MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

POLICY AIM

The purpose of this policy is to ensure that all staff at the Mayor's Office for Policing and Crime (MOPAC) handle, keep, secure, store, protect, retain, review and delete information correctly, to minimise any risk of misuse, loss or damage, in line with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

INFORMATION GOVERNANCE POLICY

Introduction

To ensure compliance staff should abide by the following policies in this document:

- Handle and use – using the Government Security Classifications
- Keep and secure – using MOPAC's Information Security Policy
- Store – using MOPAC's Record's Management Policy
- Protect – using the Data Protection Policy
- Retain, review and delete – using MOPAC's Retention, Review and Disposal Policy

This policy applies to all new information created, modified or accessed from 28 March 2018.

Scope

All MOPAC staff are responsible for implementing information governance good practice on a day to day basis through compliance with the policies.

Senior management will oversee and monitor information governance issues as part of the Governance and Risk Working Group (GRWG) which meets every month.

Our Senior Information Risk Owner is the Director of Strategy.

The Data Protection Officer (Head of Strategy and Corporate Planning) will manage and report on compliance with the GDPR and information governance to the GRWG. They will also review MOPAC's policies and procedures in relation to GDPR and information governance, ensuring all staff receive annual training so they understand their roles and responsibilities.

1. MOPAC'S INFORMATION SECURITY POLICY

Aim

MOPAC recognises the importance of information and will take all necessary measures to ensure that it is secure from loss, unauthorised or unlawful processing, damage or destruction. In doing this, MOPAC will consider using ISO 27001 or equivalent (the International Standard on Information Security) as a benchmark against which to measure its progress.

Specifically, MOPAC is committed to:

- producing and communicating guidance and procedure documents covering all relevant areas of information security and ensuring that these procedures are complied with
- implementing systems, both manual and electronic, to ensure that information is kept as securely as possible
- an annual training programme for staff

Roles and Responsibilities

All MOPAC staff are responsible for implementing information governance good practice on a day to day basis through compliance with the policies.

Senior management will oversee and monitor information governance issues as part of the Governance and Risk Working Group (GRWG) which meets every month.

Our Senior Information Risk Owner is the Director of Strategy.

The Data Protection Officer will manage and report on compliance with the GDPR and information governance to the GRWG. They will also review MOPAC's policies and procedures in relation to GDPR and information governance, ensuring all staff understand their roles and responsibilities.

Each team that the GRWG identifies as having a lead role or responsibility for information security, will be required to review its relevant policies, procedures and working methods and report to the GRWG. For example:

TG

The IT infrastructure (including remote working infrastructure) will be reviewed on a regular basis to ensure that it is as secure as practicable as part of our existing contract with the Technology Group (TG).

Specification, procurement and authorisation for new information systems will include security considerations.

Information held in electronic format will be backed up securely so that it can be restored as necessary.

All emails automatically have MOPAC disclaimers added when sent.

Personal data will be processed lawfully and in line with the rights of data subjects; such data (and in particular sensitive data) will be protected from unauthorised access.

MOPAC's senior responsible officer for IT from the Technology Group will report to GRWG on information security every six months, starting in May 2018, reporting on compliance.

HR

Staff will be informed of their responsibilities for the security of MOPAC's information by relevant changes to terms and conditions, policies and procedures and training.

Information held on staff will be reviewed to ensure GDPR compliance.

Staff and others will be informed of any changes to procedures that may impact on them.

All staff must attend mandatory GDPR training so they understand their responsibilities to deliver GDPR compliance.

2. MOPAC'S RECORDS MANAGEMENT POLICY

Aim

The aim of this Records Management Policy is to aid staff in ensuring our records:

- provide authoritative information about past actions and decisions for current business purposes
- protect the legal and other rights of MOPAC
- explain, and if necessary, justify, past actions in the event of an audit, public inquiry or other investigations for example, expenditure of public funds, handling of an FOI request etc.
- provide the right to erasure

Naming conventions and filing structure

Records Creation

A document name or title is often the first point of identification, so it is crucial that the name sufficiently distinguishes it from other documents. Adopting a basic naming convention will enable consistency in naming documents and assist in navigation and searching. It also allows a shared understanding of the context of a document's content. For example:

Name_Day-Month-Year_Version would be

Police and Crime Plan_01-01-2018_v1

Version Control

The use of version control can greatly assist with retrieving records quickly and accurately. It allows users to track a document's progress during drafting and/or review and revert to previous versions if needed.

