TUS

DATA COMPLIANCE

Data Protection Policy

2023.Pol.DataProtection

Revision History:

Date of this revision: 08 May 2023	Date of next review: May 2026

Version/ Revision No.	**Revision Date**	**Summary of Changes**	**Changes marked**
1.0	08 May 2023	New Policy	N/A

Consultation History:

Version Number/ Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
1.0	March – April 2023	IT Manager; Dean of Faculty Science and Technology, and Dean of Lifelong Learning, HR Manager	

Development and Approval Log:

Responsible for:	**Title**
Policy Developer:	Information and Data Compliance Office
Policy Owner:	Vice President Finance and Corporate Governance
Recommended by:	Legislative
Approving Authority:	TUS Governing Body
Reference Documents:	N/A

Approval:

Version	**Approved By:**	**Date**
1.0	TUS Governing Body	08 May 2023

This Policy was approved by TUS Governing Body on 08 May 2023. It shall be reviewed and, as necessary, amended by the University annually. All amendments shall be recorded on the revision history section above.

Date Approved: 08 May 2023	**Date Policy to take effect: 08 May 2023**	**Date Policy to be Reviewed: May 2024**

Document Location:

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

Table of Contents

1. POLICY INTRODUCTION

TUS is responsible for the Processing of a significant volume of personal data across each of its Schools, 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 information in accordance with the information's classification.
- TUS has a Data Protection Officer ('DPO') and an Information and Data Compliance Officer (IDCO) which are available to Schools, Faculties and Functions to provide training, guidance and advice pertaining to this requirement.
- It is the responsibility of each School, Faculty and Function to ensure personal data is processed in a manner compliant with the relevant Data Protection Legislation and guidance.
- Personal Data is considered confidential information and requires the greatest protection level.

The objective of this Data Protection Policy ('Policy') is to set out the requirements of TUS relating to the protection of Personal Data where it acts as a Data Controller and / or Data Processor, and the measures TUS 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 sections, offices and staff are expected to:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy;
- Complete the Data Protection training provided by TUS.
- Read and understand this policy document;
- Process 'Personal Data' and 'Sensitive Personal Data' in line with this policy and as advised by the IDCO.
- Not jeopardise individuals' rights or risk a contravention of Data Protection Legislation; and
- In conjunction with the IDCO, carry out a Data protection impact assessment (DPIA) and prepare a privacy notice that is appropriate for the purpose, when implementing any new technologies, processes, or new collection/Processing of Personal Data.
- Where necessary seek direction from their Head of School/Faculty/Function or Information and Data Compliance Office to ensure that any Processing is compliant.

2. PURPOSE OF POLICY

TUS 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.

TUS 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 the GDPR and the Data Protection Act 2018.

3. SCOPE

This policy covers all Processing activities involving Personal Data and Sensitive Personal Data (special categories of Personal Data) whether in electronic, cloud based, or physical format.

This policy applies to:

- Any person who is an employee of TUS, who receives, handles or processes Personal Data in the course of their employment.
- Any student of TUS who receives, handles, or processes Personal Data in the course of their studies for administrative, research or any other purpose.
- Third parties (Data Processors/and or joint controllers) that receive, handle, or process Personal Data on behalf of TUS.

This applies whether you are working onsite in TUS, travelling or working remotely.

4. ROLES AND RESPONSIBILITIES

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

Governing Body	To review and approve the Policy at regular intervals. Through its Audit and Risk Committee (ARC) to receive standing reports on the operation of the Information and Data Compliance office and it's monitoring and control of Data compliance. As part of TUS's Annual Statement of Internal Control, signing a statement which provides assurance that the TU is compliant with Data Protection Legislation.
Audit and Risk Committee (ARC)	The ARC is responsible for: • Reviewing this Policy and any updates to it as proposed by the Information and Data Compliance Office. • Report on the operation of the Information and Data Compliance Office and its monitoring and control of Data protection.
Heads of Function in TUS	• To ensure compliance by staff within their function with this policy. • Ensuring ongoing compliance with Data Protection Legislation in their respective areas of responsibility. • To update and assist with the development of the record of Processing activities within their function.
Data Protection Officer	The registered DPO for TUS is the Vice President for Finance and Corporate Governance. The role of the DPO is to: • Direct the Information and Data Compliance Officer in relation to compliance requirements within TUS. • To provide guidance, direction, and support to the Information and Data Compliance Officer on all aspects of Data protection for the TU. • To act as owner of this Policy.
Information and Data Compliance Officer (IDCO)	Under the direction of the Data Protection Officer, the role of the IDCO is:

