POLICY

Data Protection Policy

1. Introduction and scope

1.1 IWM may collect and hold personal data about its staff, visitors, customers, supporters, business partners and other individuals who visit, work with or contact the organisation. It is committed to ensuring that this personal information is managed responsibly and in accordance with Data Protection legislation and any associated Codes of Practice.

1.2 This policy covers all personal information held by IWM, the IWM Trading Company and other bodies that are wholly owned by IWM. Personal information includes information contained in IWM's own business records and that held in its deposited collections.

1.3 All Museum staff, volunteers and contractors are required to ensure that they comply fully with this policy and its associated procedures.

1.4 This policy is linked closely to the Museum's Information Security Policy. A full list of associated policies can be found in the Appendices.

2. The legal framework and definitions

2.1 The UK General Data Protection Regulation and Data Protection Act 2018 (known in this policy as 'Data Protection legislation') provide a framework for the handling of personal data, defined as data relating to an identifiable living individual. Special category data consists of information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and health, sexual life or orientation. It also covers genetic and biometric data. This category attracts additional protection under the Regulation. Information relating to an individual's criminal record or criminal proceedings taken against them are covered by the Data Protection Act 2018 and have a similar level of protection as special category data.

2.2 Data Protection legislation applies to all personally identifiable information held in manual files, information systems, images, microfilm and all other media. All personal data, in whatever format, must be handled in accordance with its requirements.

2.3 Data protection legislation establishes a number of rights for individuals who are the subjects of such personal data ('data subjects') and outlines a number of rights and obligations relating to the collection, storage, use, deletion and other processing of personal data.
It provides six principles, which IWM must comply with. In addition, it sets out the rights of data subjects, including the right to access their data, to request its deletion or correction and to halt the processing of their data where appropriate. It also includes rules for the export of personal data beyond the boundaries of the UK. These requirements are summarised in Appendix B.

2.4 This policy also covers the requirements of legislation directly linked to the General Data Protection Regulation and Data Protection Act, in particular the Privacy and Electronic Communications Regulations 2003 and 2011 which now form part of UK law.

2.5 Definitions of specific terms used in this Policy can be found in Appendix A, information on how this Policy meets the Data Protection Principles can be found in Appendix B and information on associated legislation and IWM policies can be found in Appendix C.

3. The Role of the Data Protection Officer

3.1 As a public authority, IWM will appoint a Data Protection Officer, who will take responsibility for all matters relating to data protection. The Data Protection Officer for IWM is the Executive Director, Collections and Governance, as outlined in Section 4.

3.2 IWM will ensure that the Data Protection Officer is:

- Knowledgeable in Data Protection and associated legislation
- Able to give independent, uninfluenced advice and report directly to the Executive Leadership Team and Board of Trustees
- Free from responsibilities or obligations that may conflict with their role as Data Protection Officer
- Able to act as the first point of contact for internal and external enquiries relating to Data Protection

4. Responsibilities

4.1 The Board of Trustees has overall responsibility for IWM's compliance with the Act. This is exercised through the governance structure as outlined in the following:

4.2 The Information Governance Board is responsible for general oversight of Data Protection within IWM and reports to the Senior Management and Executive Leadership Teams. The Data Protection Officer, Governance Department members and Chief Information Officer are members of the Board and report to it on all issues relating to Data Protection and Information Security.

4.3 The Museum's Executive Director, Collections and Governance, is the Data Protection Officer and Senior Information Risk Owner (SIRO) for the Museum, with responsibility for:

- Briefing the Board of Trustees, Executive Leadership Team and Museum Governance Boards on Data Protection responsibilities
- Establishing and reviewing Data Protection policy and procedures
- Advising and training staff in Data Protection
- Acting as the first point of contact for data subjects with enquiries about IWM's management of their personal data
- Approving requests for the processing of personal data (including collection and the implementation of new personal data management systems)
- All correspondence with the Information Commissioner's Office (ICO) on Data Protection matters, including ensuring IWM's registration with the ICO is up to date
- Co-ordinating the Museum's Data Protection and Information Security measures

4.4 The Governance Department (part of the Strategy and Governance Assistant Directorate) is responsible for day-to-day Data Protection issues and reports to the Data Protection Officer.

4.5 The technical security of personal data is the responsibility of the Chief Information Officer who may, with the agreement of the Data Protection Officer, introduce technical security requirements as and when necessary.

4.6 Executive Directors, Assistant Directors and Heads of Department are responsible for the quality, security and management of personal information held by their particular areas. They are responsible for ensuring that this policy is communicated and implemented within their area of responsibility.

