TU Dublin Foundation Data Protection Policy

Table of Contents

1. Policy

1.1 Overview

TU Dublin Foundation (TU Dublin Development and Alumni Relations, or the Foundation) is a not-for-profit organisation and registered charity (CHY 14226). TU Dublin Foundation (the Foundation) supports TU Dublin in its' mission as a comprehensive higher education institution, and encourages philanthropic support for TU Dublin from alumni, friends, corporations, staff, charitable trusts and foundations. TU Dublin alumni and friends play an integral part in helping to deliver education programmes, technical and scientific innovation, economic and social development and culture programmes at TU Dublin.

This Data Protection Policy provides information about the ways in which the Foundation collects, stores and uses personal data relating to individuals (Data Subjects). TU Dublin Foundation is the Data Controller of Personal Data and is subject to the Data Protection Acts 1988 to 2018 and the General Data Protection Regulation 2016/679

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

The Foundation is committed to complying with all applicable data protection, privacy and security laws and regulations. The Data Protection Policy adopted by the Foundation creates a common cores set of values, principles and procedures intended to achieve a standard set of universal compliance parameters based on GDPR.

TU Dublin Foundation is responsible for the processing/controlling of a significant volume of personal information. It is vital that everyone is aware of their responsibilities in relation to data protection, as follows:

- It is our responsibility to ensure that personal information is processed in a manner compliant with the relevant data protection legislation and guidance,
- In accordance with the SLA between the Foundation and TU Dublin (the University), the University's Information and Compliance Office on each campus is available to us to provide guidance and advice pertaining to this requirement,

- All Staff must appropriately protect and handle information in accordance with the information's classification, and
- Personal Data is considered confidential information and requires the greatest protection level.

This Data Protection Policy relates to personal data controlled by the Foundation, where data subjects contact or provide personal data to the Foundation directly and also to personal data received indirectly (via a Third Party).

1.2 Purpose

The Foundation intends to meet all relevant Data Protection, privacy and security requirements, whether originating from legal, regulatory, or contractual obligations.

TU Dublin Foundation has established this Policy as an EU Data Protection Framework to comply with all relevant European Data Protection requirements and has aligned same to relevant internal policies, programs and controls.

The Foundation also embraces Privacy by Design and Privacy by Default principles in all its services and functions both current and future. This ensures that the public can maintain a high level of trust in the Foundations' competence and confidentiality while handling data.

1.3 Common Terms and Definitions

For a Glossary of Terms used in this Policy and common terms and definitions relating to Data Protection, see Appendix A (in draft).

1.4 Scope

All Data Protection Policies apply to:

- Any person who is employed by the Foundation who receives, handles or processes personal data in the course of their employment;
- Any alumnus, donor or friend of TU Dublin who receives, handles, or processes personal data in the course of their engagement with the Foundation; and
- Third party companies/individuals (data processors) that receive, handle, or process personal data on behalf of the Foundation.

This applies whether you are on campus, travelling or working remotely.

1.5 Policy Compliance

Compliance

Compliance with our Data Protection Policy will help protect the Foundation against data breaches under data protection legislation, reputational damage to the Foundation and/or an infringement of the rights of employees, alumni, or other relevant third parties.

Non-Compliance

Failure to comply with this policy may lead to disciplinary action. Failure of a third party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

2. Roles and Responsibilities

TU Dublin Foundation Audit and Governance Subcommittee	Review and approve the policy on a periodic basis
Executive Director of Foundation	Responsible for the internal controls of the Foundation, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. Responsible for: • Reviewing and approving all Data Protection Policies and any updates to them, • Ensuring ongoing compliance with the GDPR, • As part of an annual submission to the Committee, provide assurances of compliance with GDPR.
Heads of Functions	• Lead the Data Protection compliance for their Function • Provide guidance to their colleagues • Ensure prompt reporting of data protection breaches originating from their Function
Data Protection Champion	• Work with the University Information and Compliance Office to co-ordinate the Data Protection compliance and risk management function within the Foundation • Respond to queries relating to Data Protection and raise awareness where appropriate
Staff/Alumni/External Parties	• Adhere to the Data Protection Policy of the Foundation • Report suspected breaches of policy to the Executive Director of the Foundation

2.1 Compliance Organisational Chart

See Appendix B for information on the reporting structures within the TU Dublin Foundation (in development).

3. Principles of Data Protection

3.1 Personal Data Processing Principles

The following Data Protection requirements apply to all instances where Personal Data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

The Foundation has established the following high level principles relating to Data Protection in order to comply with relevant European requirements.