	• To lead the Data protection compliance and risk management function, with responsibility for advising on how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of Data protection and privacy obligations. • To monitor and review all aspects of compliance with Data protection and privacy obligations. • To act as a representative of Data Subjects in relation to the Processing of their Personal Data. • To report directly on Data protection risk and compliance to executive management. • Oversee appropriate monitoring and testing results of Data Protection compliance. • To update this policy as required and advise all staff of the requirements of the policy.
Staff/Students/External Members of TUS committees or panels	• To adhere to policy statements in this and other relevant documents. • To proactively engage with the requirements of this policy by developing a privacy first approach to daily tasks. • To report suspected breaches of policy to their Head of Department and/or Information and Data Compliance Officer. • To ensure safe practices around the Processing of Data with particular emphasis on electronic or cloud-based Data. • To exercise caution with communications, links and attachments within communications, the management of passwords, and anything else that can pose a risk or threat to University networks and Data repositories. • To avail of Cyber Security training and awareness and adhere to related University policies. • To ensure that all training offered by TUS is completed in a timely manner.

If you have any queries on the contents of this Policy, please contact the Information and Data Compliance Office at datacompliance@tus.ie.

5. POLICY STATEMENT

It is the policy of TUS that all Personal Data is processed and controlled in line with the principles of GDPR, the Data Protection Act 2018, and any other relevant legislation.

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

This policy should not be viewed in isolation. Rather, it should be considered as part of TUS's suite of Data Protection policies and procedures as listed in Appendix 1.

5.1 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.

TUS is required to adhere to the six principles of Data protection as laid down in the GDPR, which state:

1. **Lawfulness, Fairness and Transparency** - Personal Data shall only be processed fairly, lawfully and in a transparent manner;
2. **Purpose Limitation** - 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;
3. **Data Minimisation** - Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. **Accuracy** - Personal Data shall be accurate, and where necessary kept up to date;
5. **Data Storage Limitation** - 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;
6. **Integrity and Confidentiality** - 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;

TUS, 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).

5.2 Lawfulness of Processing

TUS shall conduct all Personal Data Processing in accordance with legitimate GDPR based Processing conditions in particular the following requirements under Article 6:

- the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes;
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The Technological University carries out many services and functions in the public interest and may rely on this as a lawful basis for the Processing of Personal Data.

Public Bodies are not encouraged to use Consent for the administration of Core Business Activities, due to the imbalance in the relationship between the controller and Data Subject. Where possible TUS should identify alternative justifications for Processing.

Where Consent is the basis for Processing of Personal Data then Schools, Faculties and Functions must demonstrate that the Data Subject has provided appropriate, traceable Consent for Data Processing by providing the Data Subject with the information required under Section 5.3 of the Policy. TUS must obtain a Consent for any new Processing activity, or purpose change, outside of initial Consent. It

should be understood that anyone who has provided Consent has the right to revoke their Consent at any time, without detriment to the Data Subject.

TUS will process Personal Data in accordance with the rights of Data Subjects. TUS will carry out communications with Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear, unambiguous, language.

TUS will only transfer Personal Data to another group or Third Parties outside of the European Economic Area (EEA) in accordance with Data privacy law and the guidance of National and European Data protection authorities.

A risk-based approach to Personal Data protection issues will be taken, in line with DPC guidance, and aligned to the TUS risk management policy and risk appetite statement.

