and remain accessible
- Consistency in retention of records across the GLA
- Evidence of compliance with legal and regulatory requirements for the retention of records
- Evidence of what records were created but subsequently destroyed.

Retention periods and organisational value

The retention periods in this schedule have been set according to organisational value and, if applicable, the historical value of the records.

Organisational value focuses on the GLA's needs and obligations and on the records as information assets. It is about value for accountability, legal or reference purposes, and includes protection of the legal and other rights of the GLA and those with whom it deals, and compliance with whatever regulatory framework applies.

In determining organisational value, the following factors are considered:

- The importance of the function that the records support.
- The importance of the records for protecting the interests and legal rights of the organisation and those with whom it deals.
- Any legal or regulatory requirements – even if they do not actually specify the length of time records must be kept, they may include relevant things like liability thresholds.

- The requirements of any body with a right to audit the GLA.
- Any accepted standards or best practice within the public sector.
- The relationship between the records and other related records and the data or evidence they provide.

Often information-rich, cumulative or summary records will be kept in the longer term while more detailed, bulky but ephemeral records can and should be destroyed earlier.

For example, the quarterly accounting reports will be kept in the longer term while the weekly reports that contribute to them can be destroyed once the quarterly report has been compiled.

Using the retention schedule

The retention schedule has been developed to be used in the following ways:

When new records are created

The retention schedule should be used as a point of reference in the day-to-day management of records. The most effective point in the lifecycle of any record at which to decide how long it should be retained, and for what reason, is when that record is created.

When opening a new file, creating an electronic record or typing a letter, this retention schedule will act as a guide to the conditions under which that record should be managed, stored and ultimately disposed of.

When designing or implementing a new paper filing system

Any new office system intended to improve the efficiency of paper filing should be designed with a clear understanding of the legal and business requirement for record keeping, when they should eventually be destroyed and whether records should be transferred to the London Metropolitan Archives for permanent preservation.

When transferring files to off-site storage

Office space is at a premium at City Hall and it is rarely possible to retain files on-site for the length of time for which they have to be retained. The retention schedule should always be consulted when transferring files to the Crown off-site records store.

When destroying files

In order to protect itself and minimise risk, the GLA should not maintain records longer than it needs to; nor should it destroy records sooner than is required. The retention schedule provides consistent guidelines on the retention period of all of the GLA's records.

GLA Retention Periods

Subject to the specific conditions, record-classes and situations listed below, the majority of records held by the GLA should be retained, reviewed and disposed of as follows:

- **GLA 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 GLA enters the succeeding pre-election period. For example:

- the 1st April 2012 to 31st March 2016; or
- the 1st April 2016 to 31st March 2020.

Subject to the conditions, record-classes and situations below, the GLA should only retain records relating to the current Mayoral Term and the preceding Mayoral Term – i.e. a maximum of eight years.

This retention period will cover the vast majority of information created by business areas across the GLA as part of our day-to-day activities, such as work on:

- policies, proposals, strategies and projects;
- matters relating to corporate governance and management of the authority.

This retention period will not apply in the following circumstances:

- **Information subject to the GLA Historical Archiving Policy:** certain records have been identified as having significant historical value and will be transferred to the London Metropolitan Archives for permanent preservation. Please see the *Historical Archiving Policy* at Appendix C
- **Records containing personal data:** any category of information / record / document containing personal should '*..not be kept for longer than necessary*' in order to comply with the fifth data protection principle of the Data Protection Act 1998. Please refer to the *GLA Data Protection Policy* for further information.
- **Potential litigation or regulatory investigation:** the destruction of records should always be suspended if there is existing litigation or regulatory investigation or any possibility of anticipated litigation or regulatory investigation. Deliberate destruction of relevant records in such cases could involve the criminal offence of obstructing or perverting the course of justice. See also the *Limitations Act 1980 (below)*.
- **Mayoral Correspondence:** will be indexed and retained in an electronic format and archived by the GLA.
- **Exceptional Retention Periods:** The following list identifies the specific legislative and regulatory requirements which apply to certain records held by the GLA, and apply regardless of the medium of format in which the records are created or held. Information that falls within the following record-classes, conditions or situations should be kept as specified.

