MOPAC | MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

INFORMATION SECURITY POLICY

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).

Introduction

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

To ensure compliance staff should abide by the following policies:

- Government Security Classifications provides guidance on document handling and use. Please not information above Official **SHOULD NOT** be stored on MOPAC systems.
- Data Protection Policy provides guidance of MOPACs general responsibilities and approach to data management, individual data subjects rights and storage and sharing of data (S:\GDPR\02 Policies and Procedures).
- DPIA Policy provides guidance on how and when MOPAC produces DPIAs in support of its work (S:\GDPR\02 Policies and Procedures).
- Retention, Review and Disposal Policy provides guidance on when to review and dispose of different types of information (S:\GDPR\02 Policies and Procedures)
- Cyber security framework is the GLA cyber security policy under which MOPAC IT is provided (S:\GDPR\02 Policies and Procedures) .
- Digital Security Policy outlines MOPACs specific approach to digital security, including password and pin code configurations, encryption and remote access (S:\GDPR\02 Policies and Procedures).
- Acceptable usage policy outlines expectations in terms of use of mobile technology (S:\GDPR\02 Policies and Procedures).

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.

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.

Policy Review Log

Version	Date	Author	Description of change
0.1	28 March 2018	[redacted]	
0.2	20 February 2020	James Bottomley DPO	Added reference to wider policy documents.