

Maynooth University Foundation Data Protection Policy

Author / Policy Owner:	Data Protection Office
Creation Date:	1 st June 2021
Review Date:	1 st June 2022
Version:	1 st June 2021
Scope:	This policy applies to all staff, students and public who interact with Maynooth University Foundation
Related Policies:	Student Data Privacy Notice Staff Data Privacy Notice Development and Alumni Office Data Protection Policy Personal Data Security Incident/Breach Management Procedures Data Protection Impact Assessment document

Revision History

Date of this revision:	Date of next review: 1st June 2022
------------------------	------------------------------------

Table of Contents

1. Introduction..... 4

2. Purpose 4

3. Definitions..... 4

4. Principles of Data Protection Law 5

5. Data Subject Rights 6

6. Third Party Processors..... 7

7. Documenting and Monitoring Compliance 7

8. Marketing..... 8

9. Data Security 10

10. Data Security Incidents 10

11. Responsibilities 10

12. Contact..... 11

13. Complaints 11

14. Updates 11

Maynooth University Foundation CLG Data Protection Policy

1. Introduction

Maynooth University Foundation CLG (“MU Foundation”) collects, processes and uses personal data (in electronic and manual format) about:

- alumni and non-alumni of Maynooth University who choose to make donations to MU Foundation for the benefit of Maynooth University;
- individuals who might be willing to make such donations or otherwise support Maynooth University;
- personnel of other organisations with whom MU Foundation interacts in the ordinary course of its operations, including Maynooth University;
(collectively, “External Personnel”); and
- personnel of MU Foundation (“Internal Personnel”);

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 MU Foundation under Data Protection Law and describes the steps to be taken to ensure compliance with those obligations.

This policy applies where MU Foundation acts as a controller regarding the processing of personal data. MU Foundation also acts as a processor and processes personal data on behalf of Maynooth University. Where MU Foundation acts as a processor on behalf of Maynooth University, Maynooth University is responsible for instructing MU Foundation as to how personal data are to be processed and MU Foundation complies with Maynooth University’s instructions in this regard.

This policy does not apply, among other things, where:

- MU Foundation processes personal data as a processor on behalf of Maynooth University; or
- Maynooth University, acting as a controller, processes personal data for its own purposes.

This policy applies to MU Foundation’s officers and employees and any person who provides services to or acts on behalf of MU Foundation.

2. Purpose

This policy is a statement of MU Foundation’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 MU Foundation’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, determines 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.

DARO means the Development and Alumni Relations Office of Maynooth University.

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, 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) 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.

University means Maynooth University.

4. Principles of Data Protection Law

As a controller, MU Foundation complies with its responsibilities under Data Protection Law in connection with the processing of personal data in accordance with the following key data protection principles:

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

For personal data to be obtained fairly, data subjects must be provided with certain information, generally at the time at which the personal data is obtained. It is MU Foundation's policy to do so by setting out the relevant information in an appropriately worded data protection/privacy notice and to provide this to data subjects at the time that data is collected, where it is possible to do so. The information that needs to be provided to data subjects includes: the identity and contact details of the controller; the purposes and lawful basis for the processing activities; the recipients of personal data; and, where the personal data may be transferred to a non-EEA country, the safeguards which have been adopted in relation to such transfer.

For personal data to be processed fairly, MU Foundation must be in a position to rely on one of a range of 'legal grounds' that are set out under relevant Data Protection Law. Where MU Foundation processes personal data relating to External Personnel, generally it does so on the basis that this is necessary for the purposes of legitimate interests pursued by MU Foundation or a third party (such as Maynooth University), provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.

In limited circumstances, as an alternative to relying on this 'legitimate interests' ground, MU Foundation may process personal data relating to External Personnel:

- based on their consent, where they have provided specific, informed and freely given consent to the processing of their personal data;
- where this is necessary to comply with a legal obligation applicable to MU Foundation;
- or
- where this is necessary to perform a contract with the relevant individual or to take steps at their request prior to entering into a contract.