Special Categories Personal Data Processing

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

- The Data Subject expressly Consents to the Processing
  and / or
- It is necessary to carry out TUS'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 performance of a function carried out by TUS by or under an enactment and / or
- Necessary for the purposes of preventative or occupational medicine including the assessment of the working capacity of an employee and / or
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

TUS may also process such Personal Data as necessary to protect the vital interest of the Data Subject or another natural person in the event that the Data Subject is physically or legally incapable of giving Consent (Article 6 (d) of the GDPR). For example, this may apply where the Data Subject may require emergency medical care.

Where a situation arises, which is not covered by this policy, but which is transparent to the Data Subject, and lawful, the Data Protection Officer, or their delegate, may authorise such Processing.

5.3 Transparency – Privacy Notices

To ensure fair and transparent Processing activities TUS is required to provide Data Subjects with a Privacy Notice to inform them about how their Data is being processed.

These Privacy Notices must:

- Be provided at the first contact point with the Data Subject when the Personal Data is being collected directly by TUS from the Data Subject or
- Be provided as soon as reasonably practicable, and at the latest within one calendar month, when TUS collects Personal Data from a Third Party (i.e. not directly from a Data Subject).
- Be provided in an easily accessible form.
- Be written in clear language.
- Be made in such a manner as to draw attention to the processing.

Privacy notices will contain the following information:

- What Personal data is collected.
- How the Personal Data is collected.
- Where the Personal Data is held.
- The Lawful bases for collecting and processing the Personal Data.
- Purposes for which the Personal Data is processed.
- Who the Personal Data is shared with, or who has access to the Personal Data.
- How long the Personal Data is retained.
- Data Subjects' rights and how to exercise them.
    - This can be in the form of a link to the TUS website page.
- Who the Data Subject can contact and how.

In some instances, the following additional information should be provided.

- How to make a complaint or object to the data processing.
- Changes to the privacy notice.

Where Consent is to be used as the lawful basis for Processing Personal Data then the Consent must be obtained at the point the Personal Data is being collected. The Data Subject must also be informed of each of the items listed on the headings of the privacy notice set out above.

The privacy notice's content and mechanism for distribution require prior consultation with the IDCO and with the Head of School, Faculty, or Function before it can be approved for distribution.

When TUS collects Personal Data from a Third Party (i.e. not directly from a Data Subject), the TUS must provide privacy notices to the Data Subject within a reasonable timeframe that is no more than 30 days post collection.

5.4 Data Minimisation and Data Use Limitation

Schools, Faculties, and Functions should only collect or use as much Personal Data as is necessary to accomplish a specific purpose, as set out in the relevant privacy notice.

Personal Data must only be collected for specified, explicit and legitimate purposes. The use of Personal Data for any additional purposes must be submitted to the IDCO for review to determine whether:

- the purpose is lawful and connected to the original purpose,
- additional action is required to enable the Processing to take place, or
- the Processing should not proceed because of insufficient lawful basis.

The use of aggregate, statistical Data is typically not considered to be Personal Data and therefore is not prohibited by anything in this policy. Care should be taken to remove any single or collective pieces of information in a Dataset, the combination of which may make an individual identifiable.

Personal Data can only be used for the purposes that are set out in the relevant privacy notice. Schools, Faculties and Functions are prohibited from further Processing unless these units have identified legitimate Processing conditions and documented same as per Section 5.3 of this policy or if the Personal Data involved is appropriately Anonymised and / or Pseudonymised and used for statistical purposes only.

5.6 Data Accuracy

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

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

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

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

5.7 Data Storage Limitation

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

5.8 Security of Personal Data

Information Security

Each School, 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 TUS employee or agent shall disclose a Data Subject's confidential information (including Personal Data or Special Categories of Personal Data), to a third party unless this Policy allows such disclosures. Employees should contact the IDCO for guidance.

5.9 Notification of Data Breaches

Data Protection Legislation identifies three categories of breaches:

- Confidentiality breach: unauthorised or accidental disclosure of or access to Personal Data;
- Availability breach: unauthorised or accidental loss of access to or destruction of Personal Data;
- Integrity breach: unauthorised or accidental alteration of Personal Data.