4.7 Every information system containing large amounts of personal data must have an Information Asset Owner, at Head of Department level or above, responsible for the information held in that particular system.

4.8 All staff, volunteers, or contractors working with the Museum must follow this policy and any associated procedures when handing personal data.

5. Collecting personal data

5.1 The collection of new categories of personal data must be approved (via a Data Protection Assessment) by the Head of Department concerned and the Data Protection Officer. Projects relating to new technologies, surveillance or monitoring, the processing of special category data on a large scale or otherwise deemed to be high risk, must have a full Privacy Impact assessment carried out before the project can go ahead.

5.2 When requesting personal data, IWM will ensure that the data collected is the minimum required for the purpose.

5.3 When personal information is collected about data subjects, a clear explanation must be provided about how the data will be used. This may be verbally, via a sign (usually in the case of CCTV) or via a statement on a form. The explanation must outline who will use the data and what it will be used for, unless this is already perfectly clear elsewhere. All forms, signs and statements must be approved by the Data Protection Officer before being printed or published on the IWM website.

5.4 All personal data collected by IWM, or by other organisations on the museum's behalf, must be collected in accordance with the IWM Privacy Policy. A link to the Privacy Policy must be available on all webpages where personal data is collected. For personal data collected in other formats the Privacy Policy must be supplied in the most appropriate way.

5.5 IWM will provide new members of staff with details of how their personal data will be obtained, processed, disclosed and retained.

5.6 Personal data must always be collected securely. In particular, web pages collecting personal data will always be encrypted.

6. Using and managing data within IWM

6.1 The Data Protection Officer is responsible for ensuring the Museum's Privacy Policy is kept up to date

6.2 All departments holding significant collections of personal data must register them with the Data Protection Officer as an Information Asset.

6.3 Access to personal data, including personnel files, marketing databases, CCTV and Collections acquisition information within IWM will be on a need to know basis and limited to specifically authorised personnel only.

6.4 Personal data will be kept accurate, up to date and not be held for longer than is necessary, unless it is required for archiving purposes. Every collection of personal data must have a retention period. The IWM retention schedule provides further details of how long certain categories of record should be kept.

6.5 IWM will only use personal data for the purpose for which it was collected unless the reuse is permitted by Data Protection legislation (for example to meet a legal requirement, if the consent of the data subject is obtained or if it is required for archiving purposes). A legal basis for the use of the data, as outlined in Article 6 of the General Data Protection Regulation, must be agreed before personal data can be collected or reused. Special Category Data must have a legal basis in Article 6 and Article 9 of the Regulation and criminal offence data must have a legal basis in Article 6 of the Regulation and Schedule 1 of the Data Protection Act 2018.
All proposals to use or reuse personal data must be approved by the Data Protection Officer.

6.6 Section 7 of the Data Protection Act 2018 allows IWM to use Legitimate Interests as a legal basis for processing, as long as that processing is outside of its public function. Appendix D gives a statement of IWM's public function. Personal data processed for purposes not covered by this statement can be processed using Legitimate Interests as a legal basis, as long as a Legitimate Interests Assessment is carried out and approved by the Data Protection Officer.

7. Direct Marketing and sharing data with third parties

7.1 IWM will not use personal data it has collected from individuals for direct marketing purposes unless they have provided positive consent for its use in this way. Business customers may be contacted for direct marketing purposes without consent, as long as a valid Legitimate Interests Assessment is in place, and they have the opportunity to opt out at the time their data is collected. All data subjects will be removed immediately from mailing lists on receipt of a written or verbal request.

7.2 Personal data will not be sold to any outside organisation for use in direct marketing campaigns. Data may be exchanged with similar organisations for use in direct marketing only where the positive consent of the data subject and the permission of the Data Protection Officer have been obtained first.

7.3 Personal information must not be released externally without the permission of a Head of Department. In the case of Special Category personal data, transfers of large amounts of personal data or official requests from other organisations, the approval of the Data Protection Officer must be obtained. All requests for personal data must be in writing, notified to the Governance team at foi@iwm.org.uk and a record kept of the release.

7.4 IWM does share personal information with third parties when legally required to do so, or when it is otherwise permitted by Data Protection legislation, subject to the controls outlined in Section 7.3

7.5 From time to time, IWM may act as a joint data controller for personal data collected in partnership with allied organisations for a common purpose. In these cases, the collection, use and management of the data will be subject to a data sharing agreement, signed by a senior manager and approved by the Data Protection Officer.

