Data Protection Policy

1. Purpose

This policy provides a framework for ensuring that Abertay University meets its obligations under the UK General Data Protection Regulation 2018 ("UK GDPR") and the UK Data Protection Act 2018 ("DPA"), including (where appropriate) relevant amendments to the legislation under the UK Data Usage and Access Act 2025 ("DUAA"). To better understand this policy you may wish to review the Information Commissioner's Office's website which includes a glossary of key terms and abbreviations which is published on their website at Glossary | ICO.

This policy is part of the University's wider Information Governance Framework, which outlines the governance of information as a critical business asset, essential for meeting the University's business, accountability, legal and regulatory requirements. Please ensure you familiarise yourself with this framework prior to reading this policy.

2. Scope

This policy applies to all University Members (staff (regardless of contract type), students, members of Court, consultants, contractors, and other relevant parties) where they are data controllers or processors of personal data held by the University. It applies to personal data and special categories of personal data as defined under the UK GDPR that are processed by Abertay University. This includes personal data processed for research and researchers should read this in conjunction with the GDPR for Research Policy.

3. Policy

3.1 Compliance with Data Protection Principles

Abertay University is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data it processes about students, staff, and those who work or interact with us.

It will implement appropriate technical and organisational measures in an effective manner to ensure compliance with the seven data protection principles as set out in Article 5(1) of the UK GDPR.

These are:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

It will do this by applying adequate resources and controls to implement the following actions.

- **Data Protection Officer:** a suitably qualified Data Protection Officer (DPO) will be appointed and will be provided with adequate resources to conduct their role.
- **Lawfulness, Fairness, and Transparency**: the University will process personal data lawfully, fairly, and transparently under the specified purposes as set out in the lawful bases of UK GDPR. It will inform personal data subjects within Privacy Notices and statements about processing of their data and their rights relating to that.
- **Purpose Limitation:** the University will ensure that only personal data that are necessary for each specific purpose is processed, and that any processing is limited to that necessary for each purpose, except when further processing for a different purpose is deemed to be compatible with the original purpose (e.g. research data).
- **Data Minimisation:** the University will ensure that only the minimum amount of personal data is collected and processed for any specific purpose.
- **Accuracy:** the University will maintain accurate personal data and where necessary, keep it up to date. It will destroy any data marked for destruction as per the University's Information Retention and Disposal Policy.
- **Storage Limitation, Integrity, and Confidentiality:** the University will ensure personal data is stored no longer than necessary and access is restricted to that necessary for each purpose. Decisions on determining how long to retain personal data shall be based on the University's Information Retention and Disposal Policy and consultation with the Governance Office. It will maintain records of audit trail, retention, and destruction to monitor access, and enforcement of retention periods.
- **Accountability**: the University will produce required documentation such as Privacy Notices, Data Protection Impact Assessments (DPIA), Records of Processing Activities (RoPA) in relation to the personal data it processes, and records of Personal Data Breaches. It will regularly test the privacy measures implemented, and conduct periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvements.
- **Policies and Procedures**: the University will integrate data protection into its policies, processes and procedures relating to the way that personal data is handled by it. It will

also develop procedures to handle core data protection processes of personal data Subject Access Requests (SARs), DPIAs, and Personal Data Breaches.

- **Personal Data Breaches:** the University will report losses or suspected breaches of personal data to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, if required. It will take appropriate action to mitigate against the impact and resultant risks to the rights and freedoms of data subjects affected by any data breach. Measures will also be put in place to learn from personal data breach incidents and reduce the risk of them happening again.
- **Data Protection Privacy by Design and by Default**: the University will have a procedure to assess processing of significant amounts of personal data, or perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) to be carried out, and have processes to assist staff in ensuring compliance and privacy by design is integral to any contract developed, and product, project or service that it offers. The University recognises that some of its students are under the age of 18, and that a cautious and risk-based approach therefore must be taken to provide sufficient protection for children that incorporates awareness and processes to implement this requirement.
- **Guidance, Support, and Training:** the University will raise awareness, provide support and training to University members on how to comply with data protection law, and keep a record of completion of the training. This will include regularly refreshed mandatory training for all University members on data protection and the expectations required of them in relation to handling and processing of personal data.
- **Complaints:** the University will provide a method for data protection complaints to be made, acknowledge them within 30 calendar days of receipt, take appropriate steps to respond to them, and inform complainants of the outcome without undue delay.