1. The Limitations Act 1980

1.1 Limitation Act 1980 sets time limits within which different types of legal proceedings can be commenced. Consequently, it is necessary to have minimum retention periods for some financial records, contracts, personnel records, etc. that may need to be produced in connection with legal proceedings. Recommended retention periods are set out below:

- Claims and disputes: *settlement of claim/dispute + 6 years (unless signed as a deed – see below)*
- Disciplinary hearings against staff: *settlement of case + 6 years (unless merged with staff personnel file)*
- Staff personnel files, including contracts of employment: *termination of employment + 6 years*
- Reporting and investigation of accidents/dangerous occurrences: *date of accident + 40 years*
- Negligence actions not involving personal injury: *15 years from act/omission*
- Contracts: *termination + 6 years (unless signed as a deed – see below)*
- Deeds: *settlement or termination + 12 years*
- Hiring out of conference facilities: *termination of agreement + 6 years*
- Private hire agreements: *termination of agreement + 6 years*
- Insurance policies: *termination of policy + 6 years*
- Insurance claims: *settlement of claim + 6 years*
- Conduct of testing, maintenance and statutory inspections and any necessary action: *life of plant/equipment + 6 years*
- Maintenance schedules: *creation + 2 years*
- Inspection certificates: *creation + 6 years*
- Repair reports: *life of plant/equipment + 6 years*
- Payroll payments excluding pension and superannuation records: *creation + 6 years*
- Control of disclosure of intellectual property: *disclosure + 6 years*
- Administration of intellectual property agreements: *termination of agreement + 6 years*
- Intellectual property agreements: *termination of agreement + 6 years*
- Claims of infringement of intellectual property rights: *settlement of claim + 6 years*

2. Assembly & Secretariat

2.1 Greater London Authority Act 1999: Section 58 reflects the *Local Government Act 1972* and requires that agenda papers & minutes be retained for 6 years and all background papers (associated with those agenda reports) are held for 4 years.

3. Corporate Governance & Management

3.1 Openness of Local Government Bodies Regulations 2014: S.8 specifies a requirement to create, keep and make available for inspection a record of certain kinds of decisions for 6 years after the decision was taken, as well as 4 years for background information

3.2 Internal Audit reports and audits: retain for 6 years after the publication

4. Employment and Pensions

4.1 Data Protection Act 1998: gives individuals the right to access any personal information about them that is held by organisations. The Data Protection Principles also specify mandatory record keeping standards for personal data as follows:

- data must be processed fairly and lawfully.
- data must be processed only for specified and lawful purposes.
- data must be adequate, relevant and not excessive.
- data must be accurate and, where necessary, kept up to date.
- data must not be kept longer than necessary.
- data must be processed in accordance with an individual's rights under the Act.
- data must be kept secure.
- data must be not transferred to non-EEA countries without adequate protection.

Disposal provisions for personal data as currently recommended by the National Archives to ensure compliance include:

- Personnel files:
 - o contracts and particulars of employment: until age 100*
 - o job history: until age 100
 - o current address details: termination of employment + 6 years
- Sickness record: until age 72*
- Disciplinary records which result in changes to terms and conditions of employment: until age 72
- Pensions documentation:
 - o personal payroll history: until age 100
 - o pensions estimates and awards: until age 100
- Ethnic monitoring questionnaire/reports: creation + 5 years
- Advertising of vacancies: filling of vacancy + 6 months
- Job applications:
 - o Successful (transfer to staff personnel file)
 - o Unsuccessful (filling of vacancy + 6 months)

* A destruction date of 6 years after termination of employment as per the Limitation Act is an acceptable alternative option.

4.2 Employers' Liability (Compulsory Insurance) Act 1969 and subsequent Regulations (1998) stipulate that employers' liability insurance certificates dating from 31 December 1998 must be kept for 40 years after the date on which the insurance to which the certificate relates commences or is renewed

4.3 Equality Act 2010: states that discrimination claims must be brought within 3-9 months of the alleged act (depending on the category of the claim).

4.4 Limitation Act 1980 (See above)

4.5 Pensions Act 2008: S60 stipulates that certain records relating to compliance and information sharing should be retained for a period not exceeding 6 years.

4.6 Social Security (Contributions) Regulations 2001 stipulate that records of National Insurance contributions must be kept for 3 years following the end of the tax year to which they relate.

- 4.7 Statutory Maternity Pay (General) Regulations 1986** stipulate maternity medical certificates (or a copy thereof) and a record of maternity leave and payments must be kept for 3 years following the end of tax year in which the benefit was made.

5. Finance, Contracts & Procurement

- 5.1 Companies Act 2006:** stipulates statutory minimum retention periods for: Company accounts (in the case of a private company, creation + 3 years; in the case of a public company, creation + 6 years).
- 5.2 European Social Fund (ESF); Article 60(f) Commission Regulation 1083/2006:** organisations are required to retain documents until three years after the European Commission makes the final payment for the programme for auditing purposes. Documents for the **2007-13** programme period will need to be retained until **31st December 2025** before being reviewed.
- 5.3 European Structural and Investment Funds (ESIF); Article 140(1) Commission Regulation 1303/2013:** organisations are required to retain documents until three years after the European Commission makes the final payment for the programme for auditing purposes. Documents for the **2014-20** European Social Fund (ESF) or European Regional Development Fund (ERDF) Programmes will need to be retained until **31st December 2026** before being reviewed.
- 5.4 Finance Act 1998:** companies which are required to deliver a tax return must keep relevant records for 6 years following the tax period to which the return relates.
- 5.5 Income Tax (Pay as You Earn) Regulations 2003** PAYE income tax records must be kept for three years following the end of the tax year to which they relate.
- 5.6 Limitation Act 1980** (See above)