- Personal Data shall only be processed fairly, lawfully and in a transparent manner (**Principles of Lawfulness, Fairness and Transparency)**
- Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes **(Principle of Purpose Limitation**)
- Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**Principle of Data Minimisation**)
- Personal Data shall be accurate, and where necessary kept up to date (**Principle of Accuracy**)
- Personal Data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the Personal Data are processed (**Principle of Data Storage Limitation**)
- Personal Data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
    i. prevent and / or identify unauthorised or unlawful access to, or processing of, Personal Data; and
    ii. prevent accidental loss or destruction of, or damage to, Personal Data (**Principles of Integrity and Confidentiality**)

The Foundation whether serving as a Data Controller or a Data Processor, shall be responsible for, and be able to demonstrate compliance with, these key principles (**Principle of Accountability**).

For further information on the Principles of Data Protection, please see the website of the Data Protection Commissioner (DPC):
https://www.dataprotection.ie/en/organisations/principles-data-protection

3.2 Lawful Processing and Consent

The Foundation shall be responsible for, and be able to demonstrate compliance with the following GDPR Requirements:

- To process Personal Data in accordance with the rights of Data Subjects and to communicate with Data Subjects in a concise, transparent, intelligible and easily accessible form, using clear language;

- To only transfer Personal Data to another group or Third Parties outside of the European Economic Area (EEA) in accordance with this Policy, and
- To conduct all Personal Data processing in accordance with legitimate GDPR based processing conditions in particular:
    - Data Subject Consent for one or more specific purposes, and / or
    - Necessary processing for contract performance or contract entry, and / or
    - Legislative/statutory basis underpinning Processing.

Consent
For processing based on Consent, the Foundation must demonstrate that the Data Subject has provided appropriate consent for the specific processing. Further consent must be obtained for any new processing activity.

In particular, Data Processing Consent cannot be implied and must be freely given, specific, informed, unambiguous and provided by an affirmative action (opt-in as opposed to opt-out). Appropriate Consent Request methods include: clauses in contracts and / or click boxes on online forms where Personal Data is entered.

The Foundation has established Consent Withdrawal processes and informs Data Subjects about their right to withdraw consent at any time and the process through which they can achieve this.

Direct Marketing
Any form of marketing to such audiences must follow the TU Dublin Foundation Direct Marketing Policy. For example, it must offer a way for people to 'opt out', and this preference should be recorded to ensure that they do not receive future communications.

The Foundation will communicate with TU Dublin Alumni who have consented to direct marketing within the last five years, or where the electronic contact details have been obtained in the course of a service (or event) within the last twelve months and the direct marketing material relates to a 'similar product or service', provided the individual was given an opportunity to refuse such contact at the time the data was collected, also known under electronic marketing rules as a 'Soft Opt–In'.

The TU Dublin Graduate Network collects minimum data from TU Dublin at the time of graduation, including name, county, date of birth, educational course completed, award and year of graduation. Other contact details including e-mail address are collected directly from alumni at graduations, on our website or at events.

This data is used to keep in touch with Alumni usually via e-mail, by sending a quarterly e-zine, event invitations to events in Ireland and abroad, class reunion invitations or messages from your School. Alumni also receive information from TU Dublin Foundation to further our charitable aims including for fundraising purposes.

Data Subjects have the right to unsubscribe to any of our communications by emailing graduate.network@tudublin.ie or by clicking the 'unsubscribe' link included on all communications.

For further information, see the TU Dublin Foundation Direct Marketing Policy in Appendix C (in draft).

Processing of Special Categories of Personal Data
The Foundation will not process Special Categories of Personal Data unless:

- The Data Subject expressly consents, and / or
- It is necessary to carry out Data Controller's obligations or exercise Data Subject's specific rights in the field of employment and social security and social protection law, and / or
- It is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity, and / or
- It is in the Vital Interest of the Data Subject. The Foundation may only process such data where it is necessary to protect a Data Subject's vital interest in the event that this subject is physically or legally incapable of giving consent. For example this may apply where the Data Subject may require emergency medical care. Only the Executive Director of the Foundation and / or the Company Secretary of the Foundation may authorise this exemption and only in accordance with relevant national legislation.

3.3 Transparency – Data Protection Notices (Fair Disclosure Notices)

To ensure fair and transparent processing activities, the Foundation provides Data Protection Notices to Data Subjects when directly collecting data. This Policy includes Data Protection Notices for Students (in draft), for Staff (see TU Dublin Data Protection Notice for Staff) and for Alumni (in draft).

