Galway-Mayo Institute of Technology (GMIT)

Data Protection Policy

Version 2.0

Document Location
Data Protection Officer (DPO)

Revision History

Date of this revision: 22/01/2019	**Date of next review:** Jan 2021

Version Number/Revision Number	Revision Date	Summary of Changes
1.0	31/08/2017	First Data Protection Policy approved
2.0	30/05/2019	New Data Protection Policy drafted in line with GDPR

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	12/05/2017 19/05/2017 14/06/2017 15/08/2017 31/08/2017	Executive Board Management Group CPF Executive Governing Body	Approved for consultation No changes No changes Approved for consideration by Governing Body Approved
2.0	22/01/2019 08/02/2019 25/02/2019	Executive Board Management Group CPF	Amendment to Section 9.0; Approved for consultation No changes Amendment to Section 5.0

Approval
This document requires the following approvals:

Revision Number	Title	Date
1.0	Governing Body	31/08/2017
2.0	Governing Body	30/05/2019

Table of Contents

1.0 Introduction

GMIT, as a data controller, processes the personal data of data subjects (students, staff, applicants, alumni, website users and other individuals) in order to carry out its functions.

All personal data must be processed in line with the General Data Protection Regulation (GDPR), 2016/679 and the Data Protection Acts 1988-2018 [hereafter referred to as "data protection legislation"]. This legislation confers rights on individuals as well as responsibilities on those organisations processing personal data.

2.0 Purpose of Policy

This Policy sets out GMIT's commitment to protecting the rights and privacy of individuals and details how the Institute will ensure compliance with data protection legislation.

Compliance with data protection legislation is the responsibility of all members of the Institute and GMIT is committed to ensuring that all those who access or use personal data acknowledge that they have a responsibility to exercise care in the treatment of that data.

3.0 Definitions

See Appendix A for definitions used in this policy.

4.0 Scope

This policy covers all personal data processed by GMIT, regardless of whether in electronic or physical format.

This policy applies to:

- Any person employed by GMIT who processes personal data in the course of their employment;
- Any student of GMIT who processes personal data in the course of their studies for administrative, research or any other purpose;
- Data processors that process personal data on behalf of the Institute.

5.0 Roles and Responsibilities

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

Governing Body	• To review and approve this policy on a periodic basis.
Executive Board	• To review and approve this policy and any updates to it prior to submission to the Governing Body for approval. • To oversee all aspects of data protection and privacy obligations. • To ensure ongoing compliance with data protection legislation in their respective areas of responsibility. • To ensure adequate resources are provided to safeguard compliance. • To instigate investigations of data protection matters of interest where appropriate. • As part of the Institute's Annual Statement of Internal Control, to sign a statement which provides assurance that their functional area is in compliance with data protection legislation.

All Managers	• To ensure implementation of this policy and good personal data handling practices in their areas of responsibility. • To ensure adequate resources are provided to safeguard compliance. • To review DPIAs and approve, or not, the design of data protection elements of projects.
Data Protection Officer (DPO)	• To provide the Executive Board with regular updates on data protection responsibilities, risks and issues. • To advise staff on their obligations and make training available to all staff. • To provide advice in relation to DPIAs. • To respond to individuals who wish to exercise their data subject rights. • To maintain relevant records. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To liaise with the Data Protection Commission.
VP for Finance & Corporate Services	• To lead the data protection compliance function. • To act as an advocate for data protection within the Institute. • To oversee the work of the DPO. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To liaise with the Data Protection Commission.
Staff / Students / Data Processors	• To comply with this policy.

6.0 Data Protection Officer

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

By email: dpo@gmit.ie
By phone: +353 (0)91 742769
By mail: Room 1063, GMIT Galway Campus, Dublin Road, Galway H91 T8NW

7.0 Data Protection Principles

All processing of personal data shall be conducted in accordance with the principles set out in data protection legislation, which state that personal data shall be:

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

- Processed in a secure manner by having appropriate technical and organisational measures in place to prevent and/or identify unauthorised or unlawful processing of personal data; and prevent accidental loss or destruction of, or damage to, personal data (Principle of Integrity and Confidentiality);

Also, GMIT shall be responsible for, and be able to demonstrate compliance with, these key principles (Principle of Accountability).

7.1 Principle of Lawfulness, Fairness & Transparency

7.1.1 Lawful Basis

The Institute shall process personal data only if there's a lawful basis to do so. The lawful bases for processing personal data are:

- **Contract:** the processing is necessary for a contract the Institute has with the individual, or because they have asked the Institute to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for the Institute to comply with the law.
- **Public task:** the processing is necessary for the Institute to perform a task in the public interest or for the Institute to perform its official functions.
- **Consent:** the individual has given clear consent for the Institute to process their personal data for a specific purpose. Where consent is the legal basis for processing, the individual/area gathering the consent shall demonstrate that the consent is freely given, specific, informed and unambiguous and has been provided using a clear affirmative action. The data subject shall be made aware that consent can be revoked at any time.
- **Vital interests:** the processing is necessary to protect someone's life.
- **Legitimate interests:** the processing is necessary for the legitimate interests of the Institute or a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (As a public body, the Institute cannot rely on this legal basis for processing personal data in the performance of its official tasks.)

