Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Data Protection Policy
Version 2.0

Revision History:

Date of this revision	17 February 2025
Date of next review	17 February 2028
Version Number/Revision Number	2.0
Revision Date	February 2025
Summary of Changes	- The thrust of the Policy is the same, but it has been rewritten and reformatted to provide for greater clarity and usability. - Amendment of section entitled Education and Awareness to require staff to undertake data protection training - Inclusion of new section entitled Other Relevant Legislation - Review period of 3 years.
Changes Marked	No
Date of this revision	13 April 2022
Date of next review	13 April 2023
Version Number/Revision Number	1.0
Summary of Changes	New Policy
Changes Marked	n/a

Consultation History:

Number/ Revision Number	2.0
Consultation Date	27 January 2025
Names of Parties in Consultation	Audit & Risk Committee
Summary of Changes	No changes proposed
Consultation Date	18 November 2024
Names of Parties in Consultation	UPT
Summary of Changes	Review period of 3 years (unless changes required in meantime).
Consultation Date	12 September 2024
Names of Parties in Consultation	Relevant Academic & PMSS Unions
Summary of Changes	Minor changes to phraseology
Number/ Revision Number	2.0
Consultation Date	09 September 2024
Names of Parties in Consultation	UPT
Summary of Changes	- The thrust of the Policy is the same, but it has been rewritten and reformatted to provide for greater clarity and usability. - Amendment of section entitled Education and Awareness. - Inclusion of new section entitled Other Relevant Legislation.

Number/ Revision Number	1.0
Consultation Date	March-April 2022
Names of Parties in Consultation	Corporate Governance & Data Protection Project Steering Committee
Summary of Changes	New Policy

Approval:

This document requires the following approvals:

Version:	2.0
Approved By:	Governing Body
Date:	17 February 2025
Approved By:	Audit & Risk Committee
Date:	27 January 2025
Approved By:	University Planning Team (UPT)
Date:	18 November 2024
Version:	1.0
Approved By:	Governing Body
Date:	13 April 2022

Quality Assurance:

Version	2.0
Date Approved	17 February 2025
Date Policy to take effect	17 February 2025
Date Policy to be reviewed	17 February 2028
Version	1.0
Date Approved	13 April 2022
Date Policy to take effect:	13 April 2022
Date Policy to be reviewed:	13 April 2023
Written by:	Information Compliance Manager/DPO
Approved by:	Governing Body Audit & Risk Committee
Approving Authority	Governing Body
Head of Function responsible	VP for Finance & Corporate Services
Reference Documents:	Data Protection Policy v1.0 GDPR and Data Protection Act

Document Location:

Website – Policies and Procedures	Yes
Website – Staff Hub	Yes
Website – Student Hub	Yes
Other: - Internal Use Only	No

This Policy was approved by the Approving Authority on **17 February 2025**. It shall be reviewed and, as necessary, amended by the University every three years or at such time as is deemed necessary or if there has been a material change to any legislation or national guidelines informing this policy area. All amendments shall be recorded on the revision history section above.

Note: Prior to publication and dissemination of policies and procedures, documents must be reviewed for accessibility as part the University's commitment to Equality, Diversity, and Inclusion (EDI). Further advice on accessibility can be obtained from the EDI Team.

Table of Contents

1. Overview / Introduction

As a Data Controller, Atlantic Technological University ("ATU" / "The University") processes personal data relating to students, staff and other individuals ("data subjects"). The EU General Data Protection Regulation ("GDPR") and the Irish Data Protection Act 2018, collectively referred to as "data protection legislation", impose responsibilities on the University and grant rights to individuals in respect of their own personal data.

2. Purpose of Policy

This Policy is a statement of ATU's commitment to comply with data protection legislation. It sets out the responsibilities of all managers, employees, students, researchers, contractors, and anyone else who processes personal data in the course of their work / study with the University.

3. Definitions

"Personal Data" means any information relating to an identified or identifiable living individual.

"Special Categories of Personal Data" relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

A "Data Controller" is an entity that determines the purposes and means of processing personal data.

A "Data Processor" is an entity that processes personal data on the instructions of the Data Controller and does not exercise responsibility or control over the personal data.

"Processing" means any operation which is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms 'Process' and 'Processed' are construed accordingly.

