Data Protection Policy

Overview

This Data Protection Policy is the overarching policy for data security and protection for Amgueddfa Cymru

Purpose

The purpose of the Data Protection Policy is to support the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy therefore seeks to ensure that:

We are clear about how personal data must be processed and the expectations for all those who process personal data on its behalf;
Comply with the data protection law and with good practice;

Protect Amgueddfa Cymru reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights

Protect Amgueddfa Cymru from risks of personal data breaches and other breaches of data protection law.

Definitions

Data controller – a person 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 will be processed.

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

Personal Data – information from which a living person can be identified.

Sensitive Information – data relating to a person's:

• racial or ethnic origin • political opinions • religious or other beliefs of a similar nature • trade union memberships • physical or mental health or condition • offences (including alleged offences) • criminal proceedings, outcomes and sentences.

Where we collect any sensitive data, we will take appropriate steps to ensure that we have explicit consent to hold, use and retain the information.

Scope

This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

This policy applies to all staff, including temporary staff and contractors.

Personal data protection principles

When you process personal data, you should be guided by the following principles, which are set out in the GDPR. Amgueddfa Cymru is responsible for, and must be able to demonstrate compliance with, the data protection principles listed below:

Those principles require personal data to be:

Processed lawfully, fairly and in a transparent manner (Lawfulness, fairness, and transparency). Detail on how to achieve this can be found in Appendix 1.

Collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (Purpose limitation). Detail on how to achieve this can be found in Appendix 2.

Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data minimisation). Detail on how to achieve this can be found in Appendix 2.

Accurate and where necessary kept up to date (Accuracy). Detail on how to achieve this can be found in Appendix 2.

Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed (Storage limitation). Detail on how to achieve this can be found in Appendix 2.

Processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Security, integrity and confidentiality). Detail on how to achieve this can be found in Appendix 2.

Data Subjects Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

Where the legal basis of our processing is Consent, to withdraw that Consent at any time.
To ask for access to the personal data that we hold (see below);
To prevent our use of the personal data for direct marketing purposes

To object to our processing of personal data in limited circumstances
To ask us to erase personal data without delay:

a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed.

b. if the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;

c. if the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;

d. if the data subject has objected to our processing for direct marketing purposes;

e. if the processing is unlawful.

To ask us to rectify inaccurate data or to complete incomplete data.

To restrict processing in specific circumstances e.g. where there is a complaint about accuracy;

To ask us for a copy of the safeguards under which personal data is transferred outside of the EU;

The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract,

To prevent processing that is likely to cause damage or distress to the data subject or anyone else;

To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
To make a complaint to the ICO; and
In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Responsibilities

Amgueddfa Cymru responsibilities

As the Data Controller, Amgueddfa Cymru is responsible for establishing policies and procedures in order to comply with data protection law.

Staff responsibilities

Staff members must ensure that:
All personal data is kept securely.
No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
Personal data is kept in accordance with the Amgueddfa Cymru retention schedule.
Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance team;
Any data protection breaches are swiftly brought to the attention of the Information Compliance team
Where there is uncertainty around a data protection matter advice is sought from the Information Compliance Team.

Policy

We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, the common law duty of confidentiality, the General Data Protection Regulation, and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time,

We ensure that it is as easy to withdraw as to give consent.

We will undertake / commission **delete as appropriate** annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

Processed lawfully, fairly and in a transparent manner.

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 (‘data minimisation’);

Accurate and 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 ('storage limitation');

Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR;

i. The right to be informed.
ii. The right of access.
iii. The right to rectification.
iv. The right to erasure.
v. The right to restrict processing.
vi. The right to data portability.
vii. The right to object.
viii. Rights in relation to automated decision making and profiling.

Underpinning policies and procedures.

This policy is underpinned by the following:

Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors;

Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share;

Data Security Policy – outlines procedures for the ensuring the security of data including the reporting of any data security breach;

Network Security Policy – outlines procedures for securing our network;

Business Continuity Plan –outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation.

Data protection by design and default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any

processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

All new systems used for data processing will have data protection built in from the beginning of the system change.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

Policy Compliance

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.

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

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

Appendix 1

Principle 1 of GDPR – Processing personal data lawfully, fairly and transparently

1. **Lawfulness and fairness**

You may only process personal data fairly and lawfully and for specified purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data for legitimate purposes without prejudicing the rights and freedoms of data subjects. In order to be justified, Amgueddfa Cymru may only process personal data if the processing in question is based on one (or more) of the legal bases set out below.

The legal bases for processing non-sensitive personal data are as follows:

1. the data subject has given his or her Consent
2. the processing is necessary for the performance of a contract with the data subject
3. to meet our legal compliance obligations
4. to protect the data subject's vital interests
5. to pursue our legitimate interests (or another's legitimate interests) which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The specific legitimate interest or interests that Amgueddfa Cymru is pursuing when processing personal data will need to be set out in relevant Privacy Notices. This ground can only be relied upon for private functions e.g., marketing, fundraising and not for public functions.

You must identify the legal basis that is being relied on for each processing activity, which will be included in the Privacy Notice provided to data subjects.

(a) Consent

You should only obtain a data subject's Consent if there is no other legal basis for the processing. Consent requires genuine choice and genuine control.

A data subject consents to processing of his/her personal data if he/she indicates agreement clearly either by a statement or positive action to the processing. Silence, pre-ticked boxes, or inactivity are therefore unlikely to be sufficient. If Consent is given in a document that deals with other matters, you must ensure that the Consent is separate and distinct from those other matters.

Data subjects must be able to withdraw Consent to processing easily at any time. Withdrawal of Consent must be promptly honoured. Consent may need to be renewed if you intend to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented, or if the Consent is historic.

