# Privacy by Design and by Default Policy

## 1. Purpose

This Policy provides the University's approach to embedding appropriate technical and organisational measures to implement Data Protection Principles effectively, safeguard individual rights, and thus ensure compliance with the UK General Data Protection Regulation ("GDPR") Article 25 requirement to embed data protection "privacy by design and by default" across its operations. Examples of appropriate technical and organisational measures are provided in the Appendix to this policy. 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.

It applies to all University activities involving processing of personal data and should be read in conjunction with the Data Protection Impact Assessment (DPIA) procedure and form. This includes personal data processed for research and researchers should read this in conjunction with the GDPR for Research Policy.

## 3. Policy Statement

### 3.1 Privacy by Design and by Default – General Principles

The University will adhere to the general principles of Privacy by Design and by Default.

These can be summarised as:

- **Use proactive rather than reactive measures**: take a proactive approach to data protection. Anticipate, identify and prevent privacy invasive events as much as possible. Develop a culture of "privacy awareness" across the institution.
- **Privacy should be the default position**: personal data must be automatically protected in any system, service, product, and / or business practice, with no action required by the individual to protect their privacy.
- **Privacy must be embedded and integrated:** it should be included in the design of all systems, services, products, and business practices. Ensure data protection forms part of the core functions of any system or service – essentially, it becomes integral to these systems and services.
- **Privacy and security have equal importance in everything we do:** we should give privacy and security equal weight and look to incorporate all legitimate objectives whilst ensuring we comply with our obligations. No unnecessary trade-offs need to be made to achieve both privacy and security. We will look for full functionality of privacy by design and by default in everything that we do, rejecting trade-offs from the outset that negatively impact privacy and security in order to achieve other objectives e.g. design, technical, cost etc. We should always be striving for the win-win situation in this and be looking to accommodate all objectives in an innovative, and creative manner.
- **Security should be end-to-end throughout the entire lifecycle of personal data:** We must put in place strong security measures from the beginning and extend this security throughout the 'personal data lifecycle' – i.e. process personal data securely and then destroy it securely when you no longer need it.
- **Visibility and transparency are maintained:** stakeholders should be assured that business practices and technologies are operating according to objectives and subject to independent verification. We must ensure that whatever business practice or technology we use operates according to its premises and objectives and is independently verifiable. We must also ensure visibility and transparency to individuals, such as making sure they know what data we process and for what purpose(s) we process it.

## 3.2 Technical and Organisational Measures

The University will implement appropriate technical and organisational measures that are designed:

a) to implement the Data Protection Principles in an effective manner, and
b) to integrate into the processing of personal data the safeguards necessary for that purpose.

This will apply at the time of determining the means of processing personal data, and at the time of actually processing it.

In doing so, the University will take into account the available technical and organisational measures, the cost of implementation and the nature, scope, context and purposes of processing of personal data, as well as the risks of varying likelihood and severity for rights and freedoms of individuals presented by the processing of their personal data.

Where significant amounts of personal data processing is proposed or where the processing presents a **high risk** to individuals, a DPIA must be carried out in accordance with the University's procedures.

## 3.3 Privacy by Default

The University will apply appropriate technical and organisational measures to ensure that, by default, only the personal data that is used is **necessary** for each specific purpose of personal data processing in relation to:

a) the amount of personal data collected;
b) the extent of processing that personal data;
c) the period of its storage; and
d) its accessibility.

The University's aim is that by default personal data access will be restricted to those who have a business need to know.

## 3.4 Data Protection by Design

### 3.4.1 Personal Data Processing Proposals

The University's aim is that when considering a proposal involving any processing of personal data, whether for research or service / product development, the impact of this on the individuals affected must be considered, and that appropriate technical and organisational measures should be put into place to ensure that:

a) the Data Protection Principles of GDPR Article 5 are implemented; and
b) any risks to individuals' rights and freedoms are minimised.

The use and retention of personal data both internally and externally should be minimized. In the case of research datasets containing personal data, anonymised or partly/reversibly anonymised data should be used wherever possible.

### 3.4.2 Software Procurement and External Personal Data Transfers

When buying systems/software which involve personal data or considering transfers/sharing of personal data including use of the cloud, staff must evaluate the privacy and security of alternative solutions and vendors/partners during the

Procurement or Research Ethics process (whichever is applicable). The use of such systems/software should, to the maximum extent possible, avoid personal data being involved, or at a minimum present low risk of data breaches occurring. Personal data should only be placed on systems, devices or software where this is compliant with University policies and the legislation.

Managers or staff should not purchase or download new systems or software, or arrange services, without first reviewing their proposed use in terms of a Data Protection Impact Assessment if the proposed use involves processing a significant amount of personal data or presents a high risk to individuals. Procurement must also be involved to ensure data processing, data sharing, and international data transfer agreements, where appropriate, are drawn up to govern processing of University controlled personal data by external suppliers / partners.

### 3.4.3 Data Protection as Business-As-Usual

Staff must be continually vigilant to ensure the security of University personal data and to avoid risks of personal data breaches arising from all University devices, systems, and log-ins. Staff must not download identifiable personal data outside the University's systems, and must only process personal data in compliance with appropriate University guidance and policies. Reviews of, and improvements to, data protection in business areas should be undertaken regularly by staff in their areas of work, documented, and privacy risks and precautions reviewed by staff regularly.

## 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; Individual Rights Policy; Information Management Policy; Information Retention and Disposal Policy; Information Security Policy |
| Procedures | N/A |
| Guidelines | Glossary \| ICO; University Intranet Guidance on Data Protection; |
| Local Protocol | N/A |
| Forms | Data Protection Impact Assessment; 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, 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.ac.uk.

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

## Appendix: Examples of Risk Mitigation Techniques

Non-exhaustive examples of techniques which may be used to achieve the aims of Privacy by Design and Default include

- undertaking University-required data protection training and refresher training modules;
- maintaining awareness of data security and threats such as 'phishing' attacks and other scams;
- carefully considering email recipients, and avoiding emails to multiple recipients wherever possible;
- avoiding the storage of spreadsheets containing personal data (anonymise and delete after use) minimisation of collecting, storing, using and transmitting personal data used;
- regular deletion of personal data after completion of purpose of processing or retention period;
- full and irreversible anonymisation of personal data;
- regular checks to ensure personal data accuracy;
- pseudonymisation;
- encryption e.g. of spreadsheets and other documents;
- filing personal data in SharePoint/Teams and never using Outlook as a storage medium;
- always sharing files via the SharePoint/Teams functionality, and never attaching files to emails
- ensuring transparency for data subjects by Privacy Notice;
- restricting staff access to personal data to those with a need to know, e.g. by using the "manage access" functionality in SharePoint/Teams.

Another potential technique which may be helpful for research datasets, provided that the number of individuals in the dataset is large enough, may be to generate a dataset composed entirely of identity-disguised (pseudonymised) or 'fictional' individuals which can retain the statistical properties of the original dataset. Care needs to be taken however, that identity cannot be inferred from combined data of identity disguised individuals.

Researchers should also consider using entirely fictionalised "dummy" data if available (e.g. from medical data sources) in order to avoid the need for processing real personal data at all.