Maynooth University
Data Protection Office

# Development and Alumni Relations Office
# Data Protection Policy

| | |
|---|---|
| **Author / Policy Owner:** | Data Protection Office |
| **Creation Date:** | 6th July 2021 |
| **Review Date:** | 6th July 2022 |
| **Version:** | 1st March 2022 |
| **Scope:** | This policy applies to all staff, students, alumni and public who interact with Maynooth University |
| **Related Policies:** | Student Data Privacy Notice<br>Staff Data Privacy Notice<br>Maynooth University Foundation Data Protection Policy<br>Personal Data Security Incident/Breach Management Procedures<br>Data Protection Impact Assessment document |



1

## Revision History

| | |
|---|---|
| Date of this revision: | Date of next review: 6th July 2022 |

**Table of Contents**

# Development and Alumni Relations Data Protection Policy

## 1. Introduction

Maynooth University collects, processes, and uses personal data (in electronic and manual format) about:

- its alumni for a variety of purposes, including for development and alumni relations purposes; and
- non-alumni for development purposes.

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.

Maynooth University maintains and implements a Data Protection Policy that outlines the obligations of Maynooth University under Data Protection Law and describes the steps to be taken to ensure compliance with those obligations generally. This policy is supplemental to thatData Protection Policy.

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 specifically in relation to the processing of personal data relating to:

- alumni of Maynooth University for development and alumni relations purposes;
- non-alumni (such as donors, honorary conferees, event attendees and participants, volunteers, members of MU advisory councils and organisations) for development purposes.

This policy applies not only where Maynooth University (mainly acting via DARO) processes personal data for these purposes, but also where a third party acting as a processor does so on behalf of Maynooth University. The Foundation is one of the third parties that performs somefunctions as a processor on behalf of Maynooth University in connection with these purposes.

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

- Maynooth University, acting as controller, processes personal data relating to alumni of Maynooth University for purposes other than development and alumni relations (e.g. for the purposes of maintaining educational records relating to former students);
- the Foundation, acting as controller, processes personal data relating to alumni of Maynooth University or non-alumni for the Foundations' own purposes, rather than as processor on behalf of Maynooth University (the Foundation maintains its own policiesthat apply in such circumstances); or
- DARO, acting as processor on behalf of the Foundation, processes personal data relating to alumni of Maynooth University or non-alumni in accordance with instructionsgiven to it by the Foundation.

This policy applies to the University's employees and students and any other person who interacts with the University.

## 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, specifically in relation to development and alumni relations activities. 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 purposesand 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 controllerbut 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.

**DPO** means the Data Protection Officer of Maynooth University.

**Foundation** means Maynooth University Foundation Company Limited by Guarantee.

**Personal data** means information relating to a living individual who is or can be identified either directlyor 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 ethnicorigin; 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, Maynooth University will comply with its responsibilities under Data Protection Law in connection with the processing of personal data for development and alumni relations purposes 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 the University's policy to do soby setting out the relevant information in an appropriately worded data protection/privacy noticeand to provide this to data subjects at the time that data is collected, where it is possible to doso. The information that needs to be provided to data subjects includes: the identity and contactdetails 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.

See: Student Data Privacy Notice

For personal data to be processed fairly, the University must be in a position to rely on one of a range of 'legal grounds' that are set under relevant Data Protection Law. Where the University processes personal data relating to alumni or non-alumni for development and alumni relations purposes, generally it does so on the basis that this is necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the University that are provided for by law. The Universities Act 1997 provides that the functions of the University include "to do all things necessary or expedient in accordance with this Act and its charter, if any, to further the objects and development of the university" and that the University may:

- "collaborate with educational, business, professional, trade union, Irish language, cultural, artistic, community and other interests, both inside and outside the State, to further the objects of the university";
- "collaborate with graduates, convocations of graduates and with associations representing graduates of the university both inside and outside the State"; and
- "accept gifts of money, land or other property on the trusts and conditions, if any, not in conflict with this Act, specified by the donor".

As such, the University generally relies on processing being 'necessary for the performance ofa task carried out in the public interest or exercise of an official authority' as its legal basis for processing personal data relating to alumni and non-alumni for development and alumni relations purposes.

