

Individual Rights Policy

1. Purpose

The purpose of this policy is to set out how the University will uphold the rights of data subjects under UK General Data Protection Regulation 2018 (“UK GDPR”) and the UK Data Protection Act 2018 (“DPA”), including (where relevant) amendments to the legislation under the UK Data Usage and Access Act 2025 (“DUAA”) when processing personal data during the course of its business. 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

Under the terms of the Data Protection legislation, the University will ensure that it enables and responds to the following individual rights being exercised.

3.1 The right to be informed

Individuals will be informed about the data the University processes about them by Privacy Notices that will be made available to them when their personal data is collected, or within one month of collection where the data is provided via another source. The University's Privacy notices can be accessed at [Legal | Abertay University](#).

3.2 The right of access

Individuals have the right to request access to their personal data, either verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the detail of the request. The University will respond to the request without undue delay and normally within one month of the detail of the request being confirmed, and normally no fee will be charged. Where a request is complex, or where the University has received a number of requests from the same individual, the time to respond fully may be extended by up to two months.

In responding to a request to access personal data, any information from which another individual could be identified will not normally be disclosed unless that individual's consent has been obtained, or if there is a valid reason under the legislation for the data to be provided, such as an exemption.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.3 The right to rectification

Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete. A request for rectification can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the detail of the request. The University will take reasonable steps to ensure the data is accurate, will rectify any inaccuracy, and will respond to the request within one month.

Normally no fee will be charged.

Matters of opinion are by their nature subjective, and so cannot necessarily be proven to be accurate or inaccurate. As a result, matters of opinion will not normally be rectified, but it will be clearly recorded that the record was a matter of opinion.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.4 The right to erasure

In some circumstances, individuals have the right to have their personal data erased (also known as the right to be forgotten).

Individuals have the right to have their personal data erased where:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- consent was the lawful basis for holding the data, and the individual withdraws their consent;
- legitimate interests were the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- the personal data is processed for direct marketing purposes and the individual objects to that processing;
- the personal data has been processed unlawfully;
- erasure is required to comply with a legal obligation; or
- the personal data has been processed to offer information society services to a child.

The right to erasure does not apply where the processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

A request for erasure can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the details of the request. The University will determine whether the request meets the criteria outlined above and will respond to the request within one month to confirm that the data has been erased, or to explain why it cannot be erased. Normally no fee will be charged.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.5 The right to restrict processing

In some circumstances, individuals have the right to request the restriction or suppression of their personal data. Individuals have the right to request that processing of their data be restricted in the following circumstances:

- where they have contested the accuracy of the data, and the accuracy is being verified;
- where the data has been unlawfully processed and the individual requests restriction rather than erasure;
- where the data is no longer required for its original purpose but the individual wishes it to be retained in order to establish, exercise or defend a legal claim; or
- where an individual has objected to the processing of their data and the legitimate grounds for processing are still being considered.

A request to restrict processing can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the details of the request. The University will determine whether the request meets the criteria outlined above and will respond to the request within one month to confirm that processing of the data has been restricted or to explain why it cannot be restricted. Where processing is restricted, the University will confirm the period of restriction if applicable. Normally no fee will be charged.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.6 The right to data portability

In some circumstances, individuals have the right to obtain and reuse their personal data for their own purposes across different services, allowing them to move, copy or transfer personal data from one IT environment to another in a safe and secure way. Data portability applies only where:

- the lawful basis for processing the data is either consent or the performance of a contract; and
- where the processing is automated (so for example, it excludes paper records); and
- where the data has been provided by the individual or is data resulting from the individual's activities.

A data portability request can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email

the details of the request. The University will determine whether the request meets the criteria outlined above and will respond to the request within one month to provide the data to the individual, or to another data controller as requested, or to explain why the data cannot be provided.

Where data is provided, it will be in a structured, commonly used, machine-readable format. Normally no fee will be charged.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.7 The right to object

In some circumstances, individuals have the right to object to the processing of their data.

- Where the personal data is used for direct marketing purposes, the right to object is absolute, and such requests will not be refused.
- Where the legal justification for processing is public task or legitimate interests, the right to object is not absolute, and processing may be continued where compelling legitimate grounds for processing can be demonstrated, or where the processing is for the establishment, exercise or defence of legal claims.

An objection to data processing can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the details of the request. The University will determine whether the request meets the criteria outlined above and will respond to the request within one month to confirm that processing has been ceased, or to explain why processing will not be ceased.

Normally no fee will be charged.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

3.8 Rights relating to automated decision making

Individuals have rights in relation to automated decision making that involves their personal data.

Automated decision-making can be carried out using standard personal data if appropriate safeguards are put in place and if the University:

- gives the data subject information about the processing;
- provides opportunities for the data subject to make representations about it

- introduces simple ways for them to request human intervention or challenge a decision and request a review of a decision; and
- carries out regular checks to make sure that the systems are working as intended.

Stricter rules apply concerning special category data. Individuals have a right not to be subject to a decision using their special category data, based solely on automated decision making (making a decision without any human involvement) if it will have a legal or similarly significant effect on them. They also have a right not to be subject to profiling (automated processing of personal data to evaluate certain things about an individual).

The University can only carry out this type of decision-making where the decision is necessary for the entry into or performance of a contract; or authorised by domestic law applicable to the controller; or based on the individual's explicit consent.

An objection to automated decision-making can be made verbally or in writing. The University will confirm the identity of the requester, clarify the request with the individual and confirm by email the details of the request. The University will determine whether the request meets the criteria outlined above and will respond to the request within one month to confirm that processing for automated decision-making has been ceased, or to explain why processing will not be ceased. Normally no fee will be charged.

If the University considers that a request is manifestly unfounded or excessive, a reasonable fee may be charged to deal with the request, or the request may not be dealt with. In either instance a justification will be provided to the individual.

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	Data Protection Policy; GDPR for Research 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	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 and related policy documents, 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 policy, please contact dataprotectionofficer@abertay.ac.uk

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