Maynooth University
Data Protection Office

Data Protection Policy

Author / Policy Owner:	Data Protection Office
Creation Date:	27th February 2018
Review Date:	31th August 2022
Version:	17th May 2022
Scope:	This policy applies to all staff, students and public who interact with Maynooth University
Related Policies:	Student Data Privacy Notice Staff Data Privacy Notice Personal Data Security Incident/Breach Management Procedures Data Protection Impact Assessment document
Approved by UE Date:	**24th January, 2023**

Revision History

Date of this revision: 31st August 2022	Date of next review: 31st August 2024

Table of Contents

1. Introduction

- Maynooth University collects, processes and uses data (in electronic and manual format) for a variety of purposes about its staff, students and other individuals who come in contact with the University.
- The General Data Protection Regulation (GDPR) and the Data Protection Acts 1988 to 2018 ("**Data Protection Law**") confer rights on individuals regarding their personal data as well as responsibilities on those persons processing personal data.
- This policy outlines the obligations of Maynooth University under Data Protection Law and describes the steps to be taken to ensure compliance with those obligations.
- This policy applies to the University's employees and students and any other person who interacts with the University.
- It is the responsibility of all Staff and Students to comply with this policy.

2. Purpose

This policy is a statement of the University's commitment to protect the rights and privacy of individuals, and to enable them to exercise their rights, in accordance with Data Protection Law. It is the University's policy to ensure that it processes personal data in accordance with Data Protection Law and the terms of this policy.

3. Definitions

Controller or data controller means any person who, either alone or with others, controls the purposes and means of the processing of personal data. Controllers can be either legal entities such as universities, companies, government departments or voluntary organisations, or they can be individuals.

Processor or data processor means a person 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/her employment.

Data subject means an individual who is the subject of personal data.

Personal data means information relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name, an identification number, location data or an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual). This can be a very wide definition depending on the circumstances.

Processing means performing any operation or set of operations on personal data including: (a) recording the personal data; (b) collecting, obtaining, organising, structuring, storing, altering or adopting the personal data; (c) retrieving, consulting or using the information or personal data; (d) disclosing the personal data by transmitting, disseminating or otherwise making it available; or (e) adapting, aligning, combining, restricting, erasing or destroying the personal data.

Special Categories of Personal Data means personal data relating to an individual's: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life or sexual orientation. Individuals have additional rights in relation to the processing of any such data.

Data minimisation means the collection and processing of personal data to the extent that it is adequate, relevant, and limited to what is necessary in order to achieve the given purpose and no more.

4. Role of Data Protection Commission ("DPC")

The DPC oversees compliance, monitors, and enforces the Legislation. The DPC has a wide range of enforcement powers, including investigation of University records and record-keeping practices as well as the issuing of warnings, reprimands, corrective actions and administrative fines.

5. Principles of Data Protection Law

As a controller, Maynooth University complies with its responsibilities in accordance with the following general data protection principles outlined in the Data Protection Law:

a) Personal data shall be processed lawfully, fairly, and in a transparent manner.

For personal data to be obtained fairly and in a transparent manner, data subjects must be provided with certain information, generally at the time at which the personal data is obtained. It is Maynooth University's policy to do so by setting out the relevant information in the data protection/privacy notice to ensure their awareness of:

- the identity and contact details of data controller;
- the purpose and legal basis for processing personal data;
- where legitimate interests are relied upon (Article 6(1)(f)), the legitimate interests pursued by the data controller or third party;
- recipients or categories of recipients of the personal data;
- details of transfers to third countries, the fact of same and the details of the relevant safeguards and the means to obtain a copy of them or where they have been made available;
- the storage period;
- the rights of the data subject (access, rectification, erasure, restriction, objection, and portability);
- where processing is based on consent, the right to withdraw consent at any time;
- the right to lodge a complaint with Data Protection Commission;
- where relevant, the existence of automated decision making;
- contact details for the Data Protection Officer.