In limited cases, the University may also seek and, where granted, rely on consent as its lawful basis for processing personal data relating to alumni or non-alumni for development and alumni relations purposes. However, it would only do so in relation to specific initiatives and not as a general approach. For example, it might:

- invite alumni to participate in a survey on a voluntary basis and only collect and process personal data relating to alumni who decide to participate and consent to thecollecting and processing of personal data relating to them for this purpose;
- seek consent from alumni, or non-alumni, to send them unsolicited direct marketing communications by electric means (such as email or SMS – see section 8 below for further details regarding direct marketing);
- seek details of any dietary requirements from alumni or non-alumni invited to attend a meal and only collect and process personal data relating to individuals who volunteer such information for the purpose of catering for those requirements, based on their consent.

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 (unless one of the exemptions set out under relevant Data Protection Law apply) it must fall within one of the lawful bases for such processing (which are more limited). The University generally does not process special categories of personal data for development or alumni relations purposes, except in limited circumstances (e.g., to cater for dietary requirements related to a medical condition at any event), in which case it would typically rely on obtaining explicit consent as its legal basis for processing such special category personal data.

(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.**

The University only processes personal data for purposes that are specific, lawful and clearly stated. The University will not collect information about people routinely and indiscriminately without having a sound, clear and legitimate purpose for doing so. The University's practice isto keep personal data for lawful purposes which are set out in the data protection/privacy notices that are made available to staff, students and non-alumni. Further information is available on the University Website at: https://www.maynoothuniversity.ie/data-protection

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

The 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. The types of information about alumniand non-alumni which the University collects and keeps for development and alumni relations purposes are periodically reviewed to ensure compliance with this requirement, and information that is no longer required is deleted in accordance with the University'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 tothe purposes for which they are processed, are erased or rectified without delay.**

The University seeks to ensure that the personal data it holds is at all times accurate, completeand up to date. The University requests Staff and Students to notify it of changes to their personal data (e.g. upon a change of address). Keeping personal data and particularly contactdetails relating to alumni and non-alumni up to date is difficult and alumni and non-alumni are encouraged to update the University regarding any changes to such details. 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 upon becoming awarethereof in accordance with the procedures set out in the Documenting and Monitoring Compliance section of this policy and the University's Record Retention Policy.

(e) **Personal data shall be kept in a form that permits the identification of a data subject forno longer than is necessary for the purposes for which the data are processed.**

The University's policy is to ensure that its record retention, archiving and destruction practices give effect to this principle. The University records retention schedule contains details of the periods for which the University retains the various categories of records that it holds.

The University retains personal data relating to alumni indefinitely as part of its requirements to retain academic records. It retains personal data relating to alumni for development and alumni relations purposes indefinitely, unless an alumnus opts out of receiving any communications for development or alumni relations purposes, in which case the University retains limited details in relation to them for the purpose of recording and complying with this 'opt out' only.

The University retains personal data relating to non-alumni for development purposes for an initial period of [3 years] after collecting the information and for a period of no longer than [13 months] after it last communicated with the relevant individual.

(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.**

The University's practice is to ensure that access to personal data which is held by the University is restricted on a 'need to know' basis. 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, among other things, appropriate security obligations regarding such personal data. For example, there is a written agreement between the University and Foundation that governs the processing of personal data by the Foundation, acting as a processor, on behalf of the University.

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

## 5. Data Subject Rights

Data subjects for whom the University holds personal data have the following rights in relation tothe 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. The 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. These include where the processing is based on it being "necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the University that are provided for by law", which the University relies on to cover much of its processing of personal data for development and alumni relations purposes. Where an individual objects to processing on this basis, the University 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, the 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.

The 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 (generally 30 days).

## 6. Third Party Processors

**Engaging Processors**

A processor is a third party that processes personal data on behalf of the 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 withthe requirements under Data Protection Law.

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

Under Data Protection Law, the 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 protectionin 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 thepossible 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 areenforceable 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 hasbeen 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**

The University has in place policies and procedures to ensure that it can demonstrate itscompliance with Data Protection Law.

