Data Protection Policy

Document Reference and Version Number	V2
Purpose	To provide necessary information regarding handling of personal and special category personal data.
Commencement Date	Immediate – July 2021
Date of next Review	July 2026 subject to any changes in legislation
Who needs to know about this document	All Staff
Revision History	V1 – February 2018 V2 – July 2021
Policy Author	Information Officer
Policy Owner	Data Protection Officer, Directorate of Corporate Affairs

1 Overview

The members of Dun Laoghaire Institute of Art, Design and Technology (IADT)'s Executive and Management team have overall responsibility for ensuring compliance with Data Protection legislation. However, all employees and students of IADT who collect and/or control the content and use of personal data are also responsible for compliance with the Data Protection Acts.

The Institute provides support, assistance, advice and training to all faculties, offices and staff to ensure that they are in a position to comply with the legislation.

The Institute is responsible for the processing of a significant volume of personal information across each of its Departments/Faculties/Functions (Academic/Administrative/Research). 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 (See the Glossary in Appendix C for details).

IADT has appointed Mr. Bernard Mullarkey, Secretary/Financial Controller as Data Protection Officer (DPO). Contact c/o: dp@iadt.ie or 239 4947. He is available to provide guidance and advice pertaining to this requirement and will assist staff in complying with Data Protection legislation.

It is the responsibility of each Department/Faculty/Function to ensure this personal information is processed in a manner compliant with the relevant data protection legislation and guidance.

Personal data is confidential information and requires the greatest protection level.

The objective of this Data Protection Policy is to set out the requirements of the Institute relating to the protection of Personal data where it acts as a Data Controller and / or Data Processor, and the measures the Institute 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.

Any person who is employed, is a student of IADT or any external third party is expected to:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy which is supported by the Data Retention Schedule and procedures and;
- Read and understand this policy document;

- Understand what is meant by 'personal data' and 'special category or sensitive personal data' and know how to handle such data;
- Endeavour not to jeopardise individuals' rights or risk a contravention of the Act; and
- Contact the appropriate person which may include a Head of Department/Faculty/Function and/or the Information Officer or Data Protection Officer if in any doubt.

2 Purpose

IADT 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. The Irish Data Protection Act 2018 replaces and amends the DP Acts 1988 to 2003 and transposes the General Data Protection Regulation (GDPR) into Irish law.

IADT 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.

3 Scope

IADT needs to collect and use personal data (information) about its students, staff and other individuals who come into contact with the Institute for the purposes of:

- Recruitment and enrolment of students at undergraduate, postgraduate
- and part-time levels;
- Organisation and administration of courses
- Academic Quality Assurance, Evaluation and Examination
- Research activities
- Recruitment and payment of staff
- Compliance with statutory and legal obligations
- Procurement and Purchasing

This policy covers all processing activities involving personal data and special category personal data/sensitive personal data whether in electronic or physical form.

This policy applies to:

- Any person who is employed by the Institute who receives, handles or processes data in the course of their employment.
- Any student of the Institute who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process data on behalf of IADT.
- This applies whether you are in the Institute, travelling or working remotely.

4 Policy

It is the policy of IADT that all personal data is processed and controlled in line with the principles of GDPR and Data Protection Act 2018.

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

This policy should not be viewed in isolation. Rather, it should be considered in conjunction with the documents referred to in Appendix A.

Access to this policy

This policy is available on the Institute website: www.iadt.ie and from the Information Officer (Tel: 01 239 4947, Email: dp@iadt.ie).

5 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 GDPR specifies that data controllers (IADT) must comply with the following principles regarding the processing of personal data (see Glossary in Appendix C for definition):

Personal data <u>shall</u> be: (means mandatory)

- Processed lawfully, fairly and in a transparent manner in relation to the data subject (**Principles of Lawfulness, Fairness and Transparency**);
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (except for archiving purposes), (**Principle of Purpose Limitation);**
- Adequate, relevant and limited to what is necessary in relation to the purposes (**Principle of Data Minimisation**);
- Accurate and, where necessary, kept up to date (**Principle of Accuracy**);
- Kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes (**Principle of Data Storage Limitation**);
- 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**);

- The Institute, 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**).