Special Categories of Personal Data[1] are more sensitive and require more protection and shall only be processed by the Institute when there's a separate condition for the processing in addition to one of the legal bases listed above.

There are ten conditions for processing special category data in the GDPR itself, and the Data Protection Act 2018 includes additional conditions and safeguards.

Some of the lawful bases most likely to be relied on by the Institute in processing special categories of data are:

- Where the data subject explicitly **consents**;
- The processing is **necessary to carry out the Institute's obligations or exercise the data subject's specific rights in the field of employment and social security and social protection law**;

[1] *Special Categories of Personal Data (or Sensitive 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.*

- The processing is **necessary for the purposes of preventitve or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment** or the management of health or social care systems and services;
- The processing is **necessary for the purposes of providing or obtaining legal advice or for the purposes of, or in connection with, legal claims, prospective legal claims, etc**;
- The processing is **necessary for the purposes of insurance, occupational pension** or the mortgaging of a property;
- The processing is **necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**.

Personal data relating to criminal convictions/offences, including Garda Vetting disclosures made to the Institute, shall be stored securely with access restricted to a small number of authorised personnel.

7.1.2 Privacy Notices

When the Institute collects personal data, it is obliged to make certain information available to the person to whom the data relates by way of a privacy notice. The Institute shall provide data subjects with privacy notices at the point of collection. Privacy notices shall be easily understood and contain specific information including:

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

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

7.2 Principle of Purpose Limitation

The Institute shall process personal data only for specified, explicit and legitimate purposes. Personal data will only be used for a new purpose if the new purpose is compatible with the original purpose, or if there's a clear basis in law.

Staff shall ensure that personal data is only disclosed to work colleagues on a need-to-know basis.

Departing staff members shall return all personal data to the Institute and not remove any personal data from the Institute on departure.

7.3 Principle of Data Minimisation

The Institute shall process personal data which is adequate, relevant and limited to what is necessary to accomplish a specified purpose. This is particularly important for special category or criminal offence data. Data owners shall periodically review their processing to ensure that the personal data held is still relevant and adequate for their purposes. Personal data shall not be collected or held on a 'just in case' basis. Personal data no longer required shall be securely deleted/destroyed.

7.4 Principle of Accuracy

Data owners shall ensure that the personal data being processed is accurate and, where necessary, kept up-to-date.

7.5 Principle of Storage Limitation

The Institute shall not keep personal data for any longer than is necessary for the purposes for which it is processed. Each data owner shall implement the retention periods outlined in the Institute's Record Retention Schedule.

7.6 Principle of Integrity & Confidentiality (Security)

The Institute shall ensure personal data is secure by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These security measures, which should prevent alteration, loss, damage, unauthorised processing, or unauthorised access, may include:

- Adopting safe data handling practices, including:
    - Never leaving confidential documents unattended at desks or when working remotely
    - Never leaving confidential documents at printers, in meeting rooms or other public/semi-public places
    - Locking computer screens when away from desk
    - Shredding documents containing personal data
    - Regularly reviewing information stored in filing cabinets and disposing of documents in line with the Records Retention Schedule
- Adopting, implementing & reviewing IT security policies & procedures
- Using encryption and pseudonymisation where appropriate
- Ensuring appropriate back-up processes
- Ensuring our staff are trained in data protection
- Undertaking analysis of risks presented by our processing
- Conducting regular testing and reviews of our measures to ensure they remain effective
- Ensuring our data processors implement appropriate technical and organisational measures.

7.7 Principle of Accountability

The Institute shall have appropriate measures and records in place to be able to demonstrate compliance with the principles of the GDPR. These include, inter alia:

- A designated DPO
- Data protection and IT policies & procedures
- Records of processing activities / data inventories
- Privacy notices
- Records of data breaches
- Data Processor Contracts and Data Sharing Agreements
- Data Protection Impact Assessments (DPIAs)
- An education and awareness programme

7.7.1 Records of Processing Activities / Data Inventories

Each organisational unit shall maintain a record of its processing activities / data inventory. These records shall contain information on the processing purposes, the lawful basis for processing, data sharing, data transfer, retention period, etc.

These records shall be drafted as per the Data Inventory Template and shall be reviewed and signed off by the relevant Managers regularly, in consultation with the DPO.

