Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

# Data Protection Policy

## 1. Context

Trinity College Dublin, the University of Dublin ('Trinity College'/'the University') acquires, processes, uses, discloses (where permissible by law) and retains personal data of individuals when carrying out its functions. These individuals include students, staff, research participants, members of the public and other persons who engage with the University.

This processing is regulated by Irish and European data protection legislation, specifically the Data Protection Acts 1988-2018 and General Data Protection Regulation (GDPR) (EU) 2016/679 ('data protection law') which strengthen the rights of individuals and place specific data processing obligations on organisations.

## 2. Purpose

This purpose of this policy is to provide specific information and guidance to students, staff and other relevant individuals, in order to ensure consistent application of and continued compliance with data protection law at Trinity College.

## 3. Benefits

Trinity College respects the privacy rights of individuals when processing personal data. Moreover, the protection of personal data is central to the University's information security and records management practices.

This policy is a statement of the University's commitment to safeguard the privacy rights of individuals in accordance with data protection law.

The policy applies to all University-controlled activities in which personal data is processed and provides a compliance framework for Trinity College staff, students and other stakeholders.

## 4. Scope

This policy applies to:

- staff employed by Trinity College who process personal data during the course of their employment for academic, research, administrative and/or other purposes.

This includes, but is not limited to, permanent, part-time, casual, temporary, honorary, visiting and voluntary staff as well as contractors, agency workers and students employed by the University;

- students of Trinity College who process personal data during the course of their studies for academic, research and/or other purposes;
- individuals, including but not limited to, visitors on research and work placements and secondments who process personal data in the course of their access to Trinity College systems and premises.

This policy applies to personal data processed by Trinity College in paper and electronic format and is not restricted by location or form of access.

## 5. Definitions

Personal data: Any information relating to an identified or identifiable person who can be identified, directly or indirectly, by reference to an identifier such as name, image, identification number, location data or online identifier.

Data controller: An entity which determines the purposes and means of the processing of personal data. Trinity College is a data controller in relation to personal data relating to its staff and students.

Data processor: An entity which processes personal data on behalf of the controller. In certain instances Trinity College is a data processor when providing a service to another entity (e.g. analysis of data on behalf of a third party).

Processing: Any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special categories of personal data: Data revealing an individual's racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, data relating to trade union membership, genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health and data concerning an individual's sex life or sexual orientation.

Data Protection Officer: The appointed member of staff at Trinity College responsible for ensuring data protection compliance at the University.

## 6. Principles of Data Protection

Trinity College is responsible for demonstrable compliance with the principles of data protection when processing personal data ('accountability'). These principles are set out under Article 5 GDPR and state that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the individual ('lawfulness, fairness and transparency');
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- accurate and, where necessary, kept up to date ('accuracy');
- kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation'); and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

## 7. Policy

### 7.1 Legal basis for processing personal data

Trinity College shall process personal data under an appropriate legal basis, where at least one of the following conditions is met:

- the individual has consented to processing;
- processing is required due to a contract;
- processing is necessary for compliance with a legal obligation;
- processing is necessary to protect an individual's vital interests;
- 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 University;
- processing is necessary for the legitimate interests of the University or a third party and does not interfere with the rights and freedoms of individuals.

Trinity College is classified as a public body under the Universities Act, 1997. As such, the use of the 'legitimate interests' condition is not applicable to Trinity College's statutory functions but may be relied-upon as a legal basis for processing that is not related to the University's statutory functions.

Where Trinity College relies on consent as a legal basis for processing personal data, the University must:

- obtain the individual's specific, informed and freely given consent;
- ensure that the individual gives consent by a statement or clear affirmative action;
- retain evidence of that statement/affirmative action; and
- allow the individual to easily withdraw their consent at any time if they so wish.

The processing of special categories of personal data requires additional conditions to be met pursuant to Article 9 GDPR and sections 45-55 of the Irish Data Protection Acts 1988-2018.

**7.2 Rights of individuals**

Trinity College shall respond to all rights requests and protect the rights of individuals under data protection law. Detailed guidance and support on upholding individuals' rights is available from the Data Protection Officer.

The right to be informed: Individuals should be informed about the processing of their personal data. There are specific provisions set out under data protection law as to information which should be provided to individuals via a privacy notice when collecting personal data.

The right of access: Individuals have the right to make an access request for a copy of their personal data and to exercise that right easily and at reasonable intervals.

The right to rectification: Individuals have the right to have inaccurate personal data about them rectified.

The right to erasure: This is also known as the 'right to be forgotten'. Individuals have the right, under certain circumstances, to have their personal data erased.

The right to restrict processing: Individuals have the right, under certain circumstances, to request the restriction of processing of their personal data.

The right to data portability: Individuals have the right to obtain their personal data and reuse the data via different platforms and services under certain circumstances.

The right to object to processing: Individuals have the right, under certain circumstances, to object to the processing of their personal data.

These rights are not absolute and subject to certain exemptions under data protection law.

### 7.3 Data protection by design and by default

Trinity College ensures that data protection is incorporated into systems and processes from the outset of processing as standard practice. This is achieved by embedding data privacy and security features, settings and controls directly into the design of University projects and systems.