For Internal Personnel, the grounds for processing personal data relied upon by MU Foundation are:

- where this is necessary for the purposes of legitimate interests pursued by MU Foundation or a third party (such as Maynooth University), provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects;
- where this is necessary to comply with a legal obligation applicable to MU Foundation;
- where this is necessary to perform a contract with the relevant individual or to take steps at their request prior to entering into a contract; or
- in limited circumstances, based on their consent, where they have provided specific, informed and freely given consent to the processing of their personal data.

The GDPR specifies certain "special categories of personal data" which require protection, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. For special categories of personal data to be processed fairly it must fall within one of the lawful bases for such processing (which are more limited). MU Foundation generally does not process special categories of personal data. Where it does, it typically relies on:

- obtaining explicit consent as its legal basis for processing such special category personal data; or
- in connection with Internal Personnel, that the processing is necessary for the purposes of carrying out obligations and exercising rights in the field of employment and social security and social protection law; or
- that the processing is necessary for the establishment, exercise or defence of legal claims.

- (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.**

MU Foundation only processes personal data for purposes that are specific, lawful and clearly stated in its data protection/privacy notices. MU Foundation will not collect information about people routinely and indiscriminately without having a sound, clear and legitimate purpose for doing so. MU Foundation's practice is to keep personal data for lawful purposes which are set out in the data protection/privacy notices that are made available externally (e.g. to donors and potential donors) and internally to MU Foundation personnel.

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

MU Foundation's practice is to ensure that it collects and keeps only such personal data as is necessary for the purposes set out in its data protection/privacy notices. The types of information about external personnel (e.g. donors and potential donors) and internal personnel which MU Foundation collects and keeps are periodically reviewed to ensure compliance with this requirement, and information that is no longer required is deleted in accordance with MU Foundation's Record Retention Policy.

- (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.**

MU Foundation seeks to ensure that the personal data it holds is at all times accurate, complete and up to date. MU Foundation requests data subjects to notify it of changes to their personal data (e.g. upon a change of address) in its data protection/privacy notices. Keeping contact details relating to External Personnel up to date is difficult and External Personnel are encouraged to update MU Foundation regarding any changes to such details. MU Foundation 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 upon becoming aware of this.

- (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.**

MU Foundation's policy is to ensure that its record retention, archiving and destruction practices give effect to this principle. MU Foundation's record retention schedule contains details of the periods for which MU Foundation 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.**

MU Foundation's practice is to ensure that access to personal data which is held by MU Foundation is restricted on a 'need to know' basis. To the extent that any third party processes personal data on behalf of MU Foundation, MU Foundation ensures that there is a written agreement in place which includes, among other things, appropriate security obligations regarding such personal data.

5. Data Subject Rights

Data subjects for whom MU Foundation 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. MU Foundation 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. These include where the processing is based on it being “necessary for the purposes of legitimate interests”, which MU Foundation relies on to cover much of its processing of personal data, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects. Where an individual objects to processing on this basis, MU Foundation must cease that processing unless there are compelling legitimate grounds for it to continue, which override the rights and freedoms of the individual.
- (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 be forgotten.** 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, MU Foundation may be required to provide a data subject with a copy of their personal data in a structured, commonly used and machine readable format.

MU Foundation is obliged to comply with any requests by a data subject to exercise the above rights within strict timelines imposed under Data Protection Law (generally 30 days).

6. Third Party Processors

Engaging Processors

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

Prior to engaging processors, MU Foundation:

- (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.

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

Under Data Protection Law, MU Foundation 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 is in place between the data exporter and the data importer and there are enforceable data subject rights and effective legal remedies available to data subjects;
- (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.

7. Documenting and Monitoring Compliance

Ensuring Compliance

MU Foundation has in place policies and procedures to ensure that it can demonstrate its compliance with Data Protection Law.

Data Inventory

MU Foundation maintains an inventory of the personal data that it holds, which includes the following details about MU Foundation'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) 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;
- (g) where possible, a description of the technical and organisational security measures that are undertaken to protect the data; and
- (h) contact details of the controller.

