GLA Records Management and Life Cycle Policy

1. Introduction

The Greater London Authority (GLA) is committed to the efficient management of its records for the effective delivery of its services, to document its core activities and to maintain the corporate memory.

A good record-management process is beneficial to the effective running of the GLA's business because it:

- helps the GLA to conduct its business in an efficient, effective, and accountable manner

- supports information access by ensuring that the GLA can find information about its past activities; enabling access to records required for inquiries, investigation, and information requests; and identifying what is relevant, thereby supporting effective decision-making

- enables the effective use of the GLA's resources, so that it is easy to know where data is held, who to ask (especially when staff have left), and how to search for and retrieve relevant information when required

- ensures that data is kept for as long as required, and is properly disposed of at the end of its retention period

- helps the GLA meet its statutory and regulatory obligations, and adhere to best practices relating to different record types

- provides effective handling of both digital and physical records, including adhering to relevant policies in place.

Similarly, a poor record-management process can have a detrimental effect on the organisation including reputational damage; unnecessary expenses for records storage; security breaches; non-compliance with legislation; penalties in terms of fines; risk of litigation; and bad management decisions.

This document sets out the GLA's policy on the storage, access, retention and disposal of information and records. It highlights the life cycle of a record from creation or when it was received, to its disposal or destruction.

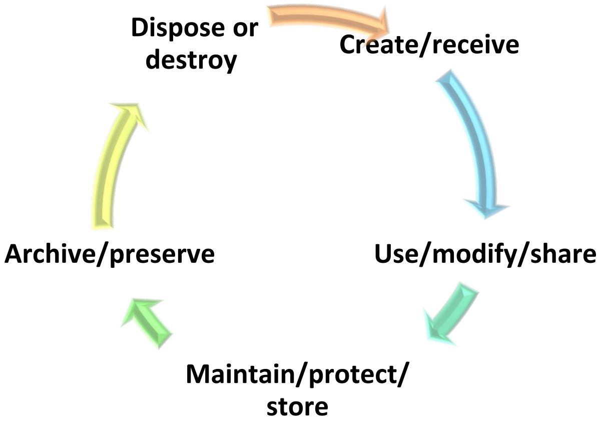
Note that records can be in electronic, digital, or hard-copy format.

The policy applies to all information and records (regardless of format) held by or transferred to the GLA, for example, following the procurement of a service.

This policy has been approved by the Governance Steering Group (GSG) and complies with legal and regulatory requirements. It is in line with the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000 (FOIA).

All staff are responsible for record management. They should familiarise themselves with the records management policy and retention schedule and adhere to it when creating and maintaining records as part of their work for the GLA.

Figure 1: Record life cycle



1.1. Definitions

The following terms are used in this policy:

- **Digital -** Information and records that exist in a digital or electronic media, for example, computer files, emails, or database contents. It includes both 'born digital' documents (those originally created in digital formats) and digital versions of physical documents, for example, scanned documents.

- **Disposal -** Any action taken, or yet to be taken, to determine the fate of records, including destruction or transfer to a permanent archive.

- **Information -** All records (plus ephemeral content) created, received, or held as part of the GLA's work, regardless of whether it is designated as a record.

- **Record -** Information created, received, and maintained as evidence, and as information, by an organisation or person in pursuance of legal obligations or in the transaction of business (this definition follows ISO standard ISO 15489-1). A record is further defined by the International Council on Archives as:

  > 'Recorded information produced or received in the initiation, conduct, completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity.'

- **Physical -** Any information or records written or recorded on a tangible physical format, including (but not limited to) paper, magnetic tapes, microfiche, CDs and DVDs.

- **Retention -** Usually, the length of time for which records are to be kept. It normally represents, and will also be expressed as, a disposal period.

- **Review -** The process by which a record that has not yet been assigned a disposal action will be considered at a specific point in the future, to determine its final disposal.

- **Site –** A Microsoft (MS) SharePoint or Teams site set up for the storage and sharing of digital data and collaborative working.

- **Information asset -** A body of information, defined and managed as a single unit so it can be understood, shared, protected, and exploited effectively. Information assets have recognisable and manageable value, risk, content, and life cycles.