The "EEA" comprises the EU member states plus Iceland, Liechtenstein, and Norway

Data is "anonymised" when individuals are no longer identifiable. Where data has been anonymised,

the original information shall be securely deleted to prevent any reversing of the anonymisation process. The data is therefore no longer considered personal data. In most cases, if this deletion does not take place, then the data is classified as “pseudonymised” rather than “anonymised” and is still considered personal data.

“Data Protection Commission (DPC)” is the supervisory authority in Ireland responsible for upholding the fundamental rights of EU individuals to have their personal data protected.

4. Scope

This Policy covers all processing activities involving personal data and special categories of personal data whether in electronic or physical format.

This Policy applies to:

- any person who is employed or engaged by the University who processes personal data in the course of their employment or engagement;
- any student of the University who processes personal data not already in the public domain in the course of their studies or research activities;
- individuals who are not directly employed by the University, but who are employed by contractors (or sub-contractors) and who process personal data in the course of their duties for the University;
- people on placement, visiting students and researchers, volunteers, etc;
- members of ATU’s Governing Body in the course of their duties.

This Policy applies to all locations from which University personal data is processed.

5. Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

University Planning Team (UPT)

The UPT is responsible for:

- Reviewing and approving this Policy and any updates to it, prior to submission to the Governing Body for final approval.

- Ensuring adequate resources are provided to safeguard compliance.
- Instigating audits of data protection matters of interest where appropriate.
- Implementing the internal controls of ATU, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk.

Senior Managers

Senior Managers are responsible for:

- Monitoring ongoing compliance with data protection legislation in their respective areas of responsibility and signing a statement as part of the University's Annual Statement of Internal Control to that effect.

Staff (and others as listed in Section 4)

ATU staff (and others as listed in Section 4) are responsible for:

- Reading, understanding and adhering to this Policy and related procedures.
- Contacting the ICO for more information as necessary.

So that staff are aware of their responsibilities, data protection training is provided.

VP for Finance & Corporate Services (or President's Nominee)

The VP for Finance & Corporate Services is responsible for:

- Overseeing the work of the Information Compliance Office.
- Acting as an advocate for data protection within the University.
- Monitoring and reviewing all aspects of compliance with data protection obligations.

Information Compliance Office (ICO)

The Information Compliance Office, under the direction of the Information Compliance Manager/DPO, is responsible for:

- Informing and advising the University of its data protection obligations.
- Monitoring compliance with data protection legislation and with this Policy and related procedures, in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

- Providing advice, where requested, in relation to Data Protection Impact Assessments (DPIAs) and monitoring their performance.
- Cooperating with the Data Protection Commission (DPC).
- Acting as the contact point for the DPC on issues relating to data processing.
- Providing regular reports to the UPT on data protection matters.

ICO Contact Details: dataprotection@atu.ie

6. Principles of Data Protection

ATU undertakes to perform its responsibilities in accordance with data protection legislation. In so doing, the University has due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The University is responsible for complying with the Data Protection Principles which state that Personal Data shall be:

- Processed lawfully, fairly and in a way that is transparent to the data subject ("lawfulness, fairness and transparency");
- Collected, created or processed only for one or more specified, explicit and lawful purpose ("purpose limitation");
- Adequate, relevant and limited to what is necessary for those purposes ("data minimisation");
- Kept accurate and, where necessary, up-to-date ("accuracy");
- Retained no longer than is necessary ("storage limitation");
- Kept safe and secure ("integrity and confidentiality").

The University must be able to demonstrate this compliance ("accountability").

6.1 Lawfulness, Fairness and Transparency

At least one of these legal bases (per Article 6 GDPR) shall apply whenever Personal Data is processed:

(a) **Consent**: the data subject has given clear consent for their personal data to be processed for a specific purpose. Consent is only valid when it's specific, informed, freely given and demonstrated by a clear affirmative action. As it can be withdrawn at any time, the University shall not normally rely on consent for core activities, but rather identify an alternative justification

for processing.

(b) **Contract**: the processing is necessary for a contract with the individual, or because the individual is taking steps to enter into a contract.

(c) **Legal obligation**: the processing is necessary for compliance with the law.