MU Foundation's Data Inventory is maintained by Maynooth University on behalf of MU Foundation.

Data Protection by Design and by 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 is the notion that the means and purposes of the processing of personal data are designed, from the beginning, with data protection in mind. The principle requires MU Foundation to implement both technical and organisational measures that will guarantee and protect the privacy of data subjects. MU Foundation seeks, where possible, to implement and practice methods of data minimisation (which could include, where feasible, the pseudonymisation of personal data). 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** – MU Foundation implements appropriate technical and organisational measures 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. In particular, such measures ensure that by default a data subject's personal data is not made accessible without the data subject's intervention to an indefinite number of natural persons.

MU Foundation 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

MU Foundation 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. Examples of such processing that are given in the GDPR are the "large scale" processing of sensitive personal data or profiling activities.

MU Foundation also considers whether a Privacy Impact Assessment ("PIA") 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

MU Foundation aims to ensure that MU Foundation personnel 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.

8. Marketing

Compliance with Data Protection Law

MU Foundation (acting through DARO) may send promotional or marketing communications to individuals where they have sought that information, and where it does so MU Foundation is required to comply with Data

Protection Law only.

MU Foundation may also engage in unsolicited direct marketing to individuals (e.g. to promote objectives pursued by MU Foundation or to seek donations to MU Foundation for the benefit of Maynooth University). For example, MU Foundation (acting through DARO) may at times invite prospective students, alumni or previous course participants to events, or send them information on upcoming courses, or seek donations, etc. In some circumstances such communications may fall within the definition of “unsolicited direct marketing” under applicable law (i.e. where the recipient has not sought the information and it is being sent for marketing or promotional purposes).

MU Foundation complies with its obligations under Data Protection Law regarding unsolicited direct marketing by, among other things:

- ensuring that appropriate wording is included in its data protection notices that it uses when collecting personal data;
- ensuring that it has an appropriate legal basis for its processing of personal data for these purposes (which may be: (a) that the processing is necessary for the purposes of legitimate interests pursued by MU Foundation or a third party, such as Maynooth University, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects; or (b) that consent has been obtained from the relevant individual). As set out in further detail below, in circumstances where ePrivacy law applies and requires an opt-in to be obtained, the only option is to rely on consent; and
- providing an “*unsubscribe*” option at the end of any unsolicited direct marketing communications.

When engaging in unsolicited direct marketing via electronic means, in addition to being required to comply with Data Protection Law, MU Foundation is also required to comply with applicable ePrivacy law. Unsolicited direct marketing via post, for example, is not subject to ePrivacy law and is governed by Data Protection Law only.

Compliance with ePrivacy Law Requirements

In addition to complying with the general principles of applicable Data Protection Law, MU Foundation must also ensure that any unsolicited direct marketing that it undertakes by electronic means complies with the provisions of applicable ePrivacy Law, which is currently set out in Directive 2002/58/EC (the “**ePrivacy Directive**”) as implemented into local law and which will, in the near future, be set out in a new EU Regulation (the “**ePrivacy Regulation**”).

In summary, ePrivacy Law requires a person who uses personal data to send unsolicited direct marketing communications by electronic means (e.g. by email or by text message) to:

- notify data subjects of such proposed use of their personal data when their data is collected and, depending on the method of communication to be used, afford data subjects an opportunity to ‘opt-out’ or, in some cases, to obtain an express ‘opt-in’, to such use of their personal data;
- only send recipients an unsolicited direct marketing communication where an appropriate opt-in or absence of an opt-out, as applicable, has been obtained (as summarised in the table below);
- provide an “unsubscribe” option at the end of any unsolicited direct marketing communication sent by electronic means.