Trinity College acknowledges that a Data Protection Impact Assessment ('DPIA') should be carried out in certain instances. Trinity College requires DPIA completion as a key component of system and process design, in particular where processing utilises new technologies and, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of individuals.

Examples of circumstances in which a DPIA is likely to be required include: health research as defined under the Health Research Regulations, processing of large quantities of personal data, where there is automatic processing/profiling of individuals, processing of special categories of personal data, or monitoring of publicly accessible areas such as CCTV or location tracking. The DPIA is a mechanism for identifying and examining the impact of new initiatives or new technologies and putting in place measures to minimise or reduce risks.

Staff and students intending to implement processes which require a DPIA should contact the Data Protection Officer for support.

### 7.4 Records of processing activities

Trinity College maintains records of processing activities involving personal data as required under data protection law. The University is also required to hold a register of personal data which it processes in its capacity as a data processor.

### 7.5 Sharing of personal data

Where Trinity College engages a third-party processor to process personal data the University implements data processing agreements, carries out due diligence and conducts information security audits where appropriate.

Such external processing includes (but is not limited to):

- IT systems and services
- HR services, including payroll, expenses, sick leave and annual leave management and pensions
- Student and staff surveys
- Transfers to third parties for research purposes

Staff and students intending to share University-controlled data with external organisations should contact the Data Protection Officer for support.

### 7.6 International data transfers

Chapter V GDPR imposes restrictions on international data transfers. These restrictions are in place to ensure that the level of protection and accountability afforded by EU law is not undermined. Trinity College transfers personal data to countries or organisations outside of the European Economic Area ('EEA') where there is adequate protection in place, in compliance with conditions for transfer as set out under Chapter V.

Staff and students intending to transfer University-controlled personal data outside of the EEA should contact the Data Protection Officer for support.

### 7.7 Data security

Trinity College implements appropriate technical and organisational measures to preserve data security and mitigate risk in order to safeguard personal data.

Personal data under the control of Trinity College should be processed in accordance with the University IT Security Policy and Records Management Policy.

University-controlled data processed using Cloud-based services must be managed in accordance with the University Cloud Computing Policy and Guidelines.

### 7.8 Data breach notifications

Trinity College has developed Personal Data Breach Procedural Guidelines to assist in identifying, investigating, reviewing and reporting incidents involving the unauthorised disclosure, loss, destruction or alteration of personal data.

The Data Protection Officer should be notified of such incidents immediately.

### 7.9 Data protection training

Trinity College provides training in data protection, information security and good research practice. University staff, students and researchers should complete relevant training and awareness activities which are provided to support compliance with this policy.

### 7.10 Data Protection Officer

Trinity College, as a public body, is required to appoint a Data Protection Officer. The Data Protection Officer must be consulted on all matters at the University which relate to the protection of personal data. The Data Protection Officer is independent, bound by confidentiality and reports to the Board of Trinity College. Individuals should contact the Data Protection Officer with regard to all issues related to processing of their personal data and to the exercise of their rights under data protection law.

The role of the Data Protection Officer is:

- to advise Trinity College and its staff and students of their responsibilities under data protection law;
- to monitor compliance with data protection law and relevant University policies;
- to provide training and increase awareness among staff and students;
- to provide guidance on the completion of DPIAs; and
- to act as the contact point with the Data Protection Commission in relation to data breaches, complaints, investigations, audits and any other matters relevant to data protection law.

Contact details:

Data Protection Officer
Secretary's Office, Trinity College Dublin, Dublin 2, Ireland.

Oifigeach Cosanta Sonraí
Oifig an Rúnaí, Coláiste na Tríonóide, Baile Átha Cliath, Baile Átha Cliath 2, Éire.

dataprotection@tcd.ie

**7.11 Data Protection Commission**

The Data Protection Commission is the Irish Supervisory Authority responsible for upholding the fundamental right of individuals to have their personal data protected.

The Data Protection Commission, under statutory authority:

- conducts investigations in the form of data protection audits;
- investigates complaints from individuals in relation to potential infringements of data protection law;
- conducts inquiries and investigations regarding infringements of data protection law and takes enforcement action, including restricting of processing, where necessary;
- imposes administrative fines on data controllers and data processors.

Individuals may complain to the Data Protection Commission in the event that they are dissatisfied with how Trinity College is processing personal data.

Contact details:

Data Protection Commission
21 Fitzwilliam Square South, Dublin 2, Ireland.

An Coimisiún um Chosaint Sonraí
21 Cearnóg Mhic Liam, Baile Átha Cliath 2, Éire.

https://forms.dataprotection.ie/contact

Further information on how the Data Protection Commission regulates data protection rights for individuals and responsibilities for data controllers, as well as general guidance on data protection is available at: www.dataprotection.ie/.

## 8. Sanctions

It is a condition of employment that staff adhere to University policies. It is a condition of the Terms and Conditions of Being a Registered Student at Trinity College that students abide by the College Regulations. Any breach of this policy is considered a serious matter and may result in Trinity College taking disciplinary action in accordance with the University's disciplinary procedures.

## 9. Responsibility

Responsibility for the operation and review of this policy lies with the Secretary to the College.

## 10. Document Control

Approved by: Board of Trinity College Dublin

Date policy approved: December 16th, 2020

Date of next review: May 15th, 2022