Emails

Emails are considered information under the terms of this policy and some emails will also be a business record. Emails which form a business record that need to be accessed and shared with other staff members should be saved in the relevant folder on the shared drive. This will ensure that they form a complete record with other associated documentation.

It is important that only essential business emails are saved to the shared drive. Documents which may be attached to an email and need to be saved as a corporate record, must be saved to the shared drive and not simply retained on an email or saved to personal drives. This will ensure business continuity and that they are available to all staff that need access to them.

Retention, review and disposal

Records that are no longer required will be disposed of in accordance with the MOPAC's Retention and Disposal Policy (at the end of this document).

3. MOPAC'S DATA PROTECTION POLICY

Aim

The Data Protection Act 2018 and General Data Protection Regulation (GDPR) cover the processing of information relating to individuals, this includes the obtaining, holding, using or disclosing of information, and covers electronic records as well as paper.

Data protection is the responsibility of all of us because we all handle personal data in the work we do. We have a legal responsibility to handle information in accordance with the law and the data protection principles. This policy will support staff to meet their obligations for the effective handling of information.

Summary

We must comply with the data protection principles. They say:

- personally identifiable data will be processed lawfully, fairly and transparently. This means you must:
    - identify valid grounds under the GDPR (known as a 'lawful basis') for collecting and using personal data
    - ensure that you do not do anything with the data in breach of any other laws
    - use personal data in a way that is fair. This means you must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned
    - be clear, open and honest with people from the start about how you will use their personal data

- personally identifiable data will be collected for specific, explicit and legitimate purposes. This means you must:
    - be clear about what your purposes for processing are from the start
    - record your purposes as part of your documentation obligations and specify them in your privacy information for individuals
    - only use the personal data for a new purpose if this is compatible with your original purpose, you get consent, or you have a clear basis in law

- to take a data minimisation approach, ensuring the data you are processing is:
    - adequate – sufficient to properly fulfil your stated purpose
    - relevant – has a rational link to that purpose
    - limited to what is necessary – you do not hold more than you need for that purpose

- personally identifiable data will be kept accurately and up to date. This means you must:
    - take all reasonable steps to ensure the personal data you hold is not incorrect or misleading as to any matter of fact
    - keep the personal data updated, although this will depend on what you are using it for

    - take reasonable steps to correct or erase personal data that is incorrect or misleading
    - carefully consider any challenges to the accuracy of personal data

- to ensure storage limitation. This means you must:
    - not keep personal data for longer than you need it
    - think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data
    - have a policy setting standard retention periods wherever possible, to comply with documentation requirements
    - periodically review the data you hold, and erase or anonymise it when you no longer need it
    - carefully consider any challenges to your retention of data. Individuals have a right to erasure if you no longer need the data
    - only keep data for longer if you are keeping it for public interest archiving, scientific or historical research, or statistical purposes

- to process personally identifiable data in a way that ensures appropriate integrity and confidentiality (security). This means you must:
    - ensure appropriate security measures are in place to protect personal data
    - when sharing personally identifiable data over email always ensure it is password protected and the password is sent separately to the data

- you and MOPAC are accountable and must take responsibility for what you do with personal data and how you comply with the other principles. This means you must:
    - have appropriate measures and records in place to be able to demonstrate compliance

All staff are required to abide by these principles at all times. Data Protection Impact Assessments are used at MOPAC to assess and understand risks around personal data. These should be completed as part of project initiation. More information can be found on the Information Commissioner's website or please refer to the Data Protection Officer and see the template in Share Point under 'Work' and 'GDPR'.

Maintaining our information

Every team at MOPAC is required, by law, to maintain a record of data processing activity that:

- is likely to result in a risk to the rights and freedoms of data subjects
- is not occasional
- includes special categories of data
- includes personal data relating to criminal convictions and offences

Staff must notify the Data Protection Officer of any filing system or computer database that contains (or will contain) the data listed above. This will then be added to the Information Asset Register (IAR). If you are uncertain what personal data is please check with the Data Protection Officer or GDPR Project Manager.

Please see the retention review and disposal at the end of this document for retention periods for all information.

MOPAC's Data Protection Officer will:

- inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- be the first point of contact for supervisory authorities and for individuals whose data are processed (employees, customers etc)

It is the responsibility of the Head of Service that all computer and manual systems within their respective service areas that contain personally identifiable information must be identified, the personally identifiable information listed in the Information Asset Register and the Data Protection Officer informed for notification purposes.