- **Information asset owner -** Senior members of staff who have the responsibility for one or more identified information asset(s). This person will be responsible for ensuring that the information asset is accurately stored and maintained on the information asset register.

- **Information asset administrator (IAA) –** A member of staff who sees to the update of the information asset register and manages these assets day-to-day. IAAs can be team leads, or staff within their respective teams who have firm knowledge and understanding of their team's information assets and location.

- **Information asset register -** A formal documentation of all the GLA's information assets, which is maintained by the Information Governance (IG) team, with the security risks therein assessed, at least quarterly. The IG Manager will update the Corporate Management team (CMT) on progress made with the register twice a year.

- **Record Of Processing Activities (ROPA) -** Accompanies the GLA's Information Asset Register. This is a legal requirement to document the GLA's Personal information processing activities. Taking stock of what information you have, where it is and what you do with it makes it much easier for the GLA to improve information governance and comply with other aspects of data protection law (such as creating a privacy notice and keeping personal data secure).

1.2. Scope

This policy applies to the entire GLA's staff including the Mayor, Deputy Mayors, and Assembly Members. It also applies to consultants engaged in GLA work. The policy covers all records created in conducting GLA business and activities. This is explained in more detail at section 2, below.

1.3. Related policies

This policy should be read together with the IG policy, and other related GLA policies. These are accessible on the intranet and, where appropriate, published externally. These policies, and their purposes, are as follows:

- **Record retention schedule -** How long different types of information should be held. This is not exhaustive but acts as a guide. The retention schedule will also be the GLA's deletion, disposal and secure destruction policy, which details: the processes for the destruction and deletion of information; and when deleted information is held for statutory purposes. The deletion of emails is overseen by Transport for London (TfL) IT in accordance with the shared-services agreement approved by the GLA's GSG.

- **Cybersecurity policy -** Information assurance roles and responsibilities, and breach processes.

- **Data protection policy -** Best practice in place for managing GLA records containing person-identifiable data.

- **Information asset register guidance -** The structure, contents, and management of the information asset register.

- **Code of ethics and standards for staff -** The standards of conduct that the GLA expects staff to achieve.

1.4. Relevant legislation and standards

The GLA will comply with legal and regulatory requirements, including the following:

- The Greater London Authority Act 1999

- The Limitations Act 1980

- The FOIA

- The FOIA, section 46: Code of Practice

- The Data Protection Act 2018 (DPA), including the England and Wales General Data Protection Regulation (GDPR)

- Managing digital records without an electronic records management system

- All other regulatory and professional guidance, and codes of practice, applicable to the records that the GLA holds.

The GLA also adheres to the guidance within the records management standards as the International Organisation for Standardization outlines in ISO 15489 and ISO 15489 Part 2.

2. Roles and responsibilities

All permanent and temporary employees, contractors, consultants, and seconded staff who have access to the GLA's records or are working on behalf of the GLA and its business, are responsible for managing the GLA's records, wherever these records are held and in whatever form they are.

The GLA owns all records created by employees carrying out its business-related activities. Except where the originator asserts ownership, records received by the GLA's employees are also owned by the GLA. Individual employees do not own records; however, they are responsible for managing them.

2.1. Executive Board

Members of the CMT have overall responsibility for the GLA's records and information management policy and standards, and for supporting their application throughout the organisation.

Significant changes to records and information management policy and standards, requiring corporate sign-off, will be presented to the GSG, chaired by the Executive Director, Resources, for approval.

2.2. The Information Governance (IG) team

The IG team, part of the Resources Directorate, will be responsible for:

- making sure records and information management policies are kept up to date and relevant to the needs and obligations of the GLA; and consulting and working with GLA staff, as well as the appropriate external regulatory bodies

- informing staff about records and information management policy, and ensuring that all staff are aware of their responsibilities for managing records and information

- undertaking audits of record of processing activities and the information asset register

- providing information-management advice and guidance to all staff as required, taking over management of the GLA's records and information for which there is no clear responsible business area

- working closely with Facilities Management (FM) in making sure the GLA's hard-copy records and information are physically well preserved, stored and accessed securely, on-site, and off-site.