These notices must be:

- Provided at the first contact point with the Data Subject or as soon as reasonably practicable,
- Provided in an easily accessible form,
- Written in clear language, and
- Made in such a manner as to draw attention to them.

If we use Consent as the Processing Personal Data condition, then this Consent should, where possible, be obtained at the data collection point, recorded and kept up to date.

See Appendix D and E for Data Protection Notices for Students and Alumni (in draft).

3.4 Data Collection from Third Party Sources

In addition to Section 3.3 above, when the Foundation collects Personal Data from a Third Party (i.e. not directly from a Data Subject), the Data Controller must provide Data Protection notices to the Data Subject either at the time of collection or within a reasonable timeframe that is no more than 30 days post collection.

3.5 Data Minimisation and Retention

The Foundation should limit Personal Data collection to what is directly relevant and what is necessary to accomplish a specified purpose.

Please see Appendix F for the Foundation's Data Retention Policy and Schedule (in draft).

3.6 Data Use Limitation

The Foundation must only collect Personal Data for specified, explicit and legitimate purposes.

3.7 Data Accuracy

The Foundation must ensure that any Personal Data collected is complete and accurate and maintained in an accurate, complete and up-to-date form as its purpose requires.

3.8 Data Storage Limitation

The Foundation must only keep Personal Data for the period necessary for permitted uses. We shall establish a destruction date and / or review schedule when defining a Personal Data permitted use under the stated purpose. This shall be recorded and aligned to the University's Data Retention Policy and Schedule. See Appendix F for the Policy and Schedule (in development).

3.9 Security of Personal Data (Integrity and Confidentiality)

Information Security
The Foundation shall ensure Personal Data security through appropriate physical, technical and organisational measures.

In accordance with the SLA between TU Dublin and the Foundation, the University is responsible for the Foundation's IT services and must adequately address European Data Protection requirements to relevant University IT Policies and Procedures.

Data Breach (Unauthorised Disclosure)
No employee or agent shall disclose Data Subject's Personal Data (including Personal Data or Special Categories of Personal Data), except where this Policy allows such disclosures.

Staff must report all suspected incidents of unauthorised access to the Executive Director of the Foundation. Incidents include disclosure, loss, destruction or alteration of personal data, regardless of whether it is in paper or electronic form. The Foundation must establish formal procedures and a point of contact to report all potential unauthorised disclosure incidents.

Please see the Foundation's Data Breach Management Guidelines in Appendix G (in draft) and the Data Breach Report Form in Appendix H (in draft) for further information.

4. Data Protection Practice / Accountability Requirements

4.1 Data Protection by Design and by Default

Privacy by Design is an essential requirement that involves minimising privacy risks to individuals. It is the consideration of data protection implications at the start or re-design of any product, service, system, IT application or process that involves the processing or personal data. It fosters a culture of embedding privacy by design into operations and ensuring proactivity instead of reactivity.

Privacy by Default promotes that, where possible, having regard to business implications and the rights of the data subject, the strictest data protection settings are applied automatically to any project.

4.2 Data Protection Impact Assessment (DPIA)

When the Foundation undertakes a processing activity which would be likely to have a privacy impact upon students, staff, donors, alumni and / or friends of the University, we should consider if a Data Protection Impact Assessment is required. A Data Protection Impact Assessment (DPIA) is a tool, required by GDPR, which can help the Foundation to identify the most effective way to comply with its Data Protection obligations as well as meeting individuals' expectation of privacy by facilitating the identification and remediation of risks in the early stages of a project. It should also identify measures which would help to reduce risks. Therefore, DPIAs are an integral part of taking a Privacy by Design approach to processing of Personal Data.

The Foundation's Data Protection Impact Assessment Template can be found in Appendix I (in development).

4.3 Record of Processing Activity and Data Inventory

The Foundation is required under GDPR to maintain a Record of Processing Activities (ROPA) under its responsibility. That record contains details of why the Personal Data is being processed, the types of individuals about which information is held, who the Personal Data is shared with and when such Data is transferred to countries outside the EU.

See Appendix J for the Foundation's ROPA (in development). The Foundation will review these records periodically and will update same accordingly.

4.4 Transfer and Sharing of Data

The Foundation may disclose Personal Data and Sensitive Personal Data (Special Category Personal Data) to external agencies to which it has obligations or a legitimate reason. Such sharing should be noted in the relevant Data Protection Notices.

The third party is operating as a Data Processor and meets the requirements of GDPR. Where a third party is engaged for processing activities there must be a written contract or equivalent (Data Sharing Agreement) in place which shall clearly set out respective parties responsibilities and must ensure compliance with relevant European and local Member State Data Protection requirements/legislation.