You will need to ensure that you have evidence of Consent, and you should keep a record of all Consents obtained so that we can demonstrate compliance.

Consent is required for some electronic marketing and some research purposes.

(b) Legal bases for Processing Sensitive Personal Data, including Special Category Data

Special Category Personal Data is data revealing:

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs,
4. trade union membership,

It also includes the processing of:

5. genetic data
6. biometric data for the purpose of uniquely identifying a natural person,

7. data concerning health
8. data concerning a natural person's sex life or sexual orientation

Personal data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences should be treated in the same way to special category data.

The processing of sensitive personal data by Amgueddfa Cymru must be based on one of the following (together with one of the legal bases for processing non-sensitive personal data as listed above):

1. the data subject has given explicit Consent (requiring a clear statement, not merely an action)
2. the processing is necessary for complying with employment law.
3. the processing is necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving Consent;
4. the processing relates to personal data which are manifestly made public by the data subject;
5. the processing is necessary for the establishment, exercise or defence of legal claims;
6. the processing is necessary for reasons of substantial public interest (provided it is proportionate to the particular aim pursued and takes into account the privacy rights of the data subject)
7. the processing is necessary for the purposes of preventive or occupational medicine, etc. provided that it is subject to professional confidentiality
8. the processing is necessary for reasons of public interest in the area of public health, provided it is subject to professional confidentiality;
9. the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes if it is subject to certain safeguards (i.e. pseudonymisation or anonymisation where possible, the research is not carried out for the purposes of making decisions about particular individuals (unless it is approved medical research) and it must not be likely to cause substantial damage/distress to an individual and is in the public interest).

2. Transparency (notifying data subjects)

Under the GDPR Amgueddfa Cymru is required to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. That information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever we collect personal data directly from data subjects, for example for the recruitment and employment of staff, at the time of collection we must provide the data subject with all the prescribed information which includes:

1. Amgueddfa Cymru's details

2. Contact details of DPO
3. Purposes of processing
4. Legal basis of processing
5. Where the legal basis is legitimate interest, identify the particular interests (e.g., marketing, fundraising)
6. Where the legal basis is Consent, the right to withdraw
7. Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision

When personal data is collected indirectly (for example, from a third party or publicly available source), you must also provide information about the categories of personal data and any information on the source. The data subject must be provided with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

Appendix 2

Principle 2 of GDPR - Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

You cannot therefore use personal data for entirely new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes. Where the further processing is not based on the data subject's Consent or on a lawful exemption from data-protection law requirements, you should assess whether a purpose is incompatible by taking into account factors such as:

The link between the original purpose/s for which the personal data was collected and the intended further processing
The context in which the personal data has been collected – in particular the Amgueddfa Cymru-data subject relationship. You should ask yourself if the data subject would reasonably anticipate the further processing of his/her personal data
The nature of the personal data in particular whether it involves special categories of personal data (i.e. sensitive) or personal data relating to criminal offences/convictions
The consequences of the intended further processing for the data subjects
The existence of any appropriate safeguards e.g., encryption or pseudonymisation.

Principle 3 of the GDPR – Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. You should not therefore amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. Conversely, personal data must be adequate to ensure that we can fulfil the purposes for which it was intended to be processed.

You may only process personal data when performing your job duties requires it and you should not process personal data for any reason unrelated to your job duties.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Amgueddfa Cymru's data retention policy and schedule.

Principle 4 of the GDPR - Accuracy

Personal data must be accurate and, where necessary, kept up to date. You should ensure that personal data is recorded in the correct files.

Incomplete records can lead to inaccurate conclusions being drawn and in particular, where there is such a risk, you should ensure that relevant records are completed.

You must check the accuracy of any personal data at the point of collection and at regular intervals thereafter. You must take all reasonable steps to destroy or amend inaccurate records without delay and you should up-date out-of-date personal data where necessary (e.g. where it is not simply a pure historical record).

Where a data subject has required his/her personal data to be rectified or erased, you should inform recipients of that personal data that it has been erased/rectified, unless it is impossible or significantly onerous to do so.

Principle 5 of the GDPR – Storage limitation

You must not keep personal data in a form that allows data subjects to be identified for longer than needed for legitimate Amgueddfa Cymru business purposes or other purposes for which Amgueddfa Cymru collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of personal data can be kept for longer than necessary if anonymised.

You will take all reasonable steps to destroy or erase from Amgueddfa Cymru's systems all personal data that we no longer require in accordance with all relevant Amgueddfa Cymru records retention schedules and policies.

You will ensure that data subjects are informed of the period for which their personal data is stored or how that period is determined in any relevant Privacy Notice.

Principle 6 of the GDPR – Security, Integrity, and Confidentiality

Amgueddfa Cymru is required to implement and maintain appropriate safeguards to protect personal data, taking into account in particular the risks to data subjects presented by unauthorised or unlawful processing or accidental loss, destruction of, or damage to their personal data. Safeguarding will include the use of encryption and pseudonymisation where appropriate. It also includes protecting the confidentiality (i.e. that only those who need to know and are authorised to use personal data have access to it), integrity and availability of the personal data. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

You are also responsible for protecting the personal data that you process in the course of your duties. You must therefore handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality. You must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

You must comply with all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction.

You must comply with all applicable aspects of our Information Security Policy, and comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Law standards to protect personal data.

You may only transfer personal data to third-party service providers (i.e. data processors) who provide sufficient guarantees to implement appropriate technical and organisational measures to comply with Data Protection Law and who agree to act only on Amgueddfa Cymru's instructions. Data processors should therefore be appointed subject to Amgueddfa Cymru's standard contractual requirements for data processors.

Revision History

Date of Change	Responsible	Summary of Change