2.3. Facilities Management (FM)

FM team, part of the Resources Directorate, is responsible for the coordination of off-site storage for non-current records, including tracking the movement of held records, thereby ensuring effective record-search capability is maintained. They will oversee storage processes, including payment of invoices due.

2.4. Line managers

Managers at all levels are responsible for working with the Information Governance team to develop suitable information management procedures, covering both digital and hard-copy records, that:

- are efficient and fit for purpose

- comply with internal policies and standards

- ensure appropriate resources exist within the manager's business unit to fulfil the responsibilities for managing records

- enable the communication of local information and record management procedures to staff

- ensure that local records are in line with this and all other central policies

- ensure that staff follow procedures for the off-site storage of hard-copy records

- ensure that staff follow the internal procedure for the management and storage of hard-copy and digital records, including managing the leavers process, by:

    - promptly completing the starters, movers, and leavers (SML) process, which includes departing Mayors, Deputy Mayors and Assembly members; staff with oversight of this area must start the SML process before the leaver's final departure date (contact the IG team for further guidance)

    - ensuring that: there is an outline of the steps taken to file, destroy or transfer records for which the leaver has been responsible; and relevant information is retained, and remains accessible, by completing the checklist within the SML process for record management

    - assisting the IG team in the creation and maintenance of retention schedules.

2.4.1. Starters, movers, and leavers (SML) process

- As mentioned in paragraph 2.4, above, when a staff member starts with a team or leaves (either to move within the GLA or externally on secondment or to leave entirely), the responsibility for starting the leavers process lies with the staff member's line manager, or the staff member with responsibility for that business area.

- The line manager must ensure that the SML process is started before the leaver's last day, to enable TfL IT or FM to confirm that all permissions have been updated accordingly. The line manager must therefore complete the checklist within the SML process, ensuring all required actions are taken regarding the mover's or leaver's records, email storage and owned sites. This will include taking steps to ensure that all GLA business-related information or records for which the individual was responsible – held in email accounts or personal drives – are either filed in, or transferred to, a shared area or deleted as necessary.

- Any restricted folder for which the individual has responsibility, or is the owner, must be transferred to another staff member with permission sought from TfL IT. This includes MS Teams channels and SharePoint sites.

- When a member of staff leaves temporarily and does not require access in the interim, their permissions will be revoked and, on their return, reinstated.

- When a member of staff leaves the GLA, their MS Office 365 licence will be revoked immediately; they will no longer have access to their OneDrive, Outlook account or any other information based within MS Office 365. The account will then be closed, and retention policies applied. Access to the account whilst it is still held will be handled in line with section 3 below. The leaver's staff pass must also be handed into security, and then appropriately destroyed.

- If the member of staff has any corporate information saved on their OneDrive, or in their email account, they must transfer this to the corporate storage before they leave. If they wish to retain any personal information held in the account, it is their responsibility to ensure it is extracted prior to departure. The retention of any data left in the account is not guaranteed, and any requests for personal data to be extracted from a former staff member's account will need to be submitted to the IG team as a subject access request.

2.5. Project managers

Project records are the responsibility of the project manager, who is responsible for:

- identifying project-related records and liaising with relevant local contacts

- ensuring that the records are managed efficiently, and comply with our record retention and management policy and standards

- ensuring that there are appropriate resources within the project for fulfilling the responsibilities for managing records

- quality assurance of records and information management processes and procedures within the project

- ensuring the appropriate disposition of project records where necessary.

2.6. Site owners

Site owners are administrators of specific MS Teams and SharePoint sites. They are responsible for:

- managing MS Teams sites; adding and removing members when needed; and ensuring there are always at least two individual owners of a site

- approving requests from non-members of a site to access information, considering the need and appropriateness of the sharing

- ensuring records are appropriately transferred to a corporate shared drive when necessary

- arranging for sites to be archived in line with information management processes.

Private channels should not be created in Teams sites, as this creates a separate, hidden SharePoint library of which administrator accounts are not members.