Any breach, or suspected breach, of the Data Protection Policy must be referred to the Data Protection Officer immediately. Deliberate or negligent breaches may lead to disciplinary action being taken or even a criminal prosecution.

4. MOPAC's RETENTION, REVIEW AND DISPOSAL POLICY

Purpose

The Mayor's Office for Policing and Crime (MOPAC) will ensure that information is not kept for longer than is necessary and will retain the minimum amount of information required to carry out our statutory functions.

Specifically, in line with the GDPR, MOPAC will ensure that personally identifiable information will not be kept any longer than is necessary and is saved and destroyed securely in line with this policy.

Records held by the Metropolitan Police Service (MPS) will be covered by the MPS's own policies and procedures.

Aim

Information is a vital asset. We depend on reliable, up-to-date information to support the work we do. These policy and retention standards will help MOPAC to:

- ensure the retention and availability of the appropriate level of information for MOPAC to operate efficiently and effectively
- comply with legal and regulatory requirements, including the Data Protection Act 1998, Data Protection Act 2018, Freedom of Information Act 2000 and the General Data Protection Regulation (GDPR)
- increase employees' efficiency when retrieving information by reducing the amount of information that is held unnecessarily
- minimise the administrative overhead to MOPAC and save money in terms of storage costs
- preserve corporate memory and ensure business continuity

Record Retention

Retention periods are given in whole years and are from the end of the financial year to which the records relate. Records should be disposed of by arranging for collection of confidential waste for destruction or shredding, including all copies in whatever formats.

Information needs to be managed for continuity reasons as this will increase operational efficiency through the streamlining of documents. MOPAC's intranet and document storage will be used to improve responsiveness in MOPAC by enabling staff to access accurate, up-to-date information and provide a "single version of the truth".

Aside from the standard procedure, set out below, whenever there is a possibility of litigation or a request under the Freedom of Information Act, the records that are likely to be affected should not be amended or disposed of until the threat of litigation has ended or the appeal processes under the Freedom of Information Act have been exhausted. In these circumstances the Chief Executive Officer who is the Monitoring Officer should be consulted.

Standard Procedure

Information which is duplicated, unimportant or of short term use can be destroyed under this standard procedure, including:

- catalogues and trade journals
- telephone message slips
- messages or notes not related to MOPAC business
- requests for standard information provided by MOPAC
- out of date distribution lists
- working papers which lead to a final report
- duplicated and superseded material such as stationery, manuals, drafts, address books and reference copies of annual reports
- e-copies of documents where a hard copy has been printed and filed
- emails that do not form a business record
- electronic drafts and copies of correspondence

Records which do not need to be retained should be disposed of in line with this policy.

The schedule below sets out the retention periods for particular records, which should be retained for the periods shown.

This policy applies to documents held in either hard copy and/or electronic format (including scanned documents).

Retention & Disposal Schedule Function	Example of Records	Retention action
MOPAC Business, Management and Administration		
Unstructured Records (emails)	Emails that do not support a business process or decision i.e. there is no existing place for them in the filing structure and none will be created. This applies to paper and electronic formats including emails.	Destroy as soon as use has ceased
Meetings (where the MOPAC owns the record – includes formal, partners and external meetings)	Minutes, agendas and reports Appendices General correspondence Hand written notes from Meetings	Permanent Permanent 8 years after date of meeting or last action (*if applicable*) Destroy on completion of agreed documentation
External meetings (where the MOPAC does not own the record)	Minutes, agendas and reports	8 years after last action
Working Groups/Steering Groups	Minutes, agendas and reports	8 years after last action
DMPC Decisions	Decision Records	Permanent
Assurance – process of assessing quality, efficiency or performance of the Met	Minutes, agendas, reports, supporting documentation, dip sampling records, Oversight Board etc.	8 years after last action
Complaints Professional standards	Correspondence, Enquiries Summary reports Details of investigations Police Appeal	8 years after last action 8 years from date of leaving or retirement 8 years after last action – if advice sets major precedent, consider transferring to archives
Independent Custody Visiting	Minutes, agendas, reports, registers of visits, custody visitor details, expense claims	8 years after last action

