Museum of London Data Protection Policy

1. Introduction

This document sets out the Museum of London's policy regarding the handling of personal data, as defined by the Data Protection Act 2018 and with reference to the EU General Data Protection Regulation (GDPR). It specifies the framework which the Museum uses to manage compliance with the requirements of the law. It outlines the steps that are taken to ensure this compliance and identifies the responsibilities of staff at the various levels of the organisation.

2. Scope

This policy applies to all personal data held by the Museum, whether in manual or electronic systems, which provides access to information relating to a specific individual. This includes information in the form of CCTV footage.

The policy applies to all Museum sites and staff.

3. Purpose

- To ensure the security and proper handling of personal data as defined by the law
- To uphold the rights of data subjects
- To ensure the application of the Data Protection Principles (see Appendix 1)
- To ensure all staff are aware of the Museum's obligations under the law and their role in compliance
- To define what personal data the Museum holds and how this will be safeguarded

4. Definition of Terms

4.1 *Data Controller* – A person or named organisation, who determines the purpose for which and the manner in which any personal data are, or will be, processed. The Museum of London is the Data Controller for data we collect.

4.2 *Data Subject* – an individual about whom personal data is held.

4.3 *Personal Data* – Information from which a living person can be identified.

4.4 *Special category data* – Data relating to a person's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

5. Responsibilities

5.1 *Directorate*

The Director will appoint a Data Protection Officer to oversee compliance with the Act.

5.2 *Data Protection Officer*

The Director of Assets is the Data Protection Officer for the Museum and is responsible for overseeing compliance with the law by the following measures:

a) Informing and advising senior management and all employees about the obligations to comply with the GDPR and other data protection laws
b) Monitoring compliance with the GDPR and other data protection laws, and with this data protection policy, including managing internal data protection activities, raising awareness of data protection issues, training staff and conducting internal audits
c) Advising on, and monitoring, data protection impact assessments
d) Cooperating with the supervisory authority
e) Being the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc)
f) Investigating any apparent breach of data security and informing the Executive Board

5.3 Records Manager

The Records Manager is responsible for the practical implementation of the above compliance measures with the exception of (f), which is the sole responsibility of the Data Protection Officer.

5.4 Managers

Individual managers are responsible for ensuring that their staff comply with this policy and the related procedures. If local procedures are required, managers are to draw up and issue written procedures in consultation with the Data Protection Officer. Managers are also responsible for notifying the Data Protection Officer of any new personal data they (or their staff) intend to collect if it is different from the purposes listed in Appendix 2.

5.4 Employees

Compliance with the Act is a requirement for all employees, and all staff must ensure that they read and then follow the Museum policy (this document) and the procedures and guidelines. Addtionally, all staff are responsible for ensuring that any personal information they hold about other people is kept securely and is not disclosed in any form to any unauthorised third party.

5.5 Human Resources

Human Resources, in conjunction with IRS, will ensure that Data Protection training is included as part of induction for new staff and that ongoing training is also available.

6. Policy

6.1 The Museum will comply with the data protection principles as set out in the Act.

6.2 The Museum will monitor compliance with Data Protection law by reviewing this policy every three years, and auditing the purposes for which it collects and processes data annually.

6.3 The Museum observes the rights of data subjects to have access to their personal data held and processed by the Museum (subject to the qualifications provided for in the law).

6.4 The Museum will ensure all such data is accurate and not processed unnecessarily.

6.5 Requests for personal data as defined by the Act will receive a response within one month of receipt. The Museum reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive. Charges will be based on the real administrative cost of providing the information.

6.6 The Museum will investigate any identified breach of data security and take appropriate action. (See the Museums Information Security Policy for further information).

6.7 The Museum will take appropriate steps to protect personal data from loss and unauthorised access and will review arrangements regularly.

6.8 Data will be collected and processed only for specified purposes and will only be viewed by those who need to see it.

6.9 Where someone is required to provide personal information to the Museum they will be informed of the reason(s) for its collection, and given the opportunity to agree to its use for other purposes, such as news of future events arranged by the Museum.

6.10 Where members of staff need to share personal data with third parties (either individuals or vendors/organisations) this must be approved by the Records Manager before the data is shared. See Appendix 3 for further guidance.

7. Guidance on supporting procedures, related policies and the regulatory environment

7.1 This policy is related to the *Freedom of Information Policy*, *Records Management and Museum Business Archive Policy and Information Security Policy.*

8. Queries

8.1 If you have any questions about this policy, please contact the Records Manager.

Date approved	June 2018
Approved by	Director of Assets and Assistant Director of Content
Version	3
Master file location	G:\Collections and Learning\IRS\DPA_FOI\Policy and Procedure\Current\DP\DataProtectionPolicyV3.docx
Supersedes	2.2
Related procedures	Freedom of Information Enquiries Procedure, Data Protection Enquiries Procedure
Related policies	Freedom of Information Policy, Information Security Policy
Related Guidance, Legislation and Codes of Practice	Data Protection Act Guidance for Staff; Data Protection Act 2018
Policy Owner	Information Resources
Lead Contact	Records Manager
Policy review date	June 2021

Appendix 1: Principles

The data protection principles set out by the law require that data be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and, where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Appendix 2: Purposes

The Museum holds personal information in central and local computer systems and manual systems. The Museum has identified the 'purposes' (reasons why) for which it holds personal data, the sources of this data and the use made of the data.

The purposes are:

- Accounts and records
- Administration of membership records
- Advertising, marketing and public relations
- Advertising, marketing and public relations for others
- Consultancy and advisory services
- Crime prevention and prosecution of offenders
- Education
- Fundraising
- Information and databank administration
- Journalism and media
- Pensions administration
- Processing for not for profit organisations
- Records selected as archives, for historic and other research
- Research
- Staff administration and recruitment.

Appendix 3: Data sharing with third parties

Under data protection law, where a *data controller* (in this case, MOL) shares collected personal data with a third party that processes personal data on its behalf (such as database systems developers or mailing services), this third party

organisation is known as the *data processor*. The law draws a distinction between one data controller sharing personal data with another, and a data controller sharing data with its data processor. The law requires that a data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller; and,
- it has security in place that is equivalent to that imposed on the data controller by the data protection principles.

Therefore, a *data processor* involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller (MOL), which has ultimate responsibility for the way the data is transferred, held and used. Third party data sharing is often done in accordance with the "legitimate interests" condition of the law. This condition provides us with the grounds to process personal data in a situation whereby we need to do so for the purpose of our own legitimate interests or the legitimate interests of the third party that the information is disclosed to.

In order to justify this, the law requires that we document all decisions to share data with third parties. Please use the ICO template form below to request permission from IRS to share data. IRS will then keep a record of the permissions granted, along with the requests.

Data sharing request form

Name of organisation:	[third party organisation]
Name and position of persons requesting data:	[Contact name and post]
Data requested:	[description and volume]
Reference to data sharing agreement:	[type of agreement]
Purpose:	[give reason for need to share data]
Date required by:	
Specific arrangements re: retention/deletion of data:	IRS to fill in once agreed with all parties
Date of request:	

Signed:	