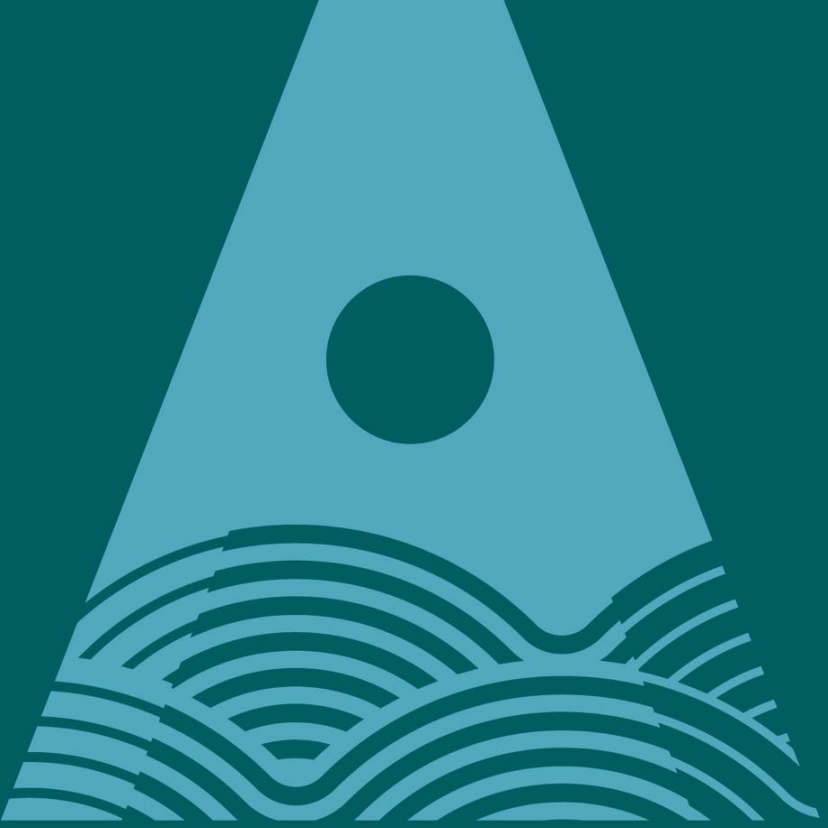


Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Data Protection Policy
Version 1.0

Revision History:

Date of this revision: 13th April 2022	**Date of next review:** 13th April 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changesmarked
1.0	13th April 2022	New Policy	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	N/a		

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	ATU Governing Body	13th April 2022

Quality Assurance:

Date Approved: 13th April 2022	Date Policy to take effect: 13th April 2022	Date Policy to be Reviewed: 13th April 2023
Written by:	CUA Data Protection and Governance PSC	
Approved by:	VP Finance and Corporate Services	
Approving Authority:	ATU Governing Body	
Head of Function responsible:	President ATU and President's Nominee	
Reference Documents:	Data Protection Policies of GMIT, LYIT, IT Sligo, and ATU	

Document Location:

Website – Policies and Procedures	X
Website – Staff Hub	X
Website – Student Hub	X
Other: - Internal Use Only	X

This Policy was approved by the Governing Body on 15th April 2022. It shall be reviewed and, as necessary, amended by the University annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1. Overview

Atlantic Technological University ('ATU' / 'The University') is responsible for the processing of a significant volume of personal data across each of its Faculties and Functions. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- All Staff are responsible for protecting and handling data in accordance with the data's classification.
- It is the responsibility of each Faculty and Function to ensure this personal information is processed in a manner compliant with the General Data Protection Regulation (GDPR), 2016/679 and the Data Protection Acts 1988-2018 [hereafter referred to as "data protection legislation"].
- Personal Data is considered Confidential Information and requires the greatest protection level.
- The University has an appointed Data Protection Officer ('DPO') who is available to Faculties and Functions to provide guidance and advice pertaining to this requirement.

The objective of this Data Protection Policy (Policy) is to set out the requirements of the University relating to the protection of Personal Data where it acts as a Data Controller and / or Data Processor, and the measures the University will take to protect the rights of Data Subjects, in line with EU legislation, and the laws of the other relevant jurisdictions in which it operates.