6. Health & Safety

- 6.1 Health and Safety at Work etc Act 1974** and its associated Regulations stipulate minimum retention periods for records relating to:
- Accident books (completion of book + 3 years)
 - Accident/dangerous occurrence report forms (date of occurrence + 3 years)
 - Categorising and disposal of waste (creation + 3 years)
 - Monitoring of employees' health (creation + 40 years)
 - New buildings health and safety file (retain until asset disposed of then pass to new asset owner)
 - Record of testing of environmental controls and protective equipment (creation + 5 years)
 - Monitoring of working environments (creation + 40 years)
 - Risk assessment (review + 3-5 years)
- 6.2 Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995:** stipulates a record of deaths, injuries at work or disease shall be kept for at least 3 years from the date on which the record was made.
- 6.3 Taxes Management Act 1970:** provisions make it advisable to retain payroll (i.e. wages or salaries) records relating to a tax assessment for 6 years from the end of the year to which the assessment relates.

- 6.4 Value Added Tax Act 1994** provides a retention period of 6 years for VAT records, such as purchase orders; delivery and goods received notes; income and expenditure accounts; management of bank accounts; assessment of tax liabilities; or submission of tax returns

7. Property and Assets

- 7.1 Limitation Act 1980** (See above)

Appendix C:

Greater London Authority Historical Archiving Policy

1. Purpose

- 1.1. The purpose of the Historical Archiving Policy is to establish the GLA's approach to the archiving of records that are of historical value, including details of the selection policy, the procedure for transferring records to London Metropolitan Archives (LMA) and responsibilities of GLA staff and LMA.

2. Scope

- 2.1. This policy applies to the whole Authority – the Mayor, members of the Assembly and all staff of the Authority. It will also apply to all consultants engaged to work within the Authority.
- 2.2. The policy covers all records created in the course of GLA business and activities. A record is recorded information, in any form (it may be an electronic file or e-mail, or a paper document), created or received by the GLA to support and show evidence of GLA activities.

3. Background

- 3.1. The GLA signed an agreement with LMA in 2006 for the transfer of GLA records of historical interest to LMA on a planned basis, generally once a year. The records are transferred to LMA as a long term deposit, ownership remaining with the GLA but other rights and responsibilities, detailed in the agreement, passing to LMA.
- 3.2. LMA is the archive repository for many London-wide organisations. The archives of the City of London Corporation (COL) and the former Greater London Council (GLC), London County Council (LCC), Middlesex County Council (MCC) and their predecessors are held at LMA. They have over 100 km of shelving holding documents, plans, audio-visual and printed material about London and its people.

4. Policy statement

- 4.1. The GLA will provide a permanent historical record of the activities of the GLA by transferring records of significance to LMA on an annual basis, once those records are no longer required.
- 4.2. This will provide protection for significant material relating to the GLA that might otherwise be lost or destroyed, for the purposes of bibliographic reference and further study by historians and members of the public.

5. Selection policy

- 5.1. The types of records that have been identified as suitable for historical preservation at LMA include, but are not limited to:
 - 5.1.1. Final bound and signed copies of committee minutes
 - 5.1.2. Mayoral Decisions and associated key decision-making documents
 - 5.1.3. Items relating to major or pan-London events and incidents such as 7/7 (eg books of condolence)
 - 5.1.4. Key strategy documents relating to core GLA business and our of historical interest (e.g. The London Plan)

- 5.1.5. Publications produced by the GLA regarding major pan-London events – official reports, brochures, newsletters, leaflets, event flyers and posters, promotional items
- 5.2. Material not for consideration includes, but is not limited to:
 - 5.2.1. 'Business as usual' records (e.g. financial records)
 - 5.2.2. Working copies or 'live' documents currently in use
 - 5.2.3. Draft, unsigned or incomplete documents (unless identified as being of significant importance)
 - 5.2.4. Non-GLA records provided by other organisations

6. Roles and responsibilities

- 6.1. The Information Governance Manager is responsible for the implementation and updating of this policy.
- 6.2. GLA officers should familiarise themselves with the selection policy and the GLA Records Retention Schedule so they are aware of records suitable for historical preservation.
- 6.3. Arrangements for the annual collection of records for transfer will be made once the invoice for the previous financial year has been paid by the GLA. The Information Governance team will seek suitable contributions for transfers – via the Intranet and London@Work – at least four weeks in advance.
- 6.4. GLA officers with relevant records to be transferred will collate items into storage boxes ready for collection. Officers must complete a transmittal form (available on the Intranet) detailing the contents of the box and send a copy of the form to the Information Governance team electronically.
- 6.5. The Information Governance team will liaise with LMA on the collection of relevant material from City Hall.