5.1 Lawfulness of processing

The GDPR requires Data Controllers & Data Processors to have one of six lawful bases on which to process personal data. These are detailed in Article (6) of the GDPR:

(a) **Consent** - The data subject has given clear consent to process their data

(b) **Contract** – Processing the data is necessary to fulfil a contract

(c) **Legal obligation** - The processing of the personal data is necessary to comply with legal requirements

(d) **Vital interests** - The processing is necessary to protect a data subject's life

(e) **Public task** - The processing is necessary to perform a task in interest of the public or to perform the functions of the organisation

(f) **Legitimate interests** - The processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party

The Institute shall conduct all personal data processing in accordance with the most appropriate lawful basis above.

The Institute will process personal data in accordance with the rights of data subjects. Moreover, the Institute will carry out communications with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.

The Institute will only transfer personal data to another group or Third Parties outside of the European Economic Area (EEA) in accordance with this Policy.

Consent

If consent is the basis for processing then all Departments/Faculties/Functions must demonstrate that the data subject has provided appropriate Consent for data processing. A new Consent must be obtained for any new processing activity outside of initial consent. It should be understood that Consent is only valid when given by an affirmative action and when the Controller has abided by the principles detailed above. Anyone who has provided Consent has the right to revoke their Consent at any time and provision must be made for this as part of the Consent process. It must be as easy to withdraw Consent as it was to give it. Withdrawal of Consent for processing of personal data in relation to optional student services i.e. Health Centre, Disability or Learning Support, Student Counsellor etc., will mean that the individual concerned is no longer able to use that service.

5.2 Special Categories of Personal Data Processing/Sensitive Personal data

IADT will not process Special Categories of Personal Data (See Appendix C) unless;

- The Data Subject expressly **Consents** and / or
- the processing is **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 functions.

IADT 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.

5.3 Transparency

To ensure fair and transparent processing activities, the Institute is required to provide data subjects with a Privacy Notice to let them know what we are doing with their personal data when directly collecting data. For a link to a sample Privacy Notice see Appendix D.

These disclosures must 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 Disclosure.

If Consent is to be used as the most appropriate lawful basis then it must be obtained at data collection point.

When collecting personal data, Departments/Faculties/Functions and those acting on behalf of the Institute will require a privacy notice to be provided at the time the personal data is collected or at the same time as consent is sought.

When the Institute collects personal data from a Third Party (i.e. not directly from a data subject), data subjects should be made aware of the indirect collection of data by including relevant details at the point where personal data is disclosed.

Departments/Faculties/Functions may not disclose personal data to Third Parties prior to informing the data subject of their rights. In addition to the above, the Institute shall

provide the data subject with the following information necessary to ensure fair and transparent processing of their personal data:

- The personal data collection source and whether this was a public source.
- The personal data categories concerned.

The following are the only exceptions:

- Where notification would be near impossible for example where systems used do not allow for this, or
- The law expressly provides for this Personal data collection, processing or transfer.

5.4 Data Minimisation

Departments/Faculties/Functions should limit Personal data collection to:

- that which is directly relevant
- that which is necessary to accomplish a specified purpose.

Departments/Faculties/Functions should identify the minimum amount of personal data needed for a particular purpose, and then align collection volumes and associated retention to this purpose.

5.5 Data Use Limitation

Departments/Faculties/Functions must only collect personal data for specified, explicit and legitimate purposes. Departments/Faculties/Functions are prohibited from further processing unless legitimate processing conditions have been identified and documented 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 Department/Faculty/Function must ensure that any collected personal data is complete and accurate and adequately protected from unauthorised access.

In addition, the Heads of Department/Faculty/Function (Academic, Administrative and Research) must maintain personal data in an accurate, complete and up-to-date form as its purpose requires.

Upon the discovery of incorrect, inaccurate, incomplete, ambiguous, misleading or outdated data each Department/Faculty/Function must make every effort to correct without prejudice to:

- 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

Departments/Faculties/Functions must only keep personal data for the period necessary for permitted uses and as permitted under the Institute's approved Data Retention Policy & Schedule.

5.8 Security of Personal Data

Information Security

Each Department/Faculty/Function shall ensure personal data security through appropriate physical, technical and organisational measures. These include but are not limited to, ensuring adherence to the Data Handling and Clean Desk Policy, regular reviews of computer account and systems and room access of staff. In addition, Departments/Faculties/Functions should ensure all staff are aware of Institute data retention periods and of other appropriate policies and procedures of data protection.

These security measures should prevent:

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

Unauthorised Disclosure

No Institute employee or agent shall disclose Data Subjects' confidential information (including Personal data and Special Category 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 confidential information in any form.

5.9 Privacy and Data Protection by Design and by Default

The Institute 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.