2.7. GLA Code of Ethics and Standards

All GLA staff are required to comply with their employment contract and abide by the Code of Ethics for standards. Records management is everyone’s responsibility.

2.8. Stakeholder engagement

When working with external bodies, consideration must be given to who is keeping the official record. In general, GLA staff should keep a copy of all records when working with:

- government bodies and agencies
- non-government bodies, such as charity organisations, commercial groups, campaign groups and lobbyists (please note this list is non-exhaustive) if involved in GLA business activities
- local authorities.

3. Storage (of digital records)

3.1. Approved corporate storage

The GLA is moving to a digital storage programme. Information is digital by default, with physical records only being created when there is a specific, legitimate need. All business units’ records must be stored on the GLA’s devices in storage locations, as outlined within this policy.

Storage location means:

- the GLA’s Share and Teams sites
- directorate and team drive archive storage
- registered paper files, where there is a legitimate business need for physical registration; these are managed by FM and, where not immediately required, stored off-site with DeepStore, the records storage company. They are covered under section 4, below.

Information that does not form part of the record or has no legislative requirement to be kept, and is not of ongoing business value, should be deleted as soon as it is no longer required.

Information such as chats on MS Teams are retained for 30 days and thereafter deleted. Where chats are official records (for example, part of an audit trail), they must be converted to a record and saved appropriately.

GLA email communications are kept for eight years and then deleted.

3.2. Shared mailboxes in Outlook

Shared mailboxes, including group mailboxes linked to Teams sites, may be used for the storage of business information. However, if this is the case, the owning team should appoint an information manager responsible for ensuring that, the information stored in the account is appropriately managed for it to be retrievable, if needed, retention or disposal is suitably applied. The IG team should be contacted for advice on the management or disposal of such information.

With the GLA's Technology Group imminent move to a shared service with TfL, all email correspondence will be retained for eight years and then deleted. It is very important, therefore, that business information is moved to corporate storage drives as soon as possible.

3.3. Personal storage

GLA information can be stored in account-specific storage, that is individual Outlook accounts and OneDrive, however, it is advised that these are reviewed periodically. Records should be transferred to a corporate storage drive (shared drives, for example, H: Drive) as soon as possible for proper management, access, and oversight by the service area.

All information in account-specific storage remains searchable by and accessible to the IG officer. The process for searches is carried out by the IG team and, where necessary, with IT. The IG team will exercise discretion with searches; where it is essentially important to search the email archives, such as for information to support an investigation, approval will be required from the Executive Director or Assistant Director of that area to progress the search.

3.4. OneDrive

OneDrive is an account-specific storage provided as part of MS Office 365. Although each OneDrive is linked to a named user, they remain held by the GLA, and the contents are subject to the same statutory requirements as other parts of the GLA's information, including freedom of information and data protection legislation.

All information stored on OneDrive is potentially accessible to the IG officer, the data protection officer and the IT provider, where there is a legitimate need to access it.

OneDrive should be used for storing business-related personal documents, for example, HR and performance-related documents. Documents of business value (including drafts) must be saved to a corporate storage location, to ensure that business continuity can be maintained.

OneDrive should **not** be used for storing data that an individual's team may need to access, including draft documents. This data should be saved to the appropriate site so that others in the team can access it and, if necessary, continue work; and any OneDrive copies should be deleted to prevent duplication of information.

Line managers must comply with the GLA’s privacy notice for staff. It is the account owner’s responsibility to manage their own personal data, including appropriately deleting copies of data from their OneDrive, prior to leaving the department.

3.5. GLA-issued devices

Devices issued to users (MS Surface Pro, laptops, and phones) come with a small amount of local storage. This should only be used for temporary storage of information when no other storage location is available. Where it is necessary to save to the device, for example in the case of some downloaded data, it must be transferred to corporate storage as soon as possible; the copy saved on the device should be deleted to avoid duplication.

Any apps installed on the device that are used to store information outside the main network (for example, WhatsApp) should not be used to store GLA information. Device storage is unmanaged; is not backed up; and is inaccessible for business continuity purposes but remains potentially disclosable under freedom of information and data protection legislation. Individuals may be required to search data stored on their devices, as set out in the data subject rights procedure.