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

All staff are expected to:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this Policy;
- Read and understand this policy document;
- Understand what is meant by 'personal data' and 'sensitive personal data' and know how to handle such data;
- Not jeopardise individuals' rights or risk a contravention of data protection legislation; and
- Contact their Head of School / Function or Data Protection Officer if in any doubt.

2. Purpose

ATU is committed to complying with all applicable Data Protection, privacy and security laws and regulations (collectively referred to as requirements) in the locations in which it operates.

ATU has adopted this Data Protection Policy, which creates a common core set of values, principles and procedures intended to achieve a standard set of universal compliance parameters based on GDPR.

3. Definitions

See Appendix B for definitions used in this policy.

4. Roles and Responsibilities

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

Governing Body	To review and approve the policy on a periodic basis.
Executive Committee	The most Senior Executive Committee (to include any interim Executive Committee) is responsible for 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. The Committee is responsible for: • Reviewing and approving this Policy and any updates to it, prior to submission to Governing Body for final approval. • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility. • As part of the University's Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the GDPR. • Ensuring oversight of data protection issues either through their own work or the Data Protection Steering Committee. • To ensure adequate resources are provided to safeguard compliance. • To instigate investigations of data protection matters of interest where appropriate.
Data Protection Officer	• To lead the data protection compliance function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacyobligations. • To monitor and review all aspects of compliance with dataprotection and privacy obligations. • To act as a representative of data subjects in relation to theprocessing of their personal data and exercising their data subject rights. • To report directly on data protection risk and compliance toExecutive Management. • Oversee appropriate monitoring and auditing of Data Protection compliance. • To provide advice in relation to DPIAs. • To maintain relevant records. • To be the designated liaison person with the Data Protection Commission and to report any data protection breaches.
VP for Finance & Corporate Services or President's Nominee	• To lead the data protection compliance function. • To act as an advocate for data protection within the University. • To oversee the work of the DPO.

	• To monitor and review all aspects of compliance with data protection and privacy obligations.
Staff/Students/External Parties	To adhere to policy statements in this document. To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.

The University has designated a DPO who may be contacted as follows:

By email: dataprotection@atu.ie
By phone: 091 742 769

5. Scope

This policy covers all processing activities involving personal data and sensitive personal data (special categories of personal data) whether in electronic or physical format.

This policy applies to:

- Any person who is employed by ATU who receives, handles or processes personal data in the course of their employment.
- Any student of ATU who receives, handles, or processes personal data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process personal data on behalf of ATU.
- Officers and permanent staff of ATU Students Union.

This applies whether you are working in the University, travelling or working remotely.

6. Policy

It is the policy of ATU that all personal data is processed and controlled in line with the principles of GDPR and relevant Irish legislation.

ATU also embraces Privacy by Design and Privacy by Default principles in all its services and functions both current and future. This ensures that the public can maintain a high level of trust in ATU's competence and confidentiality while handling data.

This policy should not be viewed in isolation. Rather, it should be considered as part of the ATU suite of Data Protection policies and procedures.