5.10 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is designed to assist the Institute 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.

Completing a DPIA is a process whereby potential privacy issues and risks are identified, examined and assessed 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.

DPIAs are mandatory for any new high-risk processing projects and should be carried out prior to the processing of data and will serve as a useful tool to review procedures and processes and to help comply with data protection law.

The Heads of Departments/Faculties/Functions (Academic/Administrative/Research) are required to conduct a Data Protection Impact Assessment where appropriate and may consult with the Information Officer where appropriate.

5.11 Record of Processing Activities

The Institute as a data controller is required under the GDPR to maintain a record of processing activities under its responsibility (Data Processing Register). The 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, the retention period and when personal information is transferred to countries outside the EU.

The Heads of Departments/Faculties/Functions (Academic/Administrative/Research) are required to review records of processing periodically and put a monitor and review process in place in line with GDPR requirements.

5.12 Sharing with a Third Party of External Processor

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:

- The Institute may disclose student's 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 Privacy Notice.
- The data subject consents to the sharing.
- Where data is required under a Statutory Instrument or other legal obligation.
- The Third Party is operating as a Data Processor and meets the requirements of 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 parties' responsibilities and must ensure compliance with relevant GDPR and Data Protection Act 2018 requirements and any other applicable legislation such as sharing for the purposes of prevention/detection or investigation of a crime.

The Data Protection Officer should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

Requests for personal information from third parties such as relatives, An Garda Síochána, employers, should be dealt with in accordance with local provisions in respect of each system.

5.13 Transfer of Personal Data outside the EEA

Transfers of personal data to third countries require certain safeguards. Personal data must not be transferred 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 also covers personal data stored in the cloud as infrastructure may be in part located outside of the EU.

Departments/Faculties/Functions must not transfer personal data to a Third Party outside of the EEA regardless of whether the Institute is acting as a Data Controller or Data Processor unless certain precautions are taken. It is the responsibility of the person or persons involved in the data processing and transfer of personal data to ensure that the third party outside of the EEA conforms to the rigorous data protection principles and conditions of GDPR and is covered under the 'adequacy decisions' made by the European Commission. An 'adequacy decision' refers to a decision by the commission as to the safety of transferring data to certain countries outside of the EEA.

In February 2019 the Commission made an 'adequacy decision' and approved the transfer of data to the following countries and territories:

Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

In June 2021 the Commission made an 'adequacy decision' in respect of the UK.

Additionally, the Commission made decisions about other countries with some restrictions as follows:

1. The transfer of personal data to Japan only covers private sector organisations.

2. The transfer of personal data to Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For further details for sharing data with Canada visit https://ec.europa.eu/info/law/law-topic/data-protection/international-dimensiondata-protection/adequacy-decisions_en#documents

3. The transfer of personal data to the USA is only for personal data transfers covered by the EU-US Privacy Shield framework. (As at July 2021, this is subject to a legal challenge which may alter this document).

The Privacy Shield places obligations on American organisations certified by the scheme to protect personal data and allows for a redress system for data subjects.

If you wish to transfer personal data to an American company under the Privacy Shield, you should:

1. Consult the Privacy Shield list https://www.privacyshield.gov/list to see if the company is currently certified; and

2. Ensure the certification covers the type of data you want to transfer.

5.14 Data Subject Rights

Data subjects have a number of rights under GDPR.

These include:

- **Right of Access:** Data subjects can request to access the data the Institute holds on them through a Subject Access Request (SAR)

- **Right to Rectification**: Data subjects can request to change or correct any inaccurate factual data;

- **Right to Erasure**/ (sometimes called the Right to be Forgotten): Data subjects can request to delete data that the Institute holds. Please note, this is not an absolute right, there are conditions attached;

- **Right to Restriction of Processing**: Data subjects have the right to object to having their data processed (sometimes with consequences).

- **Right to Data Portability**: Data subjects can request to have their data moved outside of the Institute 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.

Subject Access Requests (SAR)

The Institute 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 Institute is the Data Controller for such personal data.

The GDPR gives data subjects the right to access personal information held about them by the Institute. This may include both electronic and non-electronic records (including emails, spreadsheets, expressions of opinion about them, notes etc.). 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.

Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request (20 working days). Members of staff should refer all such data requests to the Information Officer.

Requests for personal information will normally be free of charge, however, the Institute 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 Institute 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.
- When the identity of the requester cannot be determined.