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary to perform a task in the public interest or for the official functions of the University, for example under the TU Act 2018.

(f) **Legitimate interests**: the processing is necessary for the legitimate interests of the University or a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. As a public body, the University cannot rely on this legal basis for processing personal data in the performance of its official tasks. When relying on this legal basis, a Legitimate Interest Assessment (LIA) shall be necessary.

Regarding Special Categories of Personal Data, not only shall one of the above legal bases be required, but the processing shall only take place in exceptional circumstances (per Article 9 GDPR), including for example where:

- the individual has given their explicit consent for their sensitive data to be processed.
- the processing is necessary for the University to fulfil its obligations in the context of employment, social security and social protection.
- the processing is necessary in the context of the provision of health or social care.
- the processing of sensitive data is necessary for matters of archiving purposes in the public interest, or for scientific, statistical, historical, or research purposes.

Information about a person's criminal convictions or offences shall be processed carefully in line with the National Vetting Bureau (Children and Vulnerable Persons) Act 2012 and Section 55 of the Data Protection Act 2018.

To ensure fairness and transparency, the University provides data subjects with Privacy Notices containing information about how their personal data is processed.

6.2 Purpose Limitation

The University shall process personal data for specified, explicit and legitimate purposes. Personal data shall not be processed for purposes that are incompatible with the initial purposes.

6.3 Data Minimisation

The University shall process personal data which is adequate, relevant and limited to what is necessary to accomplish a specified purpose. The University shall periodically review its processing to ensure that the personal data held is still relevant and adequate and is the minimum needed for their purposes. Personal data shall not be collected or held on a 'just in case' basis. Personal data no longer required shall be securely deleted/destroyed.

6.4 Accuracy

The University shall take measures to ensure that personal data is accurate and up to date.

6.5 Storage Limitation

Personal data shall only be retained for the period for which it is required, after which personal data shall be deleted or anonymised per the University's Data Retention Schedule.

6.6 Integrity & Confidentiality (Security)

The University shall ensure that personal data is kept safe and secure by taking appropriate physical, technical and organisational measures including, for example, access controls, logs / audit trails and encryption.

7. Demonstrating Compliance with Principles of Data Protection

The University shall demonstrate its compliance with the Principles of Data Protection.

7.1 Legal Basis

The University shall determine the appropriate legal basis as per Section 6.1 before beginning to process personal data. This basis shall be documented in relevant Privacy Notices and Records of Processing Activities (ROPAs).

7.2 Privacy Notice

When carrying out an activity that is not covered by the main University Privacy Notices, the relevant department shall produce a separate Privacy Notice for provision to data subjects at the time the personal information is collected or at the time consent is sought. Privacy Notices shall use clear language and outline:

- Types of personal data processed
- Purpose for processing the data
- Legal basis for processing the data
- Third parties with whom the personal data is shared
- Retention period of the data
- Data subject rights.

7.3 Record of Processing Activities (ROPA)

ROPAs contain the details of the personal data processed, the purpose of the processing, the categories of data subjects, the categories of recipients to whom the data is disclosed, including any transfers to third countries outside the EU, and information regarding retention periods.

Each unit within the University shall maintain a ROPA and the advice of the ICO shall be sought where necessary.

7.4 Data Protection by Design and by Default

The University shall consider “data protection by design” when selecting services and products to use in data processing activities. Data privacy features and data privacy enhancing technologies shall be implemented directly into the design of projects at an early stage.

The University shall ensure that user service settings are automatically data protection friendly (e.g. no automatic opt-ins), and that only data which is necessary for each specific purpose of the processing shall be gathered.

7.5 Data Protection Impact Assessment (DPIA)

An important part of integrating “data protection by design and by default’ is via a Data Protection Impact Assessment (DPIA). A DPIA is a process designed to identify the data protection risks associated with a new activity or technology and to minimise those risks as much as possible, as early as possible.

Under the GDPR, a DPIA is mandatory where data processing “is likely to result in a high risk to the rights and freedoms of natural persons”. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool in demonstrating compliance with data protection legislation. The DPC provides comprehensive information on DPIAs at https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

The University shall carry out DPIAs as required and the advice of the ICO shall be sought where necessary.