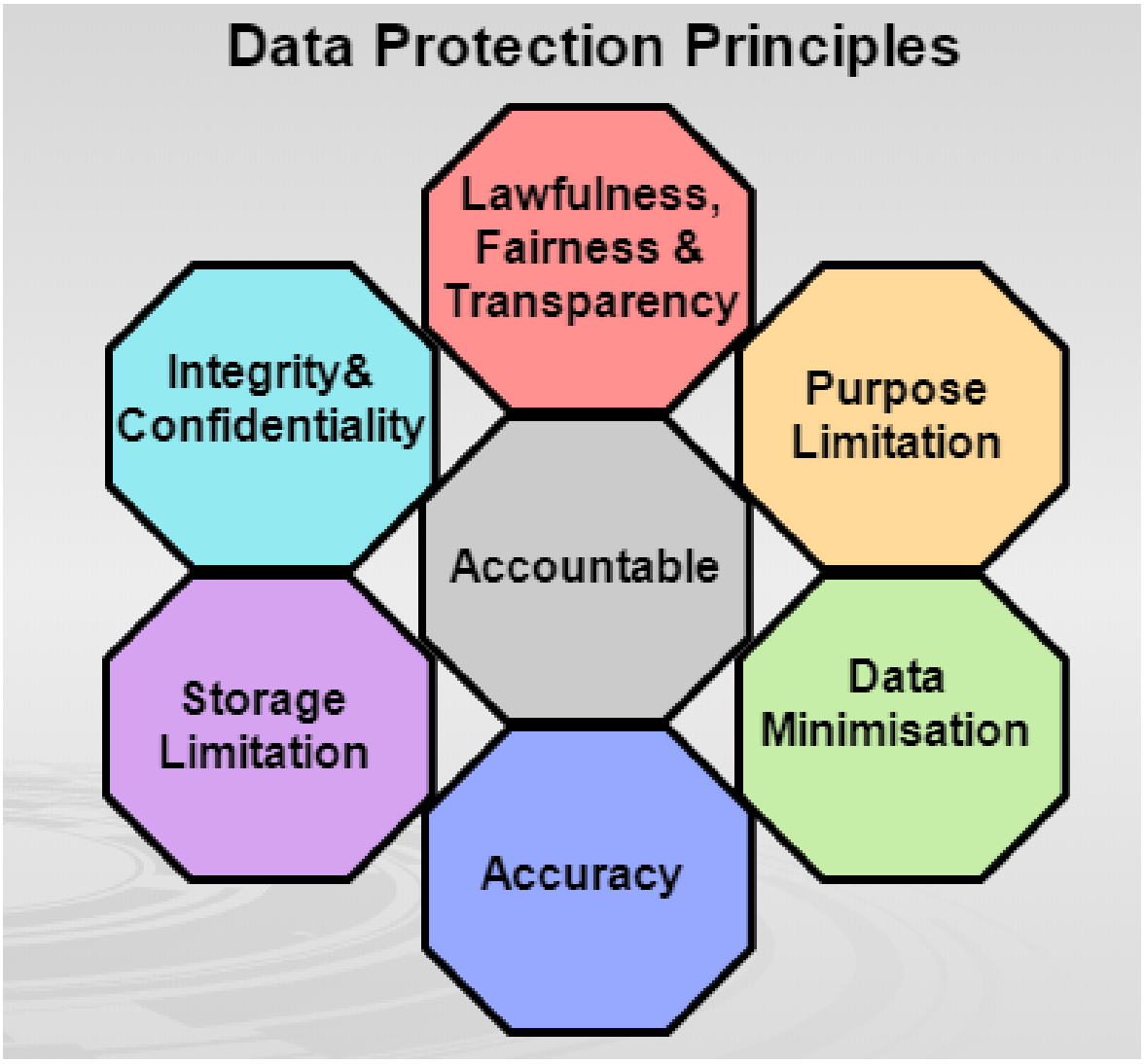
6.1 Personal Data Processing Principles

IMPORTANT NOTE: The following Data Protection requirements apply to all instances where Personal Data is stored, transmitted, processed or otherwise handled, regardless of geographic location.
The University is required to adhere to the six principles of data protection as laid down in the GDPR, which state:

1. Personal Data shall only be Processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
2. Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further Processed in any manner incompatible with those purposes (Principle of Purpose Limitation);
3. Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are Processed (Principle of Data Minimisation);
4. Personal Data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
5. Personal Data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the Personal Data are Processed (Principle of Data Storage Limitation);
6. Personal Data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
    a. prevent and / or identify unauthorised or unlawful access to, or processing of, Personal Data; and
    b. prevent accidental loss or destruction of, or damage to, Personal Data (Principles of Integrity and Confidentiality);

ATU, whether serving as a Data Controller or a Data Processor, shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability).