	Independent Custody Visitor details Handbook	8 years after end of appointment Until superseded (retain old versions for 8 years)
Corporate Planning and Reporting	Police and Crime Plan, Directorate Plans, Annual Report	Permanent
External audit reports and Reviews	External Audit reports, HMIC reports Correspondence	Permanent 8 years after last action
Governance	Corporate Governance Framework, standing orders/financial regulations	Until superseded (retain old versions for 8 years)
Ethical Framework	Code of conduct Register of staff interests, Gifts and hospitality register	8 years after period of appointment ends 8 years
Allowances/Expenses	Claim forms, letters	3 years after period of appointment ends
Policy Development	Policies, procedures, joint protocols	Until superseded (retain old versions for 8 years)
Public Consultation	Consultation documents including records, questionnaires, correspondence, supporting papers	8 years after close of consultation
Research, analysis and evaluation	Longitudinal analysis and trend data	Exemptions apply for longer retention periods. These must be documented

Information Management	Filing indices, records of transfer to archives, disposal records Routine correspondence with ICO	Permanent 8 years after last action
Media Relations	Media reports, press releases	8 years
Marketing	Developing and promoting MOPAC events Information about the MOPAC	8 years Until superseded
Office management	Contracts with suppliers	8 years from end of contract
Diaries and calendars	Electronic and manual diaries/calendars	3 years
Health and Safety	Policies Training documentation, Risk assessments and accident books	Once superseded 8 years after being superseded
Freedom of Information Act requests	Requests and responses received	8 years after last action
Unstructured Records	Emails that do not support a business process or decision i.e. there is no existing place for them in the filing structure and none will be created. This applies to paper and electronic formats including emails.	Destroy as soon as use has ceased
LEGAL		

Litigation	Correspondence, criminal and civil case files, medical appeal files, employment tribunal files	7 years after last action
Legal Advice	Briefing notes, correspondence, Counsel's opinion	8 years after last action
Agreements and agreements under seal	SLAs	8 years after agreement expires
Contract (ordinary)	Tender specification	8 years after term has expired
Contract (under seal)	Tender specification	12 years after term has expired
Tenders	Tender envelopes	1 year after start of contract
Evaluation of tenders (ordinary)	Evaluation criteria, successful tender document	8 years after terms have expired
Evaluation of tenders (where contract made is under seal)	Evaluation criteria, successful tender Document	12 years after terms have expired
Post tender negotiation	Minutes, correspondence	1 year after terms of contract have expired

Asset acquisition/disposal (non-land)	Legal documents relating to purchase/sale, leases, tender documents	Destroy after 8 years if under £50,000 Destroy after 12 years if over £50,000
Property disposal	Survey reports, tender documents, conditions of contracts	Destroy 15 years after all obligations end
Insurance	Insurance policies, correspondence	Destroy 7 years after term expire
HR		
Personnel administration	Employee file – Health and Sickness (including sickness absence records; records of major injuries at work, records of reasonable adjustments made) Employee records - (including contracts, probation records, appraisals, references and disciplinary records, including warnings and grievance records)	Age 72 or 12 years after individual dies After 10 years of leaving the employment of MOPAC or retirement
Staff recruitment	Advertisements, applications forms, interview notes, references	Unsuccessful - 6 months Successful - 8 years after end of employment or retirement
Employee relations	Agreements, correspondence re formal negotiations Correspondence re minor and routine matters	Permanent 8 years
Appointment of Non-Executive Advisers, Panel Independent Members (Audit Committee, Ethics Panel)	Personnel files	8 years after appointment ends

Medical records	Medical examinations, adjustment to work examinations	Age 72 or 12 years after individual dies
Staff leave monitoring	Leave records, flexi sheets and or Jury service	8 years
Staff termination	Resignation, redundancy, dismissal, death or retirement	8 years after termination or, if pension paid 8 years after last pension payment
FINANCE		
Annual reports	Annual statements of accounts	Permanent
Internal inspections	Internal audit reports	8 years after last action
Finance reports	Quarterly budget reports, working papers	Destroy when admin use complete
Approvals/purchase year	Purchase/sales orders	Destroy 7 years after end of financial
Expenditure	Invoices, receipts, bank statements, vouchers, ledger	Destroy 8 years after end of financial year
Payroll	Claim forms, pay/tax records	Destroy 7 years after the end of financial year
Budget setting	Final annual budget Draft budgets and estimates	Permanent Destroy 2 years after budget set
Budget monitoring	Quarterly statements	Destroy after next year's annual budget

Asset monitoring and maintenance	Asset registers Inventories	Destroy 7 years after end of financial year Destroy 2 years after admin use.
Taxation records	Taxation records	8 years after end of financial year

5. COMPLIANCE AND REVIEW

Compliance with the policies and review of the content will be monitored annually through the GDPR compliance monitoring.

Policy Review Log

Updated by	Signed off by	Date	Next review
[redacted]	Governance and Risk Working Group	28 March 2018	March 2020