7.6 Third Party Due Diligence

The University shares personal data with third parties for multiple reasons. The data sharing may be to another Data Controller for joint purposes (e.g., another institution to administer joint programmes), or to a Data Controller for their own purposes (e.g., the HEA for statistical analysis purposes), or to a Data Processor to process data on behalf of the University (e.g., Microsoft for software provision).

This sharing shall be documented in relevant Privacy Notices and only occur where there's a legal basis to do so, for example where:

- the University is legally obliged to share the personal data with external agencies (e.g., Revenue), or
- the sharing is in the performance of a task in the public interest, or
- the data subject consents to the sharing, etc.

Where required, the University shall put in place written agreements with such third parties which clearly set out the responsibilities and liabilities of both parties. The ICO shall be consulted on such agreements well in advance of initiating any new data sharing arrangements.

Parents/Guardians are third parties and any sharing of data with them shall only be done on the basis of consent from the student, except in exceptional circumstances, for example in the case of potential danger to the health or well-being of a student, their personal data may be disclosed without consent.

7.7 Data Transfers

Processing by third parties frequently results in the transfer of personal data to third countries outside the European Economic Area (EEA). The University shall ensure that any personal data transferred to third countries is adequately protected in accordance with Chapter V of the GDPR (e.g. on the basis of an adequacy decision, or pursuant to a set of Standard Contractual Clauses). This includes personal data stored in the cloud as such infrastructure may in part be located outside of the EEA.

The University shall put in place written agreements and safeguards to protect the personal data being transferred. Where relevant, an evaluation of the laws and practices of the data protection regime of the third country shall be carried out via a Transfer Impact Assessment (TIA). Supplementary measures to

protect the personal data shall be implemented, where necessary.

The ICO shall be consulted well in advance of engaging any third party that transfers personal data outside the EEA. Advice shall be obtained from external experts / legal where necessary.

7.8 Data Subject Rights

The GDPR provides the following rights to Data Subjects:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Right to data portability
- Right to object
- Right not be subject to a decision based solely on automated processing.

The University shall facilitate the exercise of these rights by data subjects in accordance with the "Data Subject Rights Procedure".

7.9 Data Breaches

Where a gap in physical, technical or organisational measures leads to an incident of accidental, unauthorised, or unlawful disclosure, loss, alteration destruction or damage to individuals' personal data, such incidents shall be reported immediately to the ICO via dataprotection@atu.ie

The University shall manage and record such breaches in accordance with the "Data Breach Procedure".

7.10 Education and Awareness

Staff are required to undertake Data Protection Training as provided by the ICO. Additional guidance is provided to staff via the ICO SharePoint Site.

8. Other Relevant Legislation

The University shall adhere to other relevant legal and regulatory requirements, including:

- The **ePrivacy Regulations 2011** protect the confidentiality of electronic communications and

contain requirements relating to electronic marketing. Unless the similar products and services exemption applies, the prior consent of subscribers is required before marketing to individuals by e-mail. The possibility to opt out must be provided in the initial communication and at every subsequent communication. Consent is needed for the use of cookies unless the cookie is strictly necessary for the provision of a service to that subscriber or user.

- The **Health Research Regulations** provide for suitable and specific measures, including making 'explicit consent' the default safeguard, for the processing of personal data for the purpose of health research, unless researchers have obtained a "consent declaration" from the Health Research Consent Declaration Committee (HRCDC).
- The **Data Sharing and Governance Act 2019 (DSGA)** provides a legal basis for public-sector bodies to share data with one another and regulates how this can be done.
- The **EU AI Act** provides for the establishment of a harmonised legal framework for the regulation of certain types of AI systems and general-purpose AI models.

9. Policy Compliance/ Monitoring and Review

This Policy has been drafted to ensure the University meets its legal obligations. Breaches of this Policy may result in non-compliance by ATU with data protection legislation, which may result in fines or legal action being taken against the University. Compliance is not open to individual discretion and any breach of the Policy will be considered a serious matter and may include referral for investigation under the University's disciplinary procedures.

10. Supporting Documents

The Policy should be read in conjunction with relevant University policies, procedures and guidelines, including:

- Data Breach Procedure
- Data Subject Rights Procedure
- Records Retention Schedule
- CCTV Policy
- Acceptable Usage Policy
- Information Security Policy