See diagram below for a visual representation of the principles:



6.2 Lawfulness of Processing / Legal Basis for Processing

The University shall conduct all Personal Data processing in accordance with legitimate GDPR based processing conditions:

- **Contract:** the processing is necessary for a contract the University has with the individual, or because they have asked the University to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for the University to comply with the law.
- **Public task:** the processing is necessary for the University to perform a task in the public interest or for the University to perform its official functions.
- **Consent:** the individual has given clear consent for the University to process their personal data for a specific purpose. Where consent is the legal basis for processing, the individual/area gathering the consent shall demonstrate that the consent is freely given, specific, informed and unambiguous and has been provided using a clear affirmative action. The data subject shall be made aware that consent can

be revoked at any time. The University will not normally rely on consent for core activities. Therefore, where possible the University should identify alternative justifications for processing. The University must obtain a consent for any new processing activity outside of initial consent.

- **Vital interests:** the processing is necessary to protect someone's life.
- **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.)
- The University will process Personal Data in accordance with the rights of Data Subjects. Moreover, the University will carry out communications with Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear language.
- The University will only transfer Personal Data to another group or Third Parties outside of the European Economic Area (EEA) in accordance with this Policy.

Special Categories Personal Data Processing

ATU will not process Special Categories of Personal Data (see Definitions) unless:

- Necessary to carry out the University's legal or statutory obligations
- The Data Subject expressly consents
  and / or
  Necessary to carry out Data Controller's obligations or exercise Data Subject's specific rights in the field of employment and social security and social protection law
  and / or
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

ATU may only process such data where necessary to protect a Data Subject's vital interest in the event that this subject is physically or legally incapable of giving Consent. For example, this may apply where the Data Subject may require emergency medical care.

ATU may process special categories of personal data where conditions are met under Article 9 GDPR and Recital 52 GDPR.

6.3 Transparency – Privacy Notices

To ensure fair and transparent processing activities, the University provides data subjects with a Privacy Notice to let them know what we are doing with their personal data when directly collecting data. Privacy notices shall be easily understood and contain specific information including:

- The types of personal data processed
- How the data is collected
- The purpose for processing the data
- The legal basis for processing the data
- Third parties with whom the personal data is shared
- Retention period of the data

- Data subject rights.

All privacy notices shall be drafted in consultation with the DPO and in accordance with the Privacy Notice Template.

The Privacy Notice will be:

- Provided at the first contact point with the Data subject or as soon as reasonably practicable.
- Provided in an easily accessible form.
- Written in clear language.
- Made in such a manner as to draw attention to the Privacy Notice.

If Consent is to be used as the legal basis for processing of personal data, Consent must be obtained at data collection point.

If we are carrying out an activity that is not covered by the main University Privacy Notices, Faculties and Functions will require a separate privacy notice to be provided at the time the personal information is collected or at the same time as consent is sought.

If consent is being sought or a privacy notice being prepared in relation to a new activity which could have an impact on the privacy of the individuals concerned then consideration should be given to carrying out a Data Protection Impact Assessment (DPIA).

The Privacy Notices content and mechanism requires prior DPO approval in consultation with the Head of Faculty or Function.

6.4 Data Minimisation

The University shall process personal data which is adequate, relevant and limited to what is necessary to accomplish a specified purpose. This is particularly important for special category or criminal offence data.
Data owners shall periodically review their 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.

6.5 Data Use Limitation

Faculties and Functions must only collect Personal Data for specified, explicit and legitimate purposes. Faculties and Functions are prohibited from further Processing unless these units have identified legitimate Processing conditions and documented same as per Section 6.3 of this policy or if the Personal Data involved is appropriately Anonymised and / or Pseudonymised and used for statistical purposes only.

6.6 Data Accuracy

Each Faculty and Function must ensure that any collected Personal data is complete and accurate subject to limitations imposed by University / Third Party contractual provisions.

In addition, each Faculty and Function must maintain Personal Data in an accurate, complete and up-to-date form as its purpose requires.

Each Faculty and Function shall correct incorrect, inaccurate, incomplete, ambiguous, misleading or outdated information without prejudice to:

- Fraud prevention based on historical record preservation.
- Legal Claim establishment, exercise or defense.
- Document Retention policy or other internal procedure.

6.7 Data Storage Limitation

Faculties and Functions must only keep Personal Data for the period necessary for permitted uses and as permitted under the University's approved Data Retention Schedule.