7. Policy Review

- 7.1. The Historical Archiving Policy will be reviewed every two years by the Governance Steering Group to ensure that it continues to fulfil the needs of the GLA.

Greater London Authority

Guidance on Mayoral and Members' recordkeeping

This guidance note aims to define the status of records created, received and held by the Mayor and London Assembly Members, and how these records are affected by the Data Protection and Freedom of Information Acts.

All Authority records should be managed in accordance with the GLA Records Management Policy previously adopted by the Mayor, which will facilitate compliance with legislation and good practice.

Records held by the Mayor

In most cases, records of GLA business conducted by the Mayor are held within the directorates of the Authority (e.g. Mayoral Approval Forms together with any appendices, planning reports and decisions, Mayoral reports to the London Assembly, directorate files for particular projects, MMB papers). It is advisable that the Mayor should ensure that either original correspondence and other records, or suitable copies, relating directly to the Mayor's functions and actions are passed on to an appropriate GLA officer for filing.

Records or information held by the Mayor which have been collected by virtue of his office, using the resources of the Authority and relating directly to its functions and powers are the property of the Authority, and will be regulated in accordance with the Data Protection Act and subject to requests under the Freedom of Information Act.

Information held by the Mayor that has been collected by virtue of being chair of a functional body can be sought from the Authority or the functional body under data protection or freedom of information legislation.

Records held by the Mayor solely for his/her own personal purposes are his/her own responsibility; they are records which do not relate to the functions of the Authority. These records will not be subject to freedom of information legislation, as they will be considered the Mayor's own records.

If a request for information is received by the GLA which relates to the Mayor's own records, the Authority would explain to applicant how that request fell outside the GLA's data protection and freedom of information responsibilities. It would then be up to the Mayor to decide how best to respond.

Records held by Assembly Members

A central record of GLA business enacted by Assembly Members is held by the Secretariat (e.g. minutes of committee meetings, scrutiny reports). Members have a responsibility to support the maintenance of this central record by ensuring that any relevant correspondence and other records relating directly to the Authority's functions and powers passed to them by virtue of their role on any committee or other group, and not already held by Secretariat, are passed on to the committee administrator or equivalent for filing.

Records or information held by an Assembly Member that have been collected by virtue of membership of the Authority, using the resources of the Authority and relating directly to its functions and powers, such as committee reports, are the property of the Authority, will be regulated in accordance with the Data Protection Act and subject to requests under the Freedom of Information Act.

Similarly, information held by an Assembly Member that has been collected by virtue of a position on a Functional Body, to which the Member has been appointed as an Assembly Member, and which relates to the functions and powers of the Functional Body can be sought from the Authority or the Functional Body under the Freedom of Information Act. A failure to produce it on request may give rise to a criminal offence.

All Assembly Members' records concerning constituency business are their own responsibility, as they are records associated with the Member's role as an elected representative rather than as a member of the Authority. These records will not be subject to a request under the Freedom of Information legislation, as they will be considered the Member's own records (i.e. they are hosted by the GLA on behalf of the Member and not 'held' for the purposes of FoIA). They will however remain subject to data protection legislation.

The Authority will register all Assembly Members with the Information Commissioner as data controllers with regard to their administration of constituency business (separate guidance is available).

Assembly Members and party groups may also hold records relating to party group discussions. Records relating solely to party group discussions may not be subject to freedom of information legislation, as they will not be considered to be records held for GLA purposes. However, as with constituency records, these records are subject to data protection legislation.

Also, where any such records do relate to information held by an Assembly Member that has been collected by virtue of membership of the Authority and relating directly to its functions and powers, those records would become subject to the Freedom of Information Act.

If a request for information is received by the GLA which is considered to relate to an Assembly Member's own records or records of party group discussions, the Authority would explain to applicant how that request fell outside the GLA's data protection and freedom of information responsibilities. It would then be up to the Assembly Member or party group concerned to decide how best to respond.

Elections and termination of office

Prior to a Mayoral election or each London Assembly election, the Mayor and/or Assembly Members should review their records. In particular, they should identify any records relating to ongoing projects or correspondence and take action in accordance with the separate guidance available.

The Greater London Authority will not accept responsibility for information retained or processed by a former Mayor or Member after a Data Protection notification has lapsed, or for records left in its buildings or archives without authority.

It is left to a former Mayor's discretion to decide what should happen to their own personal records after he or she has left office, but this could include offering them to a record office of their choice to facilitate future historical research.

Deputy Mayor

When the statutory Deputy Mayor is carrying out Mayoral business, this protocol will apply to information in his or her possession. When they are acting as an Assembly Member, the protocol on Assembly Members' recordkeeping will apply.