	Email/SMS	Fax	Phone call (by person)	Phone call (automated)
Individual, recent customer	Soft opt-in*	Opt-in	Absence of opt-out	Opt-in
Individual, not recent customer	Opt-in	Opt-in	Absence of opt-out	Opt-in
Corporate entity	Absence of opt-out	Absence of opt-out	Absence of opt-out	Absence of opt-out

* In principle, a ‘soft opt-in’ could be relevant when engaging in unsolicited direct marketing of products or services to an existing ‘customer’, which are similar to products or services provided to that person within the previous 12 months. In practice, however, it is unlikely that the ‘soft-opt in’ will arise in connection with

MU Foundation's activities. In order for MU Foundation to be entitled to rely on a 'soft opt-in' (consisting of the absence of an opt-out from such a person as their basis for sending them a direct marketing communication by email/SMS), all of the following conditions must apply:

- MU Foundation obtained the contact details of the recipient in accordance with Data Protection Law in the context of a sale of a product or service to them;
- the product or service being marketed is MU Foundation's own product or service;
- the product or service being marketed is similar to what was previously supplied to the recipient by MU Foundation;
- the recipient is clearly and distinctly given the opportunity to opt out (a) at the time their details are first collected and (b) in each direct marketing message sent to them; and
- the direct marketing message is sent not more than 12 months after (a) the previous sale of a product or service to the recipient, or (b) the last time the recipient was sent a compliant direct marketing message.

If any of these conditions are not met, then the 'soft-opt in' may not be relied upon and an 'opt- in' would be required to send the relevant individual an unsolicited direct marketing message by email/SMS.

Where MU Foundation is engaging in unsolicited direct marketing by electronic means and:

- is required to have an 'opt-in' under the ePrivacy Regulations, then it will need to rely on consent as its legal basis for processing personal data under Data Protection Law;
- is required to have the absence of an opt-out under the ePrivacy Regulations (including where the soft-opt in applies), then it could rely on the processing being "necessary for the purposes of legitimate interests pursued by MU Foundation or a third party" as its legal basis for processing personal data under Data Protection Law, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.

MU Foundation only uses personal data that it or Maynooth University collects. It does not sell or provide such data to third parties so that they can use it to promote or market their own products or services.

9. Data Security

MU Foundation implements appropriate technical and organisational measures to ensure a level of security appropriate to the risks to personal data that may arise in connection with the processing activities MU Foundation undertakes. Such measures include restricting access to personal data on a 'need to know' basis.

10. Data Security Incidents

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 are reported to Maynooth University's Data Protection Officer without delay, so that the incident can be managed and, if necessary, reported in accordance with best practice and applicable law. MU Foundation might be obliged to notify such incidents to a data protection authority within 72 hours of becoming aware of it and, in specific circumstances, to notify the affected individuals about the incident.

11. Responsibilities

MU Foundation has overall responsibility for ensuring compliance with Data Protection Law in circumstances where it acts as the controller. MU Foundation has engaged Maynooth University (acting through the DARO) to process personal data on MU Foundation's behalf and DARO is responsible for ensuring compliance with this policy regarding its processing of personal data on behalf of MU Foundation.

12. Contact

If an individual:

- wishes to make an access request; or
- exercise their rights under Data Protection Law; or
- has any queries about this policy

they can use the details set out below to contact Maynooth University's Data Protection Officer

E-mail: dataprotection@mu.ie

Telephone: +353 1 70886184

Postal Address:

Data Protection Officer
Maynooth University
Room 17
Humanity House
Maynooth
Co. Kildare

Further information is available on the Maynooth University Website:

<https://www.maynoothuniversity.ie/data-protection/>

13. Complaints

If an individual is dissatisfied with how we process their personal data or handle any data protection request that they make to MU Foundation, they have the right to make a complaint to the Data Protection Commission

Phone Number	+353 761 164 800 / +353 57 868 4800
Fax	+353 57 868 4757
E-mail	info@dataprotection.ie
Postal Address	Data Protection Commission 21 Fitzwilliam Square South Dublin 2 D02 RD28

14. Updates

MU Foundation may occasionally update this policy. We encourage you to periodically review this policy for the latest information on our privacy practices.

Maynooth University
Data Protection Office
Maynooth, Co. Kildare, Ireland.

T +353 1 708 6184 **E** ann.mckeeon@mu.ie **W** maynoothuniversity.ie