8. The rights of data subjects

8.1 Data subjects have the right to know what personal data the IWM holds about them. IWM will make available the following information when requested, subject to verification of the enquirer's identity:

- Whether IWM holds any personal data relating to the enquirer and what it is
- Why it is held and for what purpose
- How long it will be held for
- Who it may be disclosed to
- The logic involved in any automated personal data processing
- Their rights concerning that data

All requests must be forwarded to the Data Protection Officer via the foi@iwm.org.uk email address. IWM will comply with written requests within one calendar month of receipt.

8.2 Data Subjects also have the right, in certain circumstances, to request the erasure of their personal data, to object to or restrict its processing and to request that inaccurate personal data about them is corrected. All such requests, and other complaints about IWM's use of personal data, must be forwarded to the Data Protection Officer.

9. Security and data breaches

9.1 Personal data will be stored securely and in accordance with IWM Information Security Policy and procedures. Personal data is classified as Level 1 Data.

9.2 Members of staff are responsible for ensuring that all personal data they are working with is kept securely and is not disclosed, either orally or in writing, to any third party without the permission of their Head of Department and, in certain cases, the Data Protection Officer in accordance with Section 7.3. It is IWM policy that unauthorised disclosure, either knowingly or negligently, may be a valid reason for disciplinary action.

9.3 Managers must take steps to ensure that office and remote working environments and working practices take account of the security necessary to prevent the loss, theft, damage or unauthorised access to personal information. Information Asset Owners are responsible for ensuring that all systems storing personal data, or other assets or repositories of information are appropriately risk assessed and protected from identifiable threats.

9.4 The technical security of personal data is the responsibility of the Chief Information Officer who may, with the agreement of the Data Protection Officer, introduce technical security requirements as and when necessary.

9.5 Personal data can only be held on IWM approved systems.

9.6 Messaging, such as chat functions available in collaboration tools, must not be used to transmit or discuss personal information, such as issues relating to specific individuals, including staff, visitors or customers.

9.7 Personal data must never be downloaded onto laptops, memory sticks or other forms of removable media unless the written permission of the Information Asset Owner, and in the case of

special category or criminal offence data, the Data Protection Officer, is obtained first. In these cases the data must always be encrypted.

9.8 Personal data must always be transported securely, by IT Security approved channels.

9.9 All data breaches – instances where loss, unauthorised access, deletion or alteration is suspected - must be reported immediately to the IT Service Desk. The Data Protection Officer and Chief Information Officer must also be informed, as soon as the situation allows. Breaches must be managed in accordance with IWM's Data Breach guidance. Serious data breaches will be reported to the Information Commissioner within 72 hours.

9.10 Personal data will be disposed of confidentially. Hard copy information and removal media such as memory sticks and CDs must be shredded, and all information removed from other electronic storage media prior to disposal.

10. Procurement and outsourcing

10.1 The Data Protection Officer must approve any procurement plans for the management of personal data. This includes the purchase of new IT systems or the outsourcing of IWM functions where personal data is involved.

10.2 All information systems containing personal data must comply with this policy and have a minimum level of records and information functionality, as set out by the Governance Department. This includes information security, access controls and the ability to implement retention periods for records stored in the system.

10.3 Business cases for new systems or outsourcing the management of personal data must include a Data Protection Assessment. .

10.3 Any third party processing personal data on behalf of the Museum will be required to comply with the Data Protection legislation and this policy. All third party processing arrangements must be governed by a contract, which must contain the IWM's standard Data Protection clauses. The Data Protection Officer may decide that additional clauses are necessary and must approve the final contract.

10.4 Security arrangements for the external storage of electronic personal data must be approved by the Chief Information Officer.

10.5 Personal data is not to be stored or sent outside the UK unless the country is approved by the UK government as suitable for the storage of personal data, or if specific safeguards are in place. Special category and criminal offence data should be stored in the UK wherever possible.

11. Monitoring and record keeping

11.1 All areas processing personal data must keep records that clearly show:

- The source of the personal data
- When it was collected
- The information supplied at the time the personal data was collected
- The condition(s) met for the processing of the personal data
- How it has been used
- How long it is to be kept

- Who has access to the data and the training they have received
- Any security breaches affecting the personal data

These records must be made available to the Data Protection Officer when required.

11.2 This policy will be monitored via the annual Information Asset Owner returns; by Quarterly Reporting and via spot checks carried out by the Data Protection Officer or Governance Department.

11.3 Information Asset Owners, Senior Managers and Heads of Department are responsible for reporting to the Governance Department any changes to the management of personal data in their work areas.