**Data Inventory**

The University maintains an inventory of the personal data that it holds, which includes details regarding personal data relating to alumni and non-alumni that it processes for development andalumni relations purposes. The inventory includes 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) categories of recipients to whom the personal data have been or will be disclosed includingrecipients in third countries or international organisations;
(e) details of transfers of personal data to a third country, including the identification of thatthird country;
(f) where possible, time limits for retention;
(g) where possible, a description of the technical and organisational security measures thatare undertaken to protect the data; and
(h) contact details of the controller and the DPO.

The University's Data Inventory is maintained by the DPO and reviewed on a periodic basis.

**Data Protection by Design and by Default**

Two of the key principles under Data Protection Law are that data protection compliance shallbe 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 the University to implement both technical and organisational measures that will guarantee and protect the privacy of data subjects. The University 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 –** The University implements appropriate technical andorganisational measures to ensure that, by default, only personal data which is necessaryfor 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'spersonal data is not made accessible without the data subject's intervention to an indefinitenumber of natural persons.

The 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**

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

The University also considers whether a Privacy Impact Assessment ("**PIA**") is necessary whenit engages in changes to its processing of personal data that do not require a DPIA. Both DPIAsand PIAs are carried out before the processing activity in question is commenced.

**Training**

The 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.

## 8. Marketing

**Compliance with Data Protection Law**

The University (acting through DARO) may send promotional or marketing communications to alumni or non-alumni where they have sought that information, and where it does so the University is required to comply with Data Protection Law only.

The University may also engage in unsolicited direct marketing to individuals (e.g. to promote objectives pursued by the University or to seek to raise funds for the University). For example, the University (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).

The University 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 performance of tasks carried out in the public interest or in the exercise of official authority vested in theUniversity that are provided for by

law or (b) that consent has been obtained from the relevant individual). As set out in further detail below, in circumstances where ePrivacylaw 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, the University 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, the University 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 (byperson)** | **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 |

* A 'soft opt-in' is potentially 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. This may arise where a person has paid to attend a courseat the University and the University wishes to promote another similar course to that individual. The University may rely on the absence of an opt-out from such a person as their basis for sending them a direct marketing communication by email/SMS where all of the followingconditions apply:

- the University 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 the University's own product or service;
- the product or service being marketed is similar to what was previously supplied to the recipient by the University;
- 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 saleof 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 the same requirements would apply as if the individual was not a recent customer (i.e. an 'opt-in' would be required to send them an

unsolicited direct marketing message by email/SMS).

Where the University 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 onconsent 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 (includingwhere the soft-opt in applies), then it could rely on the processing being "necessary for the performance of tasks carried out in the public interest or in the exercise of official authority vested in the University that are provided for by law" as its legal basis for processing personal data under Data Protection Law.

The University only uses personal data that it collects for development and alumni relations purposes for its own development and alumni relations activities. 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

The University 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 the University undertakes. Such measures include restricting access to alumni and non-alumni details 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 the DPO without delay, and that the procedures set out in the University's Personal Data Security Incident/Breach Management Procedure are followed. The University 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. Further information is available on the University Website at: https://www.maynoothuniversity.ie/data-protection

## 11. Responsibilities

The University has overall responsibility for ensuring compliance with Data Protection Law. The DARO has responsibility for ensuring compliance with this policy regarding the processing of personal data relating to alumni and non-alumni for development and alumni relations purposes.

All Staff and Students who collect and/or control the contents and use of personal data are also responsible for compliance with Data Protection Law.

The DPO will assist the University and its Staff in complying with Data Protection Law 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 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 7086184

**Postal Address**: Data Protection Officer

Maynooth University
Room 17, Humanity House
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
**T:** +353 1 708 6000
**W:** www.maynoothuniversity.ie

## 13. Complaints

If you are dissatisfied with the decision of the Data Protection Officer, you have the right to makea 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 Commission21 Fitzwilliam Square South Dublin 2 D02 RD28 |

## 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.

## 15. General

All Data Protection issues should be addressed to the:

**Data Protection Officer**
Ann McKeon
**E:** dataprotection@mu.ie
**T:** +353 1 7086184

**Data Controller**
Maynooth University
Maynooth
County Kildare
Ireland
**T:** +353 1 708 6000
**W:** www.maynoothuniversity.ie