Cork Institute of Technology

Data Protection Policy

Version 1.0

May 2018

Document Location

https://gateway.cit.ie/CITDocuments/Documents/Forms/AllItems.aspx?RootFolder=%2FCITDocuments%2FDocuments%2FGovernance%20and%20Management%2F12%20Freedom%20of%20Information%20and%20Data%20Protection%2FData%20Protection%2FGDPR%20Policies&InitialTabId=Ribbon%2EDocument&VisibilityContext=WSSTabPersistence

Revision History

Date of this revision:	**Date of next review:**

Version Number/Revision Number	**Revision Date**	**Summary of Changes**
1.0	28/05/18	Sectoral Template Customised for CIT

Consultation History

Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
	15/06/2018	Unions	

Approval

This document requires the following approvals:

Name	**Title**	**Date**
GB	Governing Body	05/07/2018

This Policy was approved by the Governing Body on 5 July 2018. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1. OVERVIEW

The Institute is responsible for the processing of a significant volume of personal information across each of its Schools 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.
- The Institute has an appointed Data Protection Officer ('DPO') who is available to Schools and Functions to provide guidance and advice pertaining to this requirement.
- It is the responsibility of each School and Function[1] to ensure this personal information 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 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.

Further information for staff can be found in the Institute's Data Protection Procedures Document which provides detailed guidance, templates and forms to enable staff comply with GDPR.

2. PURPOSE

The Institute must comply with all applicable Data Protection, privacy and security laws and regulations (collectively referred to as requirements) in the locations in which it operates. In Europe, the key Data Protection requirement, the General Data Protection Regulation (GDPR), came into effect on May 25, 2018.

The Institute 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. 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 the Institute who receives, handles or processes personal data in the course of their employment.
- Any student of the Institute 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 the Institute.

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

4. POLICY

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

The Institute 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 the Institute's competence and confidentiality while handling data.

This policy should not be viewed in isolation. Rather, it should be considered as part of the Institute suite of Data Protection policies and procedures (see Appendix B).

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.

The Institute 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);

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)

5.2 Lawfulness of Processing

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

- Necessary processing for contract performance or contract entry.
  and / or
- Legislative/statutory basis underpinning Processing
  and / or
- Data Subject Consent for one or more specific purposes

  Public authorities are not encouraged to use consent for core activities due to the imbalance in the relationship between the controller and data subject. Therefore where possible the Institute should identify alternative justifications for processing.

  If consent is the basis for processing then the Institute must demonstrate that the Data Subject has provided appropriate consent for data processing. The Institute must obtain a consent for any new processing activity outside of initial consent. It should be understood that anyone who has provided consent has the right to revoke their consent at any time.

- 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.

- All personal data processing shall be conducted in line with the Institute's Risk Management Policy.

Special Categories Personal Data Processing

The Institute will not process Special Categories of Personal Data (see Definitions) unless;

- 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.

The Institute 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. Only the Data Protection Officer may authorise this exemption and only in accordance with relevant national legislation.

Exception to processing in the absence of one of these conditions requires the approval of the Data Protection Officer.

5.3 Transparency - Privacy Notices

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.

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 Processing Personal Data condition then this Processing Consent must be obtained at data collection point.

If carrying out an activity that is not covered by the main Institute Privacy Notices, Head of Function (Academic/Administrative/Research) 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 fair disclosure notices content and mechanism requires prior DPO approval in consultation with Head of Function (Academic/Administrative/Research).

When The Institute collects Personal Data from a Third Party (i.e. not directly from a Data Subject), it must provide "Fair Disclosure Notices" to the Data Subject either at the time of collection or within a reasonable timeframe that is no more than 30 days post collection.

Personal Data may not be disclosed to Third Parties prior to informing the Data Subject of their rights. In addition to the fair disclosure notice content 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 and whether this was a public source.
- The Personal Data categories concerned.

The following are the only exceptions:

- If the Data Subject has already received the required information, or
- Notification would require disproportionate effort, or
- The law expressly provides for this Personal Data collection, processing or transfer.

5.4 Data Minimisation

Personal Data collection must be limited to:

- What is directly relevant
- What is necessary to accomplish a specified purpose

Head of Function (Academic/Administrative/Research) should identify the minimum amount of Personal Data needed for a particular purpose, and then align collection volumes and associated retention to this purpose.

5.6 Data Use Limitation

Personal Data must only be collected for specified, explicit and legitimate purposes. Further processing is prohibited unless Head of Function (Academic/Administrative/Research) have identified legitimate processing conditions and documented same or if the Personal Data involved is appropriately Anonymised and / or Pseudonymised and used for statistical purposes only.

5.7 Data Accuracy

Head of Function (Academic/Administrative/Research) must ensure that any collected Personal data is complete and accurate subject to limitations imposed by Institute/ Third Party contractual provisions.

In addition, Head of Function (Academic/Administrative/Research) must maintain Personal Data in an accurate, complete and up-to-date form as its purpose requires.

Head of Function (Academic/Administrative/Research) 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.

5.8 Data Storage Limitation Policy

Head of Function (Academic/Administrative/Research) must only keep Personal Data for the period necessary for permitted uses and as permitted under the Institute's approved Data Retention Schedule.

5.9 Security of Personal Data

Information Security
Head of Function (Academic/Administrative/Research) 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 Institute 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.

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

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed to enable the Institute 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

Head of Function (Academic/Administrative/Research) are required to conduct a Data Protection Impact Assessment (DPIA) where appropriate and then consult with the DPO.

5.11 Record of Processing Activities

The Institute as a data controller is required under GDPR to maintain a record of 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 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.

5.12 Data Sharing

Sharing with a Third Party or External Processor

As a general rule personal data should not be passed on to third parties, 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.
- The Third Party is operating as a Data Processor and meets the requirements of GDPR. Where a third part 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 European and local Member State Data Protection requirements/legislation.

The DPO 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 Siochana, employers etc. should be dealt with in line with Institute Guidelines.

Transfer of Personal Data outside the EEA

Transfers of personal data to third countries are prohibited without certain safeguards. The means the Institute 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.

Head of Function (Academic/Administrative/Research) 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 conditions are met.

The DPO and Institute Solicitors must be consulted prior to any Personal Data transfer outside the EU and must record the determination in writing.

5.13 Subject Access Request (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. 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 Institute holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

Data Subject Rights:

- Data subjects will be able to request to access the data the Institute 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 Institute 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 Institute 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 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.
- It would be illegal to do so.
- The identity of the requester cannot be determined.

5. POLICY COMPLIANCE

6.1 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 the the Institute.

6.2 Compliance Exceptions

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

6.3 Non-Compliance

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 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 – 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
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.
Head of Function (Academic/Administrative/Research)	• Implementing 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
Data Protection Officer	• 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
Staff/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; • Not jeopardise individuals' rights or risk a contravention of the Act; • Contact their Heads of Schools & Support Functions, Directors of Research Centres or Data Protection Officer if in any doubt
Audit & Risk Committee	• To oversee all aspects of data protection and privacy obligations.

Appendix B – Supporting Documents

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

- Information Security Policy
- Data Access Management and Privileged User Policy
- Information Governance Policy
- Data Retention Policy
- Data Handling & Clean Desk Policy
- Data Protection Breach Response Policy

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.
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 or 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 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 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 the GDPR and/or local requirements.