Any individual who accesses, uses or manages Personal Data is responsible for reporting Data breach incidents (breach) to their Head of School/Faculty/Function and the IDCO immediately.
The Data Protection Commissioner (DPC) must be notified of a breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

The DPC must be notified of the breach by TUS without undue delay and not later than 72 hours after becoming aware of the breach. It is therefore imperative that all breaches are notified internally immediately.

The DPO, in conjunction with the IDCO, Head of School/Faculty/Function will determine who needs to be notified of the breach. This may include the individuals affected by the breach and the Data Protection Commissioner.

Subsequent to any Personal Data breach, a full review of the causes of the breach and the effectiveness of the response will be carried out. The IDCO will provide a report on Data breaches to TUS's Audit and Risk Committee on a bi-annual basis.

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

TUS 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 the Processing of 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.

When implementing any new technologies, processes, or new collection/Processing of Personal Data, the IDCO must be contacted in order to carry out a Data protection impact assessment (DPIA) and prepare a privacy notice appropriate for the purpose.

5.11 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a requirement under Article 35 of the GDPR and is designed to assist in assessing the risks associated with Data Processing activities that may pose a high risk to the rights and freedoms of individuals.

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed to enable TUS 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, but not limited to, the following:

- When implementing new technologies or processes that engage the Processing of Personal Data
- 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 for a purpose other than that for which it was initially collected,
- Large scale Processing of special categories of Personal Data,
- Where there is automated Processing/profiling

Schools, Faculties and Functions are required to conduct a Data Protection Impact Assessment (DPIA) where appropriate in consultation with the IDCO.

5.12 Record of Processing Activities

TUS as a Data Controller is required under Article 30 of the GDPR to maintain a Record of the Processing Activities 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 Data is shared with and when Personal Data is transferred to countries outside the EU.

New activities involving the use of Personal Data which are not covered by one of the existing Records of Processing Activities require consultation with the IDCO prior to the commencement of the activity.

The IDCO will review Records of Processing Activities periodically and will update same accordingly, in consultation with the relevant Head of School/Faculty/Function. The IDCO will provide Records of Processing Activity to a supervisory authority on request.

5.13 Data Sharing

Sharing with a Third Party or External Agencies

As a general rule Personal Data should not be passed on to third parties, particularly if it involves special categories of Personal Data but there are certain circumstances when it is permissible for example:

- TUS may disclose Personal Data and Sensitive Personal Data/Special Category Data to external agencies to which it has obligations or a legitimate reason. Such sharing should be noted in the relevant Privacy Notice.
- The Data Subject gives consent for the sharing of the Personal Data.
- The Third Party is operating as a Data Processor and meets the requirements of the GDPR. Where a Third Party is engaged for Processing activities there must be a written contract, or equivalent, in place which shall clearly set out respective party responsibilities and must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

The IDCO should be consulted where a new contract, that involves the sharing or Processing of Personal Data, is being considered.

Transfer of Personal Data outside the EEA

Transfers of Personal Data to Third Countries are prohibited without certain safeguards. This means TUS 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 EEA.

Schools, Faculties and Functions must not transfer Personal Data to a Third Party outside of the EEA regardless of whether TUS is acting as a Data Controller or Data Processor unless certain conditions are met.

The IDCO must be consulted prior to any Personal Data transfer to a Third County. The IDCO will review the transfer details, draft appropriate agreements, and record the final determination in writing. Agreements may include but are not limited to; Standard Contractual Clauses, Article 46 of the GDPR, Binding Corporate Rules, Article 47 of the GDPR, or a record of the reasons why the derogations specified under Article 49 of the GDPR apply.

The Information and Data Compliance Office will carry out regular reviews of the Data transfers within the organisation to ensure compliance with national and European regulations.

A list of approved Third Countries – i.e. those with adequacy agreements aligning them with the GDPR is available here and at Appendix 3 of this document.

5.14 Education and Awareness of Data Protection

TUS is committed to the provision of mandatory Data Protection training to ensure all individuals are aware of their respective obligations under Data Protection Legislation. This is especially important for staff who handle Personal Data and / or Sensitive Personal Data in the course of their everyday business.