Personal devices should not be used to store GLA information. However, as with devices issued by the GLA, any GLA information that is stored in these locations remains potentially disclosable under freedom of information and data protection legislation, regardless of the device’s ownership.

Deliberate destruction of relevant records in this case, where information in scope has been requested, could involve the criminal offence of obstructing or perverting the course of justice. See the Limitations Act 1980; also, section 77 of the FOIA.

3.6. Individual mailboxes in Outlook

Individual official mailboxes on Outlook are not currently recognised as part of the official GLA record-keeping system. It is the responsibility of staff to ensure that any emails relating to business activity are saved in approved corporate storage locations, and then deleted from the mailbox.

It is the responsibility of the individual holding the account (or in their absence, their line manager) to ensure that all business-related emails within the mailbox are transferred to an appropriate site **before** the individual leaves the GLA.

Auto-forward of emails from a mailbox account to an external account is not permitted.

Outlook should be used for short-term storage of communications and ephemeral information. Records of business decisions stored in emails should be transferred to a corporate storage location as soon as practically possible.

3.7. Personal digital files

The IG team recommends that files that are purely personal should not be stored anywhere on the GLA's information systems. This includes (but is not limited to) personal photos and other media files; personal documents unrelated to work; and documents relating to any external business commitments individuals may have.

Any personal documents stored temporarily on the GLA's IT systems must be reviewed regularly by the owner and deleted. Work-related personal documents (for example, Performance Management Reviews) should be saved to account-specific storage (OneDrive).

Any purely personal files identified on the network may be deleted on sight. Whilst stored on the network they may be identified as part of routine searches for freedom of information requests; inquiries; and any other legitimate search activity.

3.8. PST files

Personal Storage Table (pst.) files are archived emails, a feature in MS Outlook. These are not an approved form of information management and must not be created or used. They are not supported by TfL IT; any pst. files discovered on the GLA's IT systems may be subject to deletion.

3.9. Instant messaging

Instant messages fall into two types, both of which are covered by the FOIA and may be considered for disclosure:

- **Chat** messages are private instant messages between two or more individuals for example, Skype. They are retained for 30 days. Any chat messages that need to be retained as part of an official record must be copied into another format or taken as a screenshot and saved (for example, as a jpg, or pasted onto a Word file saved to the site).

- **Posts** are messages that can be seen within an MS Teams site by any members of that site. Posts on MS Teams are currently kept for 30 days, in line with TfL's retention period. Posts will be treated as part of the entire team's record.

3.10. Other MS apps

If other MS apps are used to record information that is required for business purposes, or that needs to form part of the corporate record, the information must be transferred to SharePoint or Group drives for storage. They should not be kept in personal storage locations.

4 Storage (of physical records)

4.1. Physical storage

All registered paper files should be stored off-site with the GLA's appointed off-site records storage contractor. This process is overseen and managed by FM.

Appropriate measures will be taken to protect files according to their sensitivity. Only registered paper files, or registered boxes containing paper material, will be accepted for storage without separate agreement from staff. If business areas have requirements for storing information on other physical media (for example, magnetic tapes), they should first speak to TfL IT.

4.2. Paper files

The FM team is responsible for maintaining the GLA's record catalogue of registered paper files. All paper records are identified for either destruction or disposal, for review of their potential historical value according to their retention period, as set out in the record retention schedule.

Paper records that become due for destruction (which depends on their retention category) are destroyed by either:

- the GLA's off-site file storage provider on receipt of a destruction request from the FM team

- the FM team on-site.

A record destruction register, detailing deletion date and records reference, should be kept by the FM team for future reference and as proof of destruction due to the retention schedule.

Paper records identified as potentially being of historical value are reviewed by the IG team to decide if they are, indeed, of historical value. If they are of value, the records are transferred to the London Metropolitan Archives. If not, they are destroyed. Deletion or destruction of records must be permanent.

Personnel records are to be kept in line with the applicable legislation and the applicable retention period. Different retention periods may apply to staff contracted on a fixed-term contract.