Procedure for obtaining personal data (Right of access)

A request under section 4 must be in writing, should be addressed to the Data Protection Officer and should include any additional details that may be necessary to enable the organisation to locate the requested record; e.g. student number, staff number, or PPS number. Proof of identity will be required before release of any data.

Exceptions to the Right of Access

Chapter 4 Part 5 of the Irish Data Protection Act 2018 sets out the rights of an individual to obtain access to their personal records and also circumstances in which these rights can be limited. This is necessary in order to strike a balance between the rights of the individual, on the one hand, and some important needs of civil society, on the other hand. For example, a criminal suspect does not have a right to see the information held about him by An Garda Síochána, where that would impede a criminal investigation; and you do not have a right to see communications between a lawyer and his or her client, where that communication would be subject to legal privilege in court.

6 Policy Compliance

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

Any exception to the policy shall be reported to the Data Protection Officer in advance.

Failure to comply with this policy may lead to disciplinary action being taken in accordance with the Institute's disciplinary procedures. Failure of a third-party contractor (or sub-contractors) 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 – Roles & Responsibilities

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

Governing Body	• To review and approve the policy on a periodic basis
Audit & Risk Committee	• To oversee all aspects of data protection and privacy obligations and receive notification of all notified breaches.
President	• Ensure processes and procedures are in place within the Institute to facilitate adherence to the Data Protection Policy.
Institute Executive Board	• Implement the Data Protection policy and advocate a GDPR compliant culture.
Data Protection Officer (a member of the Institute Executive Board)	• To lead the data protection compliance and risk management 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 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 the Institute Executive Board and the Audit & Risk Committee. • Oversee appropriate monitoring and testing results of Data Protection compliance

Heads of Departments /Faculties /Functions (Academic/Administrative/Research)	• Implement the Data Protection Policy in their areas of responsibility • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility. • Ensuring information required for the record of processing activities is provided to the Data Protection Officer
Staff	• Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy which is supported by the Data Retention Schedule and procedures and; • Read and understand this policy document; • Understand what is meant by 'personal data' and 'special category or sensitive personal data' and know how to handle such data; • Endeavour not to jeopardise individuals' rights or risk a contravention of the Act; • Contact the appropriate person which may include a Head of Department/Faculty/Function and/or the Information Officer or Data Protection Officer if in any doubt.
Students/External Parties	• 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; • Endeavour not to jeopardise individuals' rights or risk a contravention of the Act; • Contact their Heads of Faculty/Department, or Data Protection Officer if in any doubt

Information Officer	• 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.

Appendix B – Supporting Documents

The below is a list of a suite of IADT policies and procedures to be used in conjunction with this policy where developed and in place.

Data Handling & Clean Desk Policy

Data Protection Breach Response Policy

Data Retention Schedule

ICT Acceptable and Appropriate usage Policy

Information Security Policy

Network Security Policy

Password Standard Procedures

The above list is not exhaustive and other Institute policies, procedures and standards and documents may also be relevant.

Appendix C - Glossary of Terms

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organization 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 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.
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 the Institute. 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.

Special or Sensitive Personal Data	Special or Sensitive Category 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 Faculty or Department/Faculty/Function within an Institute which is processing personal data for the Institute 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 Institute 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 the Institute 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 the Institute, that is in a business arrangement with the Institute 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 the Institute 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.
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. In this context, "signifies" means that there must be some active communication between the parties. Thus, a mere non-response to a communication from the Institute cannot constitute Consent.
Data Protection Commissioner	Means the office of the Data Protection Commission (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 country within 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 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 in the Irish Data Protection Act 2018 and/the GDPR.

Appendix D – Sample of Privacy Notice

A privacy notice is a public document from an organization that explains how that organization processes personal data and how it applies data protection principles.

It is a requirement under the GDPR that a Privacy Notice be:

- in a concise, transparent, intelligible, and easily accessible form
- written in clear and plain language, particularly for any information addressed specifically to a child
- delivered in a timely manner
- provided free of charge

A Privacy Notice or Statement must include (among other details):

- who we are
- the purposes for which we are collecting personal data
- details of any sharing of that data and with whom
- retention period of such data
- data subject rights such as the correction of incorrect factual information and
- the right to request a copy of their personal data and
- the right to complain to the Data Protection Commission
- Contact details of our Data Protection Officer

This link is to our Student, Staff and Applicant Privacy Notices on our website.

https://iadt.ie/about/your-rights-entitlements/gdpr/