Personal data is obtained lawfully where at least one of the following applies:

- the data subject has given consent to the processing of their personal data for one or more specific purposes. Where the University relies solely on consent as a condition of processing personal data, it must:
  - obtain the data subject's specific, informed, and freely given consent;
  - ensure the data subject gives consent by a statement or clear affective action;
  - document the consent;
  - allow data subjects to withdraw their consent at any time (where provided in Data Protection Law).
- Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the controller is subject (for instance compliance with the Universities Act 1997 (Section 13(2) refers) the organisation and administration of courses, research activities, the recruitment and payment of staff, contractual obligations, and compliance with statutory obligations);
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The Staff and Student Data Privacy Notices can be found here:
https://www.maynoothuniversity.ie/data-protection/policies-privacy-notices

b) Personal data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes.

Maynooth University only processes personal data for purposes that are specific, explicit, and for a legitimate purpose. Staff and students should not collect information about people routinely and indiscriminately without having a clear and legitimate purpose for doing so. The University's practice is to keep personal data for lawful purposes which are set out in the data protection/privacy notices.

c) Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.

Maynooth University's practice is to ensure that it collects and keeps only such personal data as is necessary for the purposes set out in its privacy notices and follows the "data minimisation principle". The types of information about individuals which the University collects and keeps are periodically reviewed to ensure compliance with this requirement, and information that is no longer required is deleted in accordance with Maynooth University's Record Retention Schedules.

d) Personal data shall be accurate, and, where necessary, kept up to date, and every reasonable step shall be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Maynooth University seeks to ensure that the personal data it holds is at all times accurate, complete and up to date. The University takes every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay in accordance with the procedures set out in the Documenting and Monitoring Compliance section of this policy and Maynooth University's Record Retention Schedules.

e) Personal data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed.

Unless legally required Maynooth University does not retain personal data in a form that permits the identification of data subjects indefinitely. The University's policy is to ensure that its record retention schedules give effect to this principle. Maynooth University's records retention schedules contain details of the periods for which the University retains the various categories of records that it holds.

f) Personal data shall be processed in a manner that ensures appropriate security of the data, including, by the implementation of appropriate technical or organisational measures, protection against—

(i) unauthorised or unlawful processing, and
(ii) accidental loss, destruction or damage.

Maynooth University's practice is to ensure that access to personal data which is held by the University is restricted relevant to work processes. To the extent that any third party processes personal data on behalf of the University, the University ensures that there is a written agreement in place which includes appropriate security obligations regarding such personal data.

Access to the University's IT systems and manual systems that hold personal data are subject to security and acceptable use policies which outline responsibilities in using these systems.

Maynooth University implements the following technical and organisational measures:

- Use, storage and transfer of personal data in electronic format is subject to stringent controls (e.g. use of password protection, timed log-out of systems, encryption of PC folders and portable devices, regular backup, use of anonymisation software etc.);
- Employees must ensure that personal data they have access to as part of their duties is kept securely at all times and is protected from inadvertent disclosure, loss, destruction, alteration or corruption;
- Screens, printouts, documents, and files showing personal data must only be accessible to authorised persons and must be retained in a secure manner at all times;
- Paper records containing personal data must be stored securely, for example in locked rooms or cabinets;
- Personal data must be kept confidentially and must never be discussed with/disclosed to any unauthorised third party, either internal or external to the University without the prior consent of the data subject, except where there is a statutory obligation to do so (e.g. if required for the purpose of preventing, detecting or investigating offences, required urgently to prevent damage to health or serious loss/damage to property, required under law etc.);
- Personal data relating to a data subject must not be disclosed to any third party, even if they identify themselves as a parent, current/potential employer, professional body, sponsor, etc. Such disclosures must only be with the consent of the individual concerned. This includes requests for contact details (e.g. address, mobile phone number) or even a request to confirm a person's attendance at the University;
- Ensure that mobile devices issued to employees are secure.