The IDCO will provide access to training in the GDPR for all staff members on a regular basis, no less than every three years. In addition to GDPR training, staff may receive additional training when applicable to their duties or position. The IDCO will maintain employee training completion records.

Schools, Faculties and Functions must also ensure that all staff are trained on relevant Privacy, Data Protection and Information Security requirements and contact the IDCO to provide additional training where a need is identified.

5.15 Data Handling and Clean Desk

TUS Records should be managed in a systematic, structured manner, and information security requirements should be maintained throughout the document lifecycle (i.e., creation, transmission, storage, modification, retention and destruction).
Protecting the integrity of confidential Data that resides within TUS is critical. To comply with GDPR regulations, Schools, Faculties and Functions are required to implement a data handling and clean desk strategy as part of their normal business practice.

5.16 Data Protection Audit

The IDCO will schedule and carry out regular audits to ensure compliance with the policy. System audits will be carried out in line with the TUS Data Access Management Policy. Physical audits will be scheduled and carried out within each School, Faculty, and Function to ensure compliance with section 5.15.

5.17 Data Subject Requests

The GDPR provides Data Subjects with a number of rights in relation to their Personal Data. These include the following:

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

Under the Right of Access, individuals can request to see any information that TUS holds about them which includes copies of email correspondence referring to them or opinions expressed about them. Requests for personal information will normally be free of charge, however, TUS reserves the right, under Article 12 (5) of the GDPR, 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.

TUS 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.
- Where it would be illegal to do so.
- Where the identity of the requester cannot be determined.

6. POLICY COMPLIANCE AND REVIEW

6.1 Compliance

Breaches of this policy may result in non-compliance by TUS with the relevant Data Protection Legislation which may result in fines or legal action being taken against TUS.

6.2 Non-Compliance

Failure to comply with this policy may lead to disciplinary action being taken in accordance with TUS'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.

6.3 Review

This policy will be subject to review every three years from the date of policy approval. Changes to requirements or legislative changes may require a review outside of this time frame.

Appendix 1: Supporting Documents

The list below sets out those policies and procedures that are to be used in conjunction with this Policy.

- Data Protection Procedures
- Data Retention Policy
- Data Retention Schedule
- TUS Computer Services Policies
  - Acceptable Usage Policy
  - Information Security Policy

Appendix 2: DEFINITIONS

Content	Content is information with relevant MetaData that has a specific use or is used for a particular business purpose.
Core Business Activities	The main business processes of TUS which enable the provision of Teaching, Learning, and Research and Development, and all ancillary activities.
Records	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
Consent	Means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to them. It must be demonstrated that the Data Subject has provided appropriate, traceable Consent for Data Processing. TUS must obtain a Consent for any new Processing 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 TUS. 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 • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour and discipline.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of Data which are defined as Data relating to a person's racial 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 in response to instructions given for that purpose;

	• is recorded with the intention that it should be processed by means of such equipment; • is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System; • does not fall within any of the above, but forms part of a readily accessible record. Data therefore includes any digital Data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes 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, or a School, Faculty or Function within an Institution which is Processing Personal Data for TUS 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 Institution or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether TUS 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 TUS that is in a business arrangement with TUS 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 TUS 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 this Policy, 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 Protection Legislation	Means the GDPR and the Irish Data Protection Acts 1988 - 2018
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 country within this area.
Third Country	Refers to a country outside the European Economic Area (the "EEA").
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 Regard to 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, 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' 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 kept separately 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.

Appendix 3: Third Countries with Adequacy Decisions

The European Commission has the power to determine, on the basis of article 45 of Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection.

The adoption of an adequacy decision involves:

- a proposal from the European Commission;
- an opinion of the European Data Protection Board;
- an approval from representatives of EU countries;
- the adoption of the decision by the European Commission.

At any time, the European Parliament and the Council may request the European Commission to maintain, amend or withdraw the adequacy decision on the grounds that its act exceeds the implementing powers provided for in the regulation.

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transmissions of data.

As of April 2023, The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection.

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

The adequacy list is updated as more applications are processed and approved, or where changes to the data protection laws of a particular country means that adequacy decision needs to be reviewed. An up to date list is available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.