4.3. Hard-copy papers

The GLA aims to retain digital copies of documents, rather than paper ones. Unless there is a legal requirement to keep paper copies, such documents should be scanned and saved to shared drives or SharePoint as digital files. Scanned documents should be saved with a meaningful name and, where possible, should include optical character recognition (OCR) of any text.

There is no requirement to keep printouts of papers, printed for the GLA's business, where these are identical to the digital copies. However, if any additional manuscript notes or markings have been added to the paper, and if these are required for the corporate record or for business purposes, these printouts should be scanned and saved to the relevant shared drive alongside the original document. Scans should be saved with a meaningful name and, where possible, should include an OCR of any text.

4.4. Notebooks

Notebooks kept during GLA business should normally be handled as personal papers if; they are used solely for personal notes; and they do not contain business information that is unrecorded elsewhere. The only exception to this is if the notebook's contents relate to a current or expected inquiry, criminal investigation, or information access request.

4.5. Personal papers

Individuals are responsible for managing their own personal work papers and ensuring that they are held in storage with appropriate security and destroyed when no longer needed. Any allocated personal storage, for example, teams' drawers or lockers, should not be used for the storage of registered files.

4.6. Non-paper items and digital continuity

Physical items other than paper should not be put into off-site storage without first consulting the FM team.

Physical media for storing digital data (for example CDs, DVDs) changes over time, and can become obsolete and inaccessible. These media will not be accepted as part of a registered file, unless TfL IT can guarantee continued access to the data. Where it is necessary to include physical media with a deposited document (see paragraph 4.1), the business unit will be required to formally agree to accept responsibility for ensuring that the media can continue to be read as storage formats change and become outdated.

Retention periods for non-paper physical items will be agreed with business units in the same way as paper files.

5. Use of informal communication styles

5.1. GLA Style Guide

GLA staff should, when creating official records, adhere to the GLA's Style Guide, available on the intranet; official records must not include use of informal communication styles such as emojis or GIFs.

5.2. Protective markings

The GLA does not currently have a protective marking scheme in place for its business records. For records with such marking, which have been received from external stakeholders, GLA employees should comply with the Government Protective Marking System for Protectively Marked Information, as set out in the HMG Security Policy Framework, where applicable, when storing such information.

Official records must only be shared where appropriate, and in line with the applicable legislation. For instance, personal information must always be shared confidentially and on a legitimate, need-to-know basis only, in line with data protection law.

6. Social media and external platforms

6.1. GLA-approved platforms

An approved platform is a social media or other web-based platform that has been designed for either the GLA or one of its functional bodies; and has been through the TfL IT and cyber-approvals process. It includes both systems with a software-download component, and services that are entirely web-based through corporate account usage.

Every social media platform owned by the GLA is managed by the Digital Communications team, with a system owner appointed who will have responsibility for ensuring the information is appropriately managed; access controls are in place; and searches are conducted as necessary for freedom of information and other requests. The system or parts of its contents may need to be recorded on the information asset register.

The IG team does not recommend that WhatsApp be used for the GLA's business. Where WhatsApp is required and there is a real business need for it, this should be approved ahead of planned use by TfL IT on a GLA-issued mobile phone or tablet. Users must be mindful of their responsibilities to keep accurate records and ensure any decisions or important business conversations made over WhatsApp are subsequently recorded in a format that can be saved to corporate shared drive or systems.

Personal phones and WhatsApp should not be used for making GLA business decisions. Similarly personal conversations should not be carried out using GLA email. These records will be subject to requests for information if they are in scope.

6.2. Social media and external platforms – unapproved platforms

The GLA does not recognise nor support social media (for example, Twitter) or external web-based platforms (for example, Trello, Google Drive, Google Docs, Dropbox, Slack, We-Transfer, Zoom) as record-keeping systems. Personal accounts with social media and web-based platforms must never be used for the GLA's business.

As far as possible, the features of MS Office 365 should be used to replace these services, particularly for internal business activities. Work conducted on external applications is covered by the FOIA and the DPA and may be subject to disclosure.