6. Accountability

Data Protection Law obliges organisations to demonstrate that their Processing activities are compliant with the Data Protection Principles.The principle of accountability seeks to guarantee the enforcement of these principles. Maynooth University will demonstrate compliance in the following ways:

- by maintaining a Register and Inventory of Personal Data in line with Article 30 – 'Records of Processing Activities'. These can be found at this address: https://www.maynoothuniversity.ie/data-protection/register-inventory-personal-data

7. Data Subject Rights

Data subjects for whom the University holds personal data have the following rights in relation to the processing of their personal data (subject to certain limited exceptions):

(i) **The right to obtain access to personal data**. Data subjects have the right to be provided with copies of their personal data along with certain details in relation to the processing of their personal data.

(ii) **The right to information**. Data subjects have the right to be provided with certain information, generally at the time at which their personal data is obtained. Maynooth University complies with this obligation via its data protection/privacy notices.

(iii) **The right to rectification**. Data subjects have the right to have inaccurate personal data that a controller holds in relation to them rectified.

(iv) **The right to object and restrict processing**. Data subjects have the right to require that a controller restricts its processing of their data in some circumstances, and have the right to object to the processing of their personal data in certain circumstances.

(v) **Rights in relation to automated decision making**. Data subjects have the right not to be subjected to processing which is wholly automated and which produces legal effects or otherwise which significantly affects them, and which is intended to evaluate certain personal matters, such as creditworthiness or performance at work, unless one of a number of limited exceptions applies.

(vi) **The right to request erasure of personal data**. Under certain circumstances a data subject has the right to request the erasure of their personal data.

(vii) **The right to data portability**. Under certain circumstances, Maynooth University may be required to provide a data subject with a copy of their personal data in a structured, commonly used and machine readable format.

Maynooth University is obliged to comply with any requests by a data subject to exercise the above rights within strict timelines imposed under Data Protection Law (one month). Data access requests should be directed to the University's Data Protection Office so that they can be processed as efficiently as possible and within the timeframe specified in the legislation. Contact: dataprotection@mu.ie.

8. Third Party Processors

Engaging Processors

A processor is a third party that processes personal data on behalf of Maynooth University. If a third party has access to personal data that belongs to or is controlled by the University in order to provide a service to the University, then the third party is acting as a processor on behalf of the University.

Prior to engaging processors, the University:

(a) undertakes due diligence to ensure that it is appropriate to engage the processor; and
(b) ensures that it puts in place an agreement in writing with the processor that complies with the requirements under Data Protection Law.

The Personal Data Inventory sets out details of the processors that are engaged by the University. The details of processors in the Data Inventory will be kept up to data in accordance with the procedure set out in the Documenting and Monitoring Compliance section of this policy.

Transfers of Personal Data Outside the European Economic Area (EEA)

Under Data Protection Law, Maynooth University may not (save where one of a limited number of exceptions applies) transfer personal data outside of the EEA to any third country, unless that third country is deemed by the European Commission to provide an adequate level of protection in relation to the processing of personal data. The most relevant exceptions are:

(a) The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) A data transfer agreement, incorporating the model clauses in the form approved by the EU Commission;
(c) The transfer is made pursuant to a Code of Conduct or a certification mechanism that has been approved under applicable Data Protection Law, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
(d) The data importer is subject to a framework approved by the European Commission to facilitate transfers (e.g. the EU – U.S. Privacy Shield).

9. Documenting and Monitoring Compliance

Ensuring Compliance

Maynooth University has in place policies and procedures to ensure that it can demonstrate its compliance under Data Protection Law.