7.7.2 Data Protection by Design and Default

The Institute shall consider data privacy in every aspect of processing activities, thereby implementing appropriate technical and organisational measures to minimise the risk to personal data.

Data Protection 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.

Data Protection by Default states that the strictest privacy settings should apply by default to any new service or product, without the data subject having to make any changes.

An integral part of data protection by design and default is the requirement to undertake Data Protection Impact Assessments (DPIAs) in certain circumstances when a new activity is being considered which may impact on the privacy of individuals.

7.7.3 Data Protection Impact Assessments (DPIAs)

The Institute will ensure that DPIAs are carried out in circumstances when a new data processing activity is likely to result in a high risk to the rights and freedoms of a data subject, including when:

- Performing a systematic and extensive evaluation of the personal aspect of an individual, including profiling.
- Processing sensitive/special categories of data on a large scale.
- Undertaking systematic monitoring of public areas on a large scale.
- Using personal data on a large-scale for a purpose(s) other than that for which it was initially collected.
- Profiling vulnerable persons including children in order to target marketing/online services at such persons.
- Using profiling or algorithmic means or special category data as an element to determine access to services.
- Systematically monitoring, tracking or observing individuals' location or behaviour.
- Profiling individuals on a large-scale.
- Processing biometric data to uniquely identify an individual(s).
- Processing genetic data.
- Indirectly sourcing personal data where GDPR-transparent requirements are not being met.
- Combining, linking or cross-referencing separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individuals, particularly where the data sets are combined from different sources.

Prior to the commencement of a relevant activity/initative/project, a DPIA Pre-Assessment will be completed by the project team and shared with the DPO in order to determine if a full DPIA is required.

Where a full DPIA is considered necessary, it shall be undertaken by the project team in consultation with the DPO prior to the commencement of the processing.

Where the Institute is unable to identify measures that mitigate the high risks identified, the Institute will consult with the Data Protection Commission prior to the commencement of the processing.

7.7.4 Education and Awareness

The Institute is committed to ensuring all individuals are aware of their obligations under data protection legislation. Training shall be provided via face-to-face presentations and online. All staff shall complete training provided by the Institute to support compliance with this policy. The DPO will maintain training completion records in line with the accountability principle.

Staff shall also be kept informed of data protection obligations via the Data Protection SharePoint site and via email.

8.0 Personal Data Breaches

A data breach is defined as *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*[2]

The Institute shall ensure that all data breaches are managed properly in order to comply with statutory reporting obligations which require that the Institute notifies the Data Protection Commission within 72 hours of becoming aware of the breach and notifies the affected individuals, where the breach is likely to result in a 'high risk' to their rights and freedoms, without undue delay.

Any individual discovering a data breach, or suspected data breach, shall report it immediately to the DPO by emailing dpo@gmit.ie.

The "GMIT Personal Data Breach Procedure" shall be followed at all times.

An internal record of all data breaches shall be documented by the DPO in line with the accountability principle.

9.0 Data Sharing

9.1 Sharing Personal Data with Certain Organisations

The Institute shares personal data about applicants, students, staff, alumni, research participants and others with third parties (outside the Institute) for multiple reasons. This sharing shall occur only where there's a legal basis to do so, for example where:

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

The data sharing may be:

a) To a third party for joint purposes (e.g. to another institution to administer joint programmes);
b) To a third party for that party's own purposes (e.g. to the HEA for statistical analysis purposes);

[2] Article 4(12) of GDPR

c) To a third party to process data on behalf of the Institute (e.g. to Microsoft for software provision, to CCTV companies for surveillance, to a document storage company for archiving, etc). This third party is known as a Data Processor.

This sharing will be documented in relevant privacy notices.

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

The Institute will continue to put in place agreements and contracts with such third parties, clearly setting out the responsibilities and liabilities of both parties.

9.2 Sharing Personal Data with Parents/Guardians

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

10.0 Data Transfers outside the European Economic Area (EEA)

Additional restrictions and conditions exist when data sharing involves a transfer outside the EEA so as to ensure that the personal data is protected by an 'adequate' level of protection after it has been transferred.

Personal data shall not be transferred to a third country unless there are adequate safeguards in place to provide an adequate level of data protection. Sample safeguards include:

- Where the third party is based in a country that has been deemed adequate by the European Commission e.g. Canada
- Where the third party is based in the USA and has signed up to the Privacy Shield
- Where the third party signs up to Standard Contractual Clauses.

In certain circumstances the adequacy requirement can be circumvented for occasional/limited personal data transfers, for example when the data subject has explicitly consented to the transfer; the transfer is necessary for the performance of a contract; for public interest reasons; the defence of legal claims; or the vital interests of the data subject.