Where there is a need to conduct business on an external platform, the staff using it are responsible for ensuring that personal and sensitive data is adequately protected and handled in line with any relevant legislation.

Staff must ensure that a copy or screenshot of any information that needs to be kept as a record is saved to a corporate shared drive – either on an ongoing basis, or at the end of a project. Staff are also responsible for ensuring that information is deleted regularly from these platforms where possible and appropriate. Where automated retention is in place, particularly where the retention period is not based solely on date (for example, items are deleted once the maximum data allowance is reached), staff are required to regularly extract anything that needs to be kept as a record to ensure it is not deleted.

7. Retention and disposal

7.1. Records retention and disposal schedule

The retention schedule, and this policy, set out what records the GLA holds and how long they will be retained before disposal or archival. These documents should also be used in setting out what needs to happen to official records at different stages of their life cycle, to ensure that they are stored efficiently.

The schedule reflects the GLA's own corporate requirements for good record-keeping and incorporates the applicable legislative and regulatory requirements for keeping, and disposing of, records. More information about the legislative and regulatory provisions that apply to the records held by the GLA can be found within the GLA records retention and disposal schedule at Appendix B.

7.2. Business continuity plans

Business continuity plans, also known as vital records, pertain to those records without which the GLA could not function properly, and could not be reconstructed in the event of a disaster – natural or man-made.

Vital records will be identified, and steps taken to ensure their survival in the event of a disastrous occurrence.

7.3. GLA retention and disposal schedule

The GLA does not keep most information indefinitely. Records will be kept for as long as there is a business or legislative need to do so. Durations will vary according to the type of information and may be up to 20 years for some records. In a limited number of circumstances, records may need to be held for longer, including for the lifetime of an asset. Legal authority is required for the GLA to hold records for longer than 20 years. In these cases, the GLA will apply for a retention instrument from the appropriate authority, providing justification of the need to retain such information. For example, pension records are kept for 72 years in line with the Limitation Act 1980.

The metadata within the record retention and disposal schedule shows the general retention periods used by the GLA based on detailed record-management standards.

Each business area is responsible for agreeing, in consultation with the IG team, the retention period of all its records.

In circumstances where individual business areas are unsure of the retention period of a record, or there is no clear owner to advise, or there is no valid legal obligation, the default will be taken to be eight years.

7.4. Record destruction and disposal

The processes for the destruction and disposal of paper and digital records are set out in the record retention and disposal schedule.

7.5. Deletion of digital records

Where held digitally, records are to be deleted by the information asset owner in accordance with disposal agreements reached with business units. Where no agreement exists, digital records will be considered for deletion once they reach eight years of age.

Information asset owners will regularly identify digital records for review once they have reached the end of their retention period. These records will first be reviewed by the information asset owner, prior to deletion, to see if they are of historical value. Any records that are deemed to be of historic value, and selected for retention, will be transferred to London Metropolitan Archives or other appropriate place of deposit for all other records; all that are not will be permanently deleted.

7.6. Retention and deletion of legacy data held outside Office 365

Legacy information stored in systems or platforms other than the main GLA network will be assessed to evaluate what information needs to be retained; and will have its life cycle managed by the information asset owner, according to this policy and the technical constraints of the systems they are stored on.

7.7. Records of the Mayor of London, Deputy Mayors and Assembly Members

Records from the Mayor’s office, and the offices of the Deputy Mayors and Assembly Members (including senior advisers’ records), must be managed in line with the guidance provided specifically for the relevant team on the GLA’s intranet. This page will continuously be updated with relevant information to ensure clarity. There will be times when the records produced by any of these parties are either GLA records or the party’s own records. A clear distinction should be made between these two groups of records.

All mayoral correspondence will be indexed and retained in an electronic format and archived by the GLA.

GLA records should be retained for the duration of the Mayoral term in which they were created (the current Mayoral term) and the subsequent Mayoral term. For the purposes of this guidance, a Mayoral term lasts from 1 April directly before a Mayoral election, until 31 March before the GLA enters the succeeding pre-election period. To illustrate this, recent Mayoral terms include 1 April 2012 to 31 March 2016, and 1 April 2016 to 31 March 2020.

