

Data Protection Policy

1. Overview

At Amgueddfa Cymru, we value the privacy and protection of personal data. This Data Protection Policy outlines our commitment to ensuring the security and confidentiality of personal information collected, processed, and stored by our organisation. We are dedicated to complying with all applicable data protection laws and regulations to safeguard the privacy rights of individuals.

2. Purpose

See overview

3. Scope

This policy applies to all personal data collected, processed, and stored Amgueddfa Cymru, whether in electronic or physical form. It encompasses all employees, contractors, and third parties who have access to personal data in the course of their duties.

4. Policy

Principles of Data Protection

We adhere to the following principles to govern our data protection practices:

- a. **Lawfulness, Fairness, and Transparency:** We collect and process personal data in a lawful, fair, and transparent manner, ensuring individuals are informed about the purposes for which their data is collected and processed.
- b. **Purpose Limitation:** Personal data is collected for specified, explicit, and legitimate purposes, and will not be further processed in a manner incompatible with those purposes.
- c. **Data Minimisation:** We only collect and retain personal data that is necessary for the intended purposes. We ensure the data collected is adequate, relevant, and limited to what is required.
- d. **Accuracy:** We strive to maintain accurate and up-to-date personal data. Measures are in place to rectify or erase inaccurate or incomplete data promptly.
- e. **Storage Limitation:** Personal data is stored only for as long as necessary to fulfill the purposes for which it was collected. Retention periods are defined and regularly reviewed.
- f. **Integrity and Confidentiality:** We implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data, protecting it against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- g. **Accountability:** We take responsibility for complying with applicable data protection laws and regulations. We maintain records of our data processing activities and have designated personnel responsible for data protection matters.

Data Collection and Processing

a. **Lawful Basis:** We collect and process personal data based on one or more lawful bases, including the individual's consent, the performance of a contract, compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest, or legitimate interests pursued by the organisation or a third party.

b. **Consent:** When relying on consent as the lawful basis for data processing, we obtain clear and unambiguous consent from individuals and provide them with the right to withdraw their consent at any time.

c. **Data Subjects' Rights:** We respect the rights of individuals regarding their personal data. Individuals have the right to access, rectify, erase, restrict processing, object to processing, data portability, and not to be subject to automated decision-making.

d. **Data Security:** We implement appropriate technical and organisational measures to protect personal data from unauthorised access, disclosure, alteration, or destruction. These measures include access controls, encryption, secure storage, regular backups, and staff training.

e. **Third-Party Processors:** When engaging third-party processors to handle personal data on our behalf, we ensure that they provide sufficient guarantees regarding the implementation of appropriate technical and organisational measures to protect the data.

Data Breach Management

a. **Incident Response:** We have established procedures to detect, investigate, and respond to data breaches promptly. In the event of a breach, we will assess the risks, take necessary actions to mitigate the impact, and notify the appropriate authorities and affected individuals, as required by applicable laws and regulations.

b. **Record Keeping:** We maintain comprehensive records of all data breaches, including the nature of the breach, its effects, and the remedial actions taken.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

N/A

7 Definitions and Terms

8 Revision History

Date of Change	Responsible	Summary of Change
06/2024	Data Protection Team	No changes
06/2025	Data Protection Team	No changes
02/2026	Data Protection Team	No changes