12. Staff awareness and training

12.1 General procedures for the collection, management and disposal of personal data are available to all staff from the Governance Department and via the Intranet.

12.2 All staff are required to read this policy and to attend an Information Governance briefing during their probationary period with the Museum. Further training will be provided appropriate to the individual's role and seniority.

12.3 All Information Asset Owners must create procedures tailored to the use of the systems they are responsible for. Staff will be trained in these procedures before being given access to the information asset and a record should be kept of who has been trained.

13. Breach of this Policy

13.1 All complaints relating to breaches of this policy must be forwarded to the Data Protection Officer.

13.2 Staff found to be in breach of this policy will be subject to disciplinary action.

14. Policy Ownership and Review

14.1 This policy is owned by the Executive Director, Collections and Governance

14.2 It was approved in March 2010

14.3 Amended December 2017 to include GDPR requirements and approved by the Board of Trustees

14.4 Amended April 2018 to include reference to the Data Protection Bill and Public Function statement

14.5 Amended September 2022 to include general updates reflecting changes in IWM structure and IWM's departure from the European Union.

14.5 Amended June 2024 to change the Data Protection officer from Deputy Director-General to Executive Director, Collections and Governance

Appendix A: Data Protection Definitions

Data	Any information, which is being processed automatically or recorded as part of a relevant, filing system.
Data Controller	A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data Subject	An individual who is the subject of personal data.
Personal Data/Information	Data which relates to an identifiable living individual
Processing	Obtaining, accessing, altering, adding to, deleting, changing, disclosing or merging data and anything else, which can be done with data
Special Category Data	Information about an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health or condition, sexual life, commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed by him/her.

Appendix B: Data Protection Principles

Principle	Relevant section(s) of policy
GDPR Principle 5(1)(a): Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’	5, 6, 7 and 8
GDPR Principle 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving in the public interest is deemed compatible)	5, 6 and 8
GDPR Principle 5(1)(c): Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)	5
. **GDPR Principle 5(1)(d)** Personal data shall be accurate and, where necessary, kept up to date: every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)	6
GDPR Principle 5(1)(e): Personal data shall be 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 (nb exemption for this for archiving in the public interest)	6
GDPR Principle 5(1)(f): Personal data shall be 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.	6, 9,10 and 11
GDPR Chapter III: Rights of the Data Subject: Article 15: Rights of access Article 16: Right of rectification Article 17: Right of erasure (‘right to be forgotten’) Article 18/19: Right to restriction of processing Article 20: Right to data portability Article 21: Right to object to processing based on public or legitimate interests and for marketing Article 22: Right to object to automated decision making, including profiling	7 and 8

GDPR Chapter V: Transfers of personal data to third countries or international organisations Transfers of personal data shall only be within the EEA, to a country identified by the European Union as having an adequate level of protection or meet the requirements set out in Articles 46, 47, 48 or 49.	10

Appendix C: Associated legislation and IWM policies

Act
Data Protection Act 1998
Human Rights Act 2000
Privacy and Electronic Communications Regulations 2003 and 2011

Policy	**Owner**
Archives and Records Management Policy	Executive Director, Collections and Governance
IT Systems Acceptable Use Policy	Chief Information Officer
Freedom of Information Policy	Executive Director, Collections and Governance
Information Security Policy	Executive Director, Collections and Governance
Privacy Policy	Executive Director, Collections and Governance

Appendix D: IWM Statement of Public Function

IWM's 'Public Function' for the purposes of Data Protection is based upon its functions under **The Imperial War Museum Acts 1920** and 1955, relevant Statutory Instruments, the Museums and Galleries Act 1992, The Public Records Act 1958, Freedom of Information Act 2000 and the Charities Act 2011. It also includes commitments agreed by IWM with its sponsoring government department in its **Management Agreement**, the visions and objectives set out in the **Corporate Plans** agreed by the Board, and the provision of general advice relating to its core expertise to researchers and the general public.

IWM creates, holds and uses information for all the following purposes within its Public Function:

- Acquisition and management of archives, objects, artworks and printed material relating to the history of conflict in the national collection
- Provision of worldwide access to these collections, exhibitions and expertise: in the museum, (via exhibitions and the Research Room), on loan and through partnerships, in all and any media and formats or through innovative outreach and web-based programmes.
- Production or commissioning of exhibitions, educational and research-based print and digital material which draws on the unique collections and historical expertise, either directly or through partnerships or through the IWM Trading Company Ltd (IWM's wholly owned trading subsidiary).
- Conservation, maintenance, development, safety and security of its assets, including the collections, estate, infrastructure and information.