

## Records Management Policy

### Policy Statement

Information and data are central to the work of the Mayor's Office for Policing And Crime (MOPAC). The effective management of our records is essential, enabling us to work with transparency to give Londoners confidence in our work, comply with legal and regulatory obligations, preserve corporate memory and manage our operations successfully. Our Records Management Policy – publicly available on our website [www.london.gov.uk/MOPAC](http://www.london.gov.uk/MOPAC) – sets out how we manage the information we create, receive and share as we carry out our work.

### Introduction

It is recognised that information is a vital asset of MOPAC, which depends on reliable, up-to-date information systems to support the work that it does and the services provided to Londoners.

A copy of this policy will be published on the website so that the public can see the basis on which we manage our records.

Documents can be held in either hard copy or in electronic format (including scanned documents).

Compliance will be monitored periodically by the Company Secretary and the policy will be reviewed every 3 years.

### Aims and Objectives

The aim of this Records Management Policy is to ensure that 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

### Relevant legislation:

- Data Protection Bill 2017
- Freedom of Information Act 2000
- Data Protection Act 1998
- Environmental Information Regulations 1992 and Environment Information (Amendment) Regulations 1998.
- Local Government Act 1972
- Public Records Act 1958 and 1967

### **Record Keeping**

It is imperative that staff creating or filing records are aware of the need to give those records titles that reflect their specific nature and contents so as to facilitate retrieval. Where possible, records will be held electronically.

Short lived material should be disposed of regularly, therefore, print outs of electronic documents should not be kept after the meeting for which they were printed, trivial emails should be deleted after being read and keeping multiple or personal copies of documents is not encouraged.

Information needs to be managed for continuity reasons as this will increase operational efficiency through the streamlining of documents. MOPAC's intranet and document management system (Sharepoint) 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".

Corporate and Business digital documents will be retained on Sharepoint which will be maintained by the relevant officer/s in MOPAC to ensure that it is in-line with the Retention and Disposal Schedule below.

### **Roles and Responsibilities**

All staff have a responsibility to ensure that information is appropriately managed. In addition, the roles and or teams listed below have specific tasks.

**Senior Leadership Team** – overall responsibility for the Information Management Policy and for supporting its application throughout the organisation.

**Company Secretary** – responsible for ensuring policies, procedures and guidelines for good information management practice are in place, and for promoting compliance with this policy. The management of information is carried out in accordance with this policy and associated procedures.

**External Relations Officer** - maintaining folder classification schemes and file plans.

**External Relations Team** – supporting the development and delivery of external and internal modes of communication including the maintenance of Sharepoint. Manage MOPAC intranet communications (Sharepoint) ensuring that it becomes a medium of choice for MOPAC staff.

**All staff** - responsible for following policies and procedures for managing information. All staff also have a responsibility to protect sensitive and personal information. It must not be disclosed to unauthorised parties or allow it to be transmitted or transported in an unsecure way.

## Naming Conventions

### 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.

### Version Control

The use of version control can greatly assist with retrieving records quickly and accurately. It allows users' track a document's progress during drafting and/or review and revert to previous versions if needed. Version control can be achieved by adding version numbering and date in the title of a record.

### 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 (S) drive or on Sharepoint. 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 (S) 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

Records that are no longer required will be disposed of in accordance with the MOPAC's Retention and Disposal Policy.