6.8 Security of Personal Data

Information Security

Each Faculty and Function shall ensure Personal Data security through appropriate physical, technical and organisational measures. These security measures should prevent:

- Alteration
- Loss
- Damage
- Unauthorised processing
- Unauthorised access.

Unauthorised Disclosure

No ATU employee or agent shall disclose Data Subject's (strictly) confidential information (including Personal Data or Special Categories of Personal Data) unless this Policy allows such disclosures.

Staff must report all suspected incidents of unauthorised access to the DPO. Incidents include disclosure, loss, destruction or alteration of (strictly) confidential information, regardless of whether it is in paper or electronic form.

6.9 Privacy by Design, Data Protection by Design and Data Protection by Default

The University has an obligation under GDPR to consider data privacy throughout all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

This is of particular importance when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

Privacy by Design means that any system, process or project that collects or processes personal data must build privacy into the design at the outset and throughout the entire lifecycle.

Privacy by Default states that the strictest privacy settings should apply by default to any new service or process without requiring the data subject to make any changes.

6.10 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is designed to assist the University in assessing the risks associated with data processing activities that may pose a high risk to the rights and freedoms of individuals and is a requirement of the GDPR.

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed to enable the University to evaluate and address the likely impacts of new initiatives and put in place appropriate measures to minimise or reduce the risks (including non-implementation).

Data Protection Impact Assessments are required under GDPR under certain circumstances including:

- when the processing of personal data may result in a high risk to the rights and freedoms of a data subject
- processing of large amounts of personal data,
- processing of special categories of personal data,
- where there is automatic processing/profiling

Faculties and Functions are required to conduct a Data Protection Impact Assessment (DPIA) where appropriate and then consult with the DPO.

6.11 Record of Processing Activities

The University as a data controller is required under GDPR to maintain a Record of Processing Activities (ROPA) under its responsibility. That record shall contain details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU.

New activities involving the use of personal data and that is not covered by one of the existing Records of Processing Activities require consultation with the Data Protection Officer prior to the commencement of the activity.

The DPO will review records of processing periodically and will update same accordingly, in consultation with the Data Controller. The DPO will provide Processing Activity records to a supervisory authority on request.

6.12 Data Sharing

Sharing with a Third Party or External Processor

As a general rule personal data should not be passed on to third parties however, the University shares

personal data about applicants, students, staff, alumni, research participants and others with third parties (outside the University) for multiple reasons. This sharing shall occur only 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.

The data sharing may be:

a) To a third party for joint purposes (e.g., to another institution to administer joint programmes);
b) To a third party for that party's own purposes (e.g., to the HEA for statistical analysis purposes);
c) To a third party to process data on behalf of the University (e.g., to Microsoft for software provision, to CCTV companies for surveillance, to a document storage company for archiving, etc.). This third party is known as a Data Processor.

This sharing will be documented in relevant privacy notices.

Data owners will ensure that personal data is shared securely (e.g., by encrypted file transfer, password-controlled access rights or by tracked/signed-for post or courier delivery).

The University will continue to put in place agreements and contracts with such third parties, clearly setting out the responsibilities and liabilities of both parties. The DPO should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

Sharing Personal Data with Parents/Guardians

The University will not disclose the personal data of students, regardless of age, to parents/guardians unless the student has provided his/her consent. The University's preference is to receive written consent by way of an email from the student, where possible. In exceptional circumstances, for example in the case of potential danger to the health or well-being of a student, a student's personal data may be disclosed without consent.

Transfer of Personal Data outside the EEA

Transfers of personal data to third countries are prohibited without certain safeguards. The means the University must not transfer data to a third country unless there are adequate safeguards in place which will protect the rights and freedoms of the data subject. It is important to note that this covers personal data stored in the cloud as infrastructure may be in part located outside of the EU.

Faculties and Functions must not transfer Personal Data to a Third Party outside of the EEA regardless of whetherthe University is acting as a Data Controller or Data Processor unless certain conditions are met.
The DPO must be consulted prior to any Personal Data transfer outside the EU and must record the determination in writing.

6.13 Education and Awareness of Data Protection

The University is committed to the provision of data protection training.