3.2 Data Subject Rights

Data Subjects have rights under GDPR in relation to how their Personal Data is handled. These are:

- A right to be informed about the collection and use of personal data.
- A right to access and receive a copy of written or recorded (audio and video) personal data, and other supplementary information.
- A right to rectification to have inaccurate personal data rectified, or completed if it is incomplete
- A right to erasure of personal information in certain circumstances
- A right to restrict processing of personal data in certain circumstances
- A right to object to processing of personal data in certain circumstances
- Rights related to automated decision-making including profiling.

Abertay University is committed to upholding these rights. The Individual Rights Policy provides further information on how it will do this, including handling requests in relation to them.

3.3 Roles and Responsibilities

All University Members collecting, maintaining, receiving, storing, using or handling personal information are responsible for complying with data protection legislation and the University policies on this.

The following lines of responsibility show the hierarchy of responsibility throughout the university over and above this general responsibility. All members of the University should ensure they are aware of their overall role and who to go to for guidance and support, should they need to raise data protection issues.

Finance and Corporate Performance Committee provides high-level oversight of this policy and the broader Information Governance Framework, advising and reporting to University Court.

The Senior Management Team (SMT) has overall responsibility for upholding the correct management of the personal data generated by the functions and activities of the University Faculties/Other Academic Units/Professional Services. More specifically, they will ensure that the personal data controlled within their area are managed in a way that meets the requirements of data protection legislation and this Policy. They will also support staff to undertake data protection training and arrange appropriate data protection training and support for students in data protection if relevant to their courses of study and in preparation for placements that may involve processing personal data.

The Information Governance Committee reports to the University's Senior Management Team and is responsible for setting this policy and ensuring its implementation.

The Vice Principal and University Secretary is the University's Senior Information Risk Owner, responsible for ensuring the University corporately meets its legal responsibilities, and internal and external governance and accountability requirements, including those related to data protection.

The Head of Governance and Deputy Secretary is the University Data Protection Officer (DPO) and is responsible for overseeing the implementation of data protection policies, monitoring the University's compliance with data protection law, and developing related policies and guidelines where applicable. The DPO is also the first point of contact for individuals and external bodies on data protection matters, and for the ICO. The day-to-day management and implementation of this responsibility is devolved to the staff of the Governance Office. They will report to the Head of Governance and Deputy Secretary, who in turn reports to the Vice Principal and University Secretary.

The Governance Office will have a co-ordination and support role, including the development and maintenance of the Data Protection Policy and Procedure Framework, co-ordination of Personal Data Breach investigations, production of guidance and training to assist members of the University in carrying out their data protection responsibilities, and provision of advice on legislation, policy, and best practice.

4. Related Policy Documents and Supporting Documents

Legislation	UK Data Protection Act 2018; UK Data Usage and Access Act 2025; UK General Data Protection Regulation 2018
Strategy	Digital Strategy; Information Governance Framework
Policy	GDPR for Research Policy; Individual Rights Policy; Information Management Policy; Information Retention and Disposal Policy; Information Security Policy; Privacy by Design and by Default Policy
Procedures	N/A
Guidelines	Glossary | ICO; University Intranet Guidance on Data Protection;
Local Protocol	N/A
Forms	Data Protection Impact Assessment Form; Privacy Notice Template

5. Additional Information

Audience	Public
Applies to	All University Members
Classification	Corporate Governance
Category	Information Governance
Subcategory	Data Protection and Information Access
Approving Authority	University Court
Approval Date	26 November 2025
Effective Date	1 January 2026
Review Date	31 December 2028
Policy Document Author	Archivist and Information Governance Officer; Head of Governance and Deputy Secretary
Policy Document Owner	Vice-Principal and University Secretary

For the purposes of this policy document and related policy documents, general terms are defined in the Policy Document Library Glossary.

If you would like this document in a different format (e.g. large print, braille), please contact policydocumentlibrary@abertay.ac.uk

If you need any assistance to access or understand the document, please contact dataprotectionofficer@abertay.gov.uk

All printed versions of this document are classified as uncontrolled. Please ensure you access the current version in the Policy Document Library.