The DPO must be consulted prior to any personal data transfer outside the EEA and the determination must be recorded in writing. It is important to note that this covers personal data stored in the cloud as infrastructure may be in-part located outside the EEA.

11.0 Data Subject Rights

The GDPR provides data subjects with the following rights, in some instances subject to certain conditions/restrictions:

1. The right to be informed (see Privacy Notices in section 7.1.2)
2. The right of access – the right to obtain a copy of their personal data from the Institute
3. The right to rectification – the right to have inaccurate or incomplete data rectified

4. The right to erasure/right to be forgotten – the right to have data erased
5. The right to data portability – the right to receive/transfer data which is in a structured, commonly used and machine-readable format
6. The right to object – the right to object to data being used for direct marketing and in certain other limited circumstances
7. The right of restriction – the right to restrict the processing of your data
8. The right not to be subject to automated decision making, including profiling.

To exercise any of these rights, refer to the "GMIT Data Subject Rights Procedure" or contact the DPO.

Any staff member in receipt of a data subject request shall forward same to the DPO immediately.

Requests shall be administered free of charge. However, where requests are manifestly unfounded or excessive in nature, the Institute shall either charge a fee to cover the administrative costs of providing the personal data, or refuse to act upon the request.

12.0 e-Privacy

The ePrivacy Directive/Regulation aims to guarantee the right to privacy in the electronic communications sector by providing specific rules on electronic communications (e.g. direct marketing by telephone, email, text or fax) and internet tracking (e.g. cookies). Where personal data is processed to keep people informed of Institute activities and events, the communicator of that information shall provide a way for recipients to opt out of future such communications.

13.0 CCTV

Recognisable images captured by CCTV systems are personal data and are therefore subject to the provisions of data protection legislation. Refer to the Institute's CCTV Policy & Procedures.

14.0 Policy Compliance

Breaches of this policy may result in non-compliance by GMIT with data protection legislation which may result in fines or legal action being taken against the Institute.

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 subcontractor) to comply with this policy may lead to termination of the contract and/or legal action.

15.0 Supporting Documents

This policy should be read in conjunction with other Institute policies, including:

- CCTV Policy & Procedures
- Data Governance Policy
- Data Compliance Policy
- Access Control Policy
- Information Security Policy
- Acceptable Usage Policy
- Social Media Policy
- Risk Management Policy

The above list is not exhaustive and other policies may apply.

Appendix A Definitions

GDPR	The General Data Protection Regulation (GDPR) is EU regulation 2016/679 which came into force in May 2018. It is essentially a new set of data protection rules concerned with ensuring that each of us knows when personal information about us is collected and how it will be used, and giving us more control over the use of this personal data.
Data Protection	Data protection law is about everyone's fundamental right to the protection of their personal data. When personal data is given to an organisation, that organisation has a duty to comply with certain rules which limit what they can do with the personal data. Collectively, these rules, together with the rights that someone has to protect their personal data, are known as data protection.
Data	Data includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
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 GMIT. Examples of personal data include, but are not limited to: • Name, home address, email address, home phone/mobile number • DOB, age, gender, ID number, PPSN, salary, financial data, car reg details • Qualifications, education, employment history, leave details • 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 • Photographs, CCTV images, voice recordings • IP address
Special Categories of Personal Data	Special Categories of Personal Data (or Sensitive 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; genetic & biometric data.
Data Processing	Processing basically means using personal data and doing anything with it, from collecting to storing it, to retrieving it, consulting it, sharing it with someone else, erasing it and destroying it.
Data Controller	A person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data is, or is to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Subject	The individual to whom personal data held relates, including: employees, students, customers, suppliers.
Data Processor	A person or organisation who processes personal data on behalf of a controller, but does not include an employee of a controller who processes such data in the course of his or her employment.

Data Owner	A data owner is an individual who is accountable for a data set. This is typically an executive/management member within the department, team or business unit that owns a data asset.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The Institute must obtain consent for any new processing activity outside of initial consent.
EEA (European Economic Area)	An area encompassing the European member states and three EFTA states (Iceland, Liechtenstein, and Norway) which allows 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.
Standard Contractual Clauses	Standard contractual clauses are one of several mechanisms approved by the European Commission to ensure adequate safeguards for personal data transferred from the EU to countries which the European Commission has not found to offer adequate protection for personal data.
Profiling	Any form of automated processing of personal data consisting of the use of the data to evaluate certain personal aspects relating to an individual, including to analyse or predict aspects concerning the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Anonymisation	The process of stripping personal data of sufficient elements so that the data subject can no longer be identified. Anonymised data is no longer personal data. If it's possible, at any point, to use any reasonably available means to re-identify the individuals to which the data refers, the data will not have been effectivevely anonymised but will have merely been pseudonymised.
Pseudonymisation	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 is 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.