Faculties and Functions must ensure that all staff are trained on relevant Privacy, Data Protection and Information Security requirements. In addition to General Data Protection Regulation training staff may receive additional training when applicable to their duties or position. ATU will maintain employee training completion records.

6.14 Subject Access Request (SAR)

The University processes certain personal data relevant to the nature of the employment of its employees, students and, where necessary, to protect its legitimate business interests. As such the University is the Data Controller for such personal data.

The GDPR gives data subjects the right to access personal information held about them by the University. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that the University holds about them which may include copies of email correspondence referring to them.

Data Subject Rights:

- Data subjects will be able to request to access the data the University holds on them through a Subject Access Rights Request (SAR) (Right of Access);
- Data subjects can request to change or correct any inaccurate data (Right to Rectification);
- Data subjects can request to delete data that the University holds (Right to Erasure (sometimes referred to as the Right to be Forgotten));
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to have their data moved outside of the University if it is in an electronic format (Right to Data Portability);
- Data subjects can object to a decision made by automated processing and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

Requests for personal information will normally be free of charge, however, the University reserves the right where requests from a data subject are manifestly unfounded or excessive in nature to either:

- Charge a fee to cover the administrative costs of providing the personal data.
- Refuse to act upon the request.

The University may also refuse to act upon a subject access request under GDPR in the following circumstances:

- Where it would breach the rights of someone else.
- Where it is the subject of an ongoing legal case.
- It would be illegal to do so.
- The identity of the requester cannot be determined.

7. Policy Compliance

7.1 Compliance

Breaches of this policy may result in non-compliance by the ATU with Data Protection Legislation which may

result in fines or legal action being taken against the ATU.

7.2 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University ’s disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the Data Protection Officer.

Appendix A – Supporting Documents

The below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Data Protection Procedures
- Data Retention Schedule
- Data Protection Incident Response & Breach Notification procedures
- CCTV Policy
- Acceptable Usage Policy
- Information Security Policy

This Appendix will be reviewed periodically and may be amended to reflect the implementation of additional relevant policies within ATU.

Appendix B Glossary of Terms

Content	Content is information with relevant metadata that has a specific use or isused for a particular business purpose.
Records	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligationsor in the transaction of business.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. It must be demonstrated that the Data Subject has provided appropriate consent for data processing. The University must obtain a consent for any newprocessing activity outside of initial consent.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title and description, • Tags and categories, • Who created and when, • Who last modified and when, • Who can access or update.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by ATU: Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of an individual student file or HR file • An Examination Script • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour anddiscipline.
Sensitive PersonalData	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person'sracial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.
Data	Data as used in this Policy shall mean information which either: • is processed by means of equipment operating automatically inresponse to instructions given for that purpose;

	• is recorded with the intention that it should be processed by means ofsuch equipment; • is recorded as part of a Relevant Filing System or with the intentionthat it should form part of a Relevant Filing System; • Does not fall within any of the above, but forms part of a ReadilyAccessible record. • Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of aRelevant Filing System.
Data Controller	Means a person or organisation who (alone or with others) determines thepurposes for which and the manner in which any Personal Data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, ora Faculty or Function within a University which is Processing Personal Data for the University as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor. It is possible for one University or person to be both a Data Controller and aData Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the University is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Third Party	Means an entity, whether or not affiliated with ATU, that is in a business arrangement with ATU by contract, or otherwise, that warrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where ATU has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data. All other terms used in this Policy and any documents issued in support of thisPolicy, not referenced in this Glossary of Terms section, shall have the same meaning as the GDPR and/or local requirements.

Data Protection Commissioner	Means the office of the Data Protection Commissioner (DPC) in Ireland.
Data Subject	Refers to the individual to whom Personal Data held relates, including: employees, students, customers, suppliers.
EEA	European Economic Area Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any countrywithin this area.
GDPR	Means EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regardto the Processing of Personal Data and on the Free Movement of such Data.
Processing	Means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptationor alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms 'Process' and 'Processed' should be construed accordingly.
Anonymised	Means the process of making Personal Data Anonymous Data. 'Anonymise'should be construed accordingly.
Pseudonymisation	Means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is keptseparately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.