Personal Data Inventory and Personal Data Processing Register

Maynooth University maintains an inventory of the personal data that it holds. The inventory and register include the following details about the University's processing of personal data:

(a) categories of personal data held and processed
(b) the purposes of the processing;
(c) categories of data subjects to which the personal data relates;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
(e) details of transfers of personal data to a third country, including the identification of that third country;
(f) where possible, time limits for retention; and
(g) where possible, a description of the technical and organisational security measures that are undertaken to protect the data.
(h) Contact details of the controller and the Data Protection Officer;

The University's Personal Data Inventory and Personal Data Processing Register is maintained by the Data Protection Officer and reviewed on a periodic basis

Privacy by Design and Default

Two of the key principles under Data Protection Law are that data protection compliance shall be implemented by design and by default. This means:

(a) **Data Protection by Design –** Data protection by design means that the purposes of the processing of personal data are designed, from the beginning, with data protection in mind. The University seeks, where possible, to implement and practice methods of data minimisation. Other methods of data protection by design include staff training and audit and policy reviews in the context of data protection.
(b) **Data Protection by Default –** Maynooth University aims to ensure that, by default, only personal data which is necessary for each specific purpose of the processing are processed. This obligation applies to the amount of personal data collected, the extent of its processing, the period of its storage and their accessibility.

Maynooth University ensures data protection by design and data protection by default through, among other things, following the procedures set out below, whenever it implements a new project.

Data Protection Impact Assessment

Maynooth University is obliged to ensure that a Data Protection Privacy Impact Assessment ("**DPIA**") is undertaken before commencing any processing that is likely to result in a "high risk" to data subject's rights and freedoms. A DPIA form can be found at this address: https://www.maynoothuniversity.ie/data-protection/policies-privacy-notices

Examples of such processing that are given in the GDPR are the "large scale" processing of sensitive personal data or profiling activities. The University will also considers whether a Privacy Impact Assessment is necessary when it engages in changes to its processing of personal data that do not require a DPIA. Both DPIAs and PIAs are carried out before the processing activity in question is commenced.

Training

Maynooth University aims to ensure that staff and students whose roles involve the processing of personal data are made aware of and, when necessary, receive training in respect of data protection law and principles.

An online training module, available to all staff, can be found here:
https://www.maynoothuniversity.ie/data-protection/online-gdpr-training-staff

10. Data Incidents and Breaches

Data Protection Law defines a 'personal data breach' 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.

It is essential that all data security incidents and breaches or suspected incidents and breaches are reported to the Data Protection Office immediately: dataprotection@mu.ie Tel +353 1 7083654.

Where a personal data breach occurs, it must be reported to the Data Protection Commissioner's Office without delay and, where feasible, not later than 72 hours after the University becomes aware of the breach.

11. Responsibilities

- Maynooth University has overall responsibility for ensuring compliance with the Data Protection law.
- All employees and students of the University who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation.
- Students and Staff must report any personal data security breaches to the Data Protection Officer.
- The Data Protection Officer will assist the University and its staff in complying with the Data Protection legislation by providing and facilitating, support, assistance, advice and training.

12. Contact

Contact us
If you wish to make an access request
Or exercise your rights as outlined under data protection law
Or
have any queries about this policy please contact the University's Data Protection Officer:

E-mail: dataprotection@mu.ie

Telephone: +353 1 7083654

Postal Address:
Data Protection Officer,
Room 17,
Rye Hall Extension,
North Campus,
Maynooth University,
Maynooth,
County Kildare.

Further information is available on the University web:
https://www.maynoothuniversity.ie/data-protection

Data Controller
Maynooth University
Maynooth
County Kildare
Ireland

W: www.maynoothuniversity.ie

13. Complaints

If you are dissatisfied with the decision of the Data Protection Officer, you have the right to make a complaint to the Data Protection Commission**:** https://www.dataprotection.ie/

Phone	01 7650100 / 1800 437 737
E-mail	info@dataprotection.ie
Postal Address	Data Protection Commission 21 Fitzwilliam Square South Dublin 2 D02 RD28 Ireland

14. Updates

Maynooth University may occasionally update this policy. We encourage you to periodically review this policy for the latest information on our privacy practices. We also encourage you to advise us of any changes to your personal data which we hold so that we can ensure that your personal data is accurate and up to date.

15. General

All Data Protection issues should be addressed to the:
Data Protection Officer

dataprotection@mu.ie
Tel +353 1 7083654

Controller
Maynooth University
Maynooth
County Kildare
Ireland
W: www.maynoothuniversity.ie