See the retention schedule for detailed information on the retention and disposal period of such records.

8. Access and sharing

8.1. Internal sharing and access controls in Teams sites

Sites set up in MS Teams sites (commonly referred to as SharePoint) enable staff to share information and conversations within a set group of people. Each team's group includes a shared email address and mailbox that can be accessed by all members of the team.

Staff should save all their work, including drafts, to shared areas where colleagues can access it if there is a need to do so. For more on this, see section 3.

Access restrictions should be managed using the permissions features built into MS Office 365. Where there is a need to restrict access to a set of data to a limited group of people, a new site may be set up, giving only those individuals access. This simplifies the management of individual permissions within sites.

Passwords must not be used to protect documents, as these are unique to the creator and do not allow for business continuity or for the department to meet statutory requirements such as the FOIA.

Staff can share sites, folders and individual documents with other members of the GLA. It is the responsibility of the site owner to manage and, where appropriate, remove access permissions.

Staff are responsible for regularly reviewing which documents have been shared and removing permissions where there is no longer a requirement for their access to continue. This includes, but is not limited to, when a project closes or when staff move post.

8.2. Internal sharing and access controls in OneDrive and Outlook

Access to OneDrive and Outlook must normally be approved by the individual owning the account; or, if they have left, by TfL IT, who will seek approval from the data protection officer as necessary.

Where the individual is unable to give permission (for example, due to absence or departure from the GLA) access will need to be approved by the data protection officer. This access can be requested by emailing **data.protection@london.gov.uk**. Requests will be reviewed on a case-by-case basis.

Where possible, direct access by staff to OneDrive will be minimised. Requests for documents stored in OneDrive will normally be processed by the IG team, rather than individuals being granted access to the relevant account. Individual files may be transferred via email; otherwise, a suitable Teams location will need to be provided for the files to be copied to.
Where access is approved to OneDrive or a calendar, this will be for a time-limited period – typically 48 hours, unless there is a business need for access to be permitted for longer.

8.3. External sharing via SharePoint and Teams

Information should only be shared externally where there is a clear business need to do so, and where the contents and nature of the information make it appropriate to be shared. Consideration should always be given to privacy and security, and sharing must consider the implications of the information being made available outside of the GLA.

Information should only be shared externally where it is appropriate to do so, and through permitted means. Photos or screenshots of the GLA's information must not be shared externally except with the approval of TfL IT. Where there is a genuine need for regular sharing of information, an agreement or information-sharing protocol should be considered (see section 8.5, below).

8.4. External sharing via email

Care must be taken whilst sharing GLA information externally via email, as there is a risk posed by human error. Where smaller quantities of information are being shared, it should be considered whether the 'encrypt' and 'do not forward' settings are appropriate means of protecting the contents.

Outlook calendars may be opened externally to allow people outside the GLA to see when an individual is free or busy, but not the contents of that appointment. This feature must be used appropriately, and permissions must be removed when the access is no longer needed by the external person.

8.5. Sharing agreements

When information is being shared on a regular basis, a sharing agreement is required that sets out key information about the sharing, this is not mandatory but is considered best practice. This is particularly important for external sharing but may also be required for internal sharing of sensitive data. If the data being shared is personal data, the agreement should be made on the data-sharing template available from the IG team.

If the data does not include personal data, a sharing agreement may still be required.

9. Policy review

9.1. Updates to the policy

In line with section 2.1, above, this policy, together with the retention and disposal schedule and their appendices, will be reviewed every two years by the IG team. Where significant changes are made, the GSG will need to approve these changes to ensure that the documents continue to fulfil the GLA’s needs.

The policy has been written in line with the Code of Practice on the management of records issued under section 46 of the FOIA, as updated and presented to Parliament in July 2021. The code applies to all public authorities. This policy therefore adheres to the principles approach of value, integrity, accountability, as set out in the code for managing business records.

The Information Commissioner has a statutory duty to promote good practice and compliance with the code. The Commissioner may consider compliance with the code before issuing a ‘practice recommendation’ under section 48 of the FOIA to the public authority whose record-management practice does not comply with the code.