5. Data Subjects Rights

The Foundation shall maintain appropriate processes and procedures to address Data Subjects rights under GDPR.

Data Subjects have the following rights under Data Protection Law, subject to certain exemptions, in relation to their personal data:

Right	Explanation
Information	The right to be informed about the data processing the Foundation does.
Access	The right to receive a copy of and/or access the personal data that the Foundation holds about you.
Portability	The right to request that the Foundation provides some elements of your personal data in a commonly used machine readable format in order to provide it to other organisations.
Erasure	The right to erasure of personal data where there is no legitimate reason for the Foundation to continue to process your personal data.
Rectification	The right to request that any inaccurate or incomplete data that is held about you is corrected.
Object to processing	The right to object to the processing of your personal data by the Foundation in certain circumstances, including direct marketing material.
Restriction of processing concerning the data subject	The right to request the restriction of processing of personal data in specific situations where: (i) You contest the accuracy of the personal data; (ii) You oppose the erasure of the personal data and request restriction instead; (iii) Where the Foundation no longer needs the data but is required by you for the establishment, exercise or defence of legal claims.
Withdraw Consent	If you have provided consent for the processing of any of your data, you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn. This can be done by contacting the Foundation (contact details below).
The right to complain to the Data Protection Commissioner	You have the right to make a complaint in respect of our compliance with Data Protection Law to the Office of the Data Protection Commissioner.

In order to exercise any of the above rights, please the Foundation using the contact details in Section 9 below.

5.1 Subject Access Requests (SARs) and Subject Rights Requests (SRRs)

Alumni, students, staff, donors or friends of TU Dublin can contact the Executive Director of the Foundation to discuss their request requirements prior to making a formal request in order to maximise the likelihood that their request will be fulfilled in a timely, efficient and satisfactory manner. External requests for personal data should all be directed to the Data Protection Champion for response.

All Subject Access Requests are requested to be made via the Request Forms that are available on the Foundation's website. See Appendix K for the Foundation's Subject Access Request Form (in development).

5.2 Fees and refusals of SARs under GDPR

There is no fee for Subject Access Requests. However, under GDPR, the Foundation reserves the right where requests from a data subject are manifestly unfounded or excessive in nature to either charge a fee to cover the administrative costs of providing the personal data or refuse to act upon the request.

6. Personal Data Protection Incident (Breach)

6.1 Data Breach

TU Dublin Foundation is legally required to notify the Office of the Data Protection Commissioner where a personal data breach is likely to result in a risk to data subjects' rights and freedoms. The Foundation is required to notify the Data Protection Commissioner within 72 hours after having become aware of the Personal Data breach.

For further guidance on recognising and managing a data breach, please see the TU Dublin Foundation Data Breach Management Guidelines in Appendix G (in development).

Please see Appendix H for the Foundation's Data Breach Report Form (in draft).

7. CCTV

The Foundation does not operate CCTV; however, if Data Subjects attend events on the TU Dublin campuses, their image may be recorded by the TU Dublin University CCTV system. For further information on TU Dublin's CCTV Policy, see here.

8. Training – Education and Awareness

In accordance with the SLA between the Foundation and the University, staff of the Foundation have access to and must complete the mandatory GDPR training, as made available by the University. The Foundation is committed to the provision of

Data Protection training to ensure all staff are aware of their respective obligations under Data Protection regulation.

Staff are expected to:

- Acquaint themselves with, and abide by, the rules of the full suite of Data Protection Policies;
- Read and understand all Data Protection Policies;
- Understand what is meant by 'Personal Data' and 'Sensitive Category Personal Data' and know how to handle such data; and
- Not jeopardise individuals' rights or risk a contravention of the Act.

9. Data Protection Champion

The Foundation has nominated a Data Protection Champion as the point of contact for all data privacy queries that alumni, donors, students or friends of the University may have including subject access requests. The contact details of the Data Protection Champion are available on the Foundation website.

The contact details for the Data Protection Champion are as follows: foundation@tudublin.ie.

10. Accountability

The Foundation monitors compliance with Data Protection policies and procedures by way of an annual submission, provided to the TU Dublin Foundation Audit and Governance Subcommittee.

11. Supervisory Authority (Data Protection Commissioner)

The Office of the Data Protection Commissioner (DPC) is the Irish Statutory Authority for GDPR. Please see https://www.dataprotection.ie/ for further information on the Office of the Data Protection Commissioner.

12. Changes to the TU Dublin Foundation Data Protection Policy

This Data Protection Policy will be subject to revision at least every two years.

Date of this Revision: 11 May 2023