Data Protection Policy

1. Purpose of the Policy

The purpose of this Policy is to ensure that the University and its staff, students, contractors and authorised processors comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the EU General Data Protection Regulation (EU GDPR), where applicable, and any other relevant data protection legislation in jurisdictions in which the University operates, including Germany where University activities are undertaken. The University takes its responsibilities with regard to the management of the requirements of Data Protection legislation seriously, and any infringement may be considered under disciplinary procedures.

This document provides the policy framework through which effective compliance can be achieved and audited.

2. Scope/Applicability

This policy applies to staff, students, agents of the University and any authorised processors of personal data held or owned by the University, regardless of where the data is held and, in respect of automatically processed data, the ownership of the equipment used, if the processing is for University purposes. This policy also applies to personal data retained and processed by Aberystwyth University Students' Union.

The University needs to process information about its employees, its students and other individuals: for example, to allow it to monitor performance, achievements and health and safety, and so that staff can be recruited and paid, courses organised and legal obligations (e.g. to funding bodies and the government) fulfilled. Such information must be collected and used fairly, stored safely and not disclosed unlawfully.

The University is required to adhere to the data protection principles established under the UK GDPR, the EU GDPR (where applicable), the Data Protection Act 2018 and any applicable national legislation. In accordance with those principles personal data shall be:

1. Processed fairly and lawfully and in a transparent manner
2. Processed for specified, explicit and legitimate purposes
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accurate and up to date

5. 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
6. Processed in a manner that ensures appropriate security of the personal data

Personal data shall also be processed in a manner that respects the rights of data subjects and any international transfer of personal data shall comply with the applicable requirements of the UK GDPR, the EU GDPR and other relevant legislation.

The University also notes that it is required to comply with those provisions set out in the GDPR which relate to the principle of 'accountability'.

Where the University processes personal data through activities undertaken in Germany or other Member States of the European Union, such processing shall additionally comply with the EU General Data Protection Regulation (EU GDPR), applicable national data protection legislation, including the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), and the requirements of the relevant supervisory authorities.

3. Responsibility

3.1 University Responsibilities

The University is a data controller under the UK GDPR, the Data Protection Act 2018, the EU GDPR where applicable, and equivalent data protection legislation in other jurisdictions in which it operates and fully recognises its responsibilities for establishing policies and procedures in order to comply with the relevant requirements.

3.1.1 University-level Committee

The University Executive Group is ultimately responsible for approving and overseeing the operation of this Policy.

3.1.2 University's Data Protection Officer

The University will nominate an appropriate person as the University's Data Protection Officer, who will be a person of sufficient knowledge and seniority in the University.

The University will ensure that the identity of the University's Data Protection Officer is to be made known to all staff, students, contractors and volunteers and will also draw to their attention this Policy and associated documentation. The Data Protection Officer is responsible for drawing up guidance and promoting compliance with this policy.

The Data Protection Officer has access to all relevant documents relating to a legal compliance request under Data Protection legislation and it is the Data Protection Officer (in consultation, when necessary, with the relevant senior officers) that will make the decisions regarding what information is released or exempted.

The University has appointed a Data Protection Officer whose identity and contact details are published on the University's official website and are communicated to staff, students and relevant stakeholders.

3.2 Responsibilities of Heads of Academic Units and Central Service Departments

Heads of academic units and Heads of Central Service are responsible for ensuring compliance with the data protection legislation and other relevant legislation and for ensuring that the requirements of this Policy are met.

Heads of academic units and Heads of Central Service must ensure that all new members of staff receive an appropriate introductory briefing on data protection and other relevant legislation and that staff members within their areas of responsibility receive refresher courses on data protection compliance.

Heads of academic units and Heads of Central Service may choose to delegate the management of, but not the responsibility for, data protection matters to an appropriate senior member of staff.

The Data Protection Officer will perform periodic audits to ensure compliance with this Policy and with other relevant legislation.

3.3 Staff Responsibilities

3.3.1 It is a condition of employment that staff will abide by the rules and policies of the University. Any failure to follow this Policy may result in disciplinary proceedings.

3.3.2 When staff use personal information about students, other staff members, or other individuals, they must comply with the requirements of this Policy.

3.3.3 Staff must ensure that:

- all personal information entrusted to them in the course of their employment is kept securely;
- no personal information is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party;
- no personal information is accessed by staff for any reason other than for legitimate University business;
- any information that they provide to the University in connection with their own employment is accurate and up to date and that they inform the University of any changes, e.g. changes of address.

3.3.4 When members of staff are responsible for supervising students doing work which involves the processing of personal information (e.g. in research projects), they must ensure that those students are aware of the data protection principles as set out in point 2 above, and, in particular, the requirement to obtain the data subject's consent where appropriate.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from their line manager or the Data Protection and Copyright Manager.

3.4 Contractors, Casual Staff and Volunteers

Heads of academic units and Heads of Central Service who employ contractors, casual staff or volunteers must ensure that they are made aware of their obligations under the legislation and the requirements of this Policy.

4. Detailed Policy

4.1 Data Subject Access Requests

The University is required to permit individuals to access their own personal data held by the University via a Data Subject Access Request. Any individual wishing to exercise this right should do so in writing to the Data Protection officer at dpo@abergermany.de

The University aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within one calendar month of receipt of the request, unless an extension is permitted under applicable data protection legislation and within any relevant time periods set by other jurisdictions.

Individuals will not be entitled to access information to which any exemptions apply. However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the Data Protection and Copyright Manager.

4.2 Consent to process

In some cases, the University needs to process some information that, by the definition set out by the GDPR, is classified as special category personal data under the UK GDPR and EU GDPR. Such information may be needed to ensure safety, to comply with the requirements of the government or of funding bodies, to provide support for staff or students or to implement institutional policies. In some of these cases, the University may need to seek specific consent.

4.3 Information Collected by the University website

Information collected on the Aberystwyth University website is owned by Aberystwyth University (including any subsidiary companies). The University will not sell, share or rent this information to others in ways which differ from what is stated on the University's website or in any prior agreement.

4.4 Data Security Breaches

Any data-related incident or breach or potential breach of UK data protection legislation or other equivalent legislation or of the requirements of this Policy should be reported to the

Data Protection and Copyright Manager as soon as possible and, in any case, within 24 hours of discovery.

Incidents will be dealt with in accordance with the University's *Procedures in the event of a suspected breach of Data Protection.*

Where required by applicable legislation, personal data breaches shall be reported to the relevant supervisory authority within 72 hours of the University becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

4.5 Sharing of data with third parties

The sharing of personal data will comply with those details set out in staff contracts and the Data Protection Statements for staff and students.

Staff, students and others whose personal data may be held by the institution, should note that the University has a duty under the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism, and that this duty may involve the passing of information to the police / security services.

The University will implement appropriate technical and organisational measures to ensure and demonstrate compliance with applicable data protection legislation, including regular review of policies, staff training, risk assessments, records of processing activities and data protection impact assessments where required.

5. Relevant Legislation, Codes of Practice and Industry Standards

UK General Data Protection Regulation (UK GDPR)

EU General Data Protection Regulation (EU GDPR), where applicable

Data Protection Act 2018 (United Kingdom)

German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), where applicable

Data Protection Act (Mauritius) 2004 (where applicable)

Counter-Terrorism and Security Act 2015

Freedom of Information Act 2000

Limitation Act 1980

Information Commissioner's Employment Practices Guidance (or any successor guidance)