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

Data Protection Procedural Guidelines

1. Context

Trinity College Dublin, the University of Dublin, hereafter referred to as "**Trinity College**" or "**the University**", processes personal data for a variety of purposes related to its core functions. This personal data relates to Trinity College students, staff and other entities who are associated with the University.

When processing personal data in paper and electronic format, Trinity College must comply with Irish and European data protection legislation, specifically the EU General Data Protection Regulation ("**GDPR**") and the Data Protection Acts 1988 – 2018 ("**data protection law**"), which seeks to safeguard the privacy rights of natural persons ("**data subjects**").

2. Purpose

This purpose of this document and the associated Code of Practice (Appendix 1) is a statement of Trinity College's responsibility to fulfil its legal, statutory and regulatory requirements under data protection law and affirm that personal data which is under the control of the University is processed in a compliant manner.

3. Benefits

Trinity College fully respects a data subject's fundamental right to privacy and actively seeks to preserve the rights of data subjects who share personal data with the University. Any personal data which is processed by Trinity College will be treated with the highest standards of security and confidentiality, in accordance with data protection law.

4. Scope

This document applies to:

- Staff employed by Trinity College who process personal data in the course of their employment at the University;
- Individuals who are not directly employed by Trinity College, but who are

employed by contractors, who process personal data in the course of their duties for the University; and

- Students of Trinity College who process personal data in the course of their studies.

5. Definitions

Personal data: Information that relates to an identified or identifiable individual.

Data subject: A living person who can be identified, directly or indirectly, from specific information.

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. This does not include Trinity College staff or students who process personal data in the course of their employment or studies.

Processing: Any operation or set of operations which is performed on personal data.

Special categories of personal data: Sensitive personal data, including health data, as defined under Article 9 GDPR.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional, separated information.

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 must adhere to the general principles of data protection when processing personal data. These principles are set out under Article 5 GDPR:

Lawfulness, fairness and transparency: Any processing of personal data should be lawful, fair and transparent to data subjects.

Purpose limitation: Personal data should be processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data minimisation: Processing of personal data should be adequate, relevant, and limited to what is necessary.

Accuracy: Personal data should be maintained as accurate and up to date.

Storage limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary.

Integrity and confidentiality (security): Personal data should be processed in a manner that ensures appropriate security and confidentiality, including protection against unauthorised or unlawful access, use or disclosure.

Accountability: Trinity College is responsible for, and must be able to demonstrate, compliance with each of the principles of data protection when processing personal data. Accountability responsibilities should be regarded as perpetual, and will assist in mitigating data breaches and ensuring continual compliance with data protection law.

7. Guidelines

7.1 Legal basis for processing (Lawfulness)

In order to process personal data lawfully, Trinity College must rely upon a satisfactory legal basis for doing so. There are six legal bases set out under Article 6(1) GDPR for processing personal data. University staff, students and associated individuals must determine the most appropriate legal basis before processing personal data in a specific context, and should document the legal basis in a relevant Privacy Statement. The purpose of the processing and the University's relationship with the data subject will determine the appropriate basis for processing.

The legal bases for processing personal data are:

Consent: The data subject has consented to the processing.

Contractual basis: The processing is necessary for the performance of a contract.

Legal obligation: The processing is necessary for compliance with a legal obligation to which Trinity College is subject.

Vital interests: The processing is necessary to protect the vital interests of a data subject.

Public interest / Exercise of Official Authority: The processing is necessary for Trinity College to perform a task in the public interest or for the purpose of its statutory functions.

Legitimate interests: The processing is necessary for the legitimate interests of Trinity College or a third party.

7.2 Special categories of personal data

When processing special categories of personal data it is necessary for the processing to be covered by a legal basis under Article 6 GDPR and by a separate condition set out under Article 9 GDPR.

7.3 Rights of data subjects

Under Chapter III GDPR Trinity College is required to provide the following rights for data subjects:

The right to be informed: Data subjects must be informed about the processing of their personal data.

The right of access: Data subjects are entitled to make an access request for a copy of their personal data.

The right to rectification: Data subjects are entitled to have inaccurate personal data rectified.

The right to erasure: Data subjects are entitled to ask organisations to delete their personal data. This right is subject to exceptions.

The right to restrict processing: Data subjects have the right to request the restriction of processing. This right is subject to exceptions.

The right to data portability: Data subjects may obtain and reuse their personal data across different platforms and services.

The right to object to processing: Data subjects are entitled to object to certain types of processing and restrict entities from continuing to process their personal data.

7.4 Records of processing activities

Trinity College is required under Article 30 GDPR to maintain records of processing activities involving personal data and maintain such records (in writing) in a clear and easy to read format. Trinity College is also required to hold a register of personal data which it processes in its capacity as a data processor.

7.5 Third party data processors

Trinity College engages the services of third parties for certain processing activities. The University carries out due diligence when forming business relationships and utilises information security audits to identify, categorise and record personal data that is processed outside of Trinity College's direct control, so that the data, processing activity, processor and legal basis are recorded, reviewed and easily accessible.

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

- IT Systems and Services
- Legal Services
- HR Services
- Payroll
- Timekeeping and attendance records
- Student and staff surveys

The continued protection of data subject rights and the security of personal data is prioritised when choosing a processor. Trinity College recognises the importance of adequate and reliable outsourcing for processing activities as well as the University's obligations under data protection law for data processed by a third party.

Trinity College staff and students must ensure that processing is limited to third parties operating under formal agreements which satisfy the requirements of Article 28 GDPR. Staff and students intending to engage the services of third party processors should contact the Data Protection Officer for support.

7.6 International data transfers

The GDPR imposes restrictions on the transfer of personal data to third countries or international organisations located outside of the European Economic Area. These restrictions are in place to ensure that the level of protection and accountability afforded by GDPR is not undermined. Personal data may only be transferred from Trinity College to entities situated outside of the EEA in compliance with the conditions

for transfer as set out under Chapter V GDPR. Staff and students intending to transfer personal data outside of the EEA should contact the Data Protection Officer for support.

7.7 Data security

Under Article 32 GDPR, data subjects processing personal data on behalf of Trinity College must take appropriate measures to preserve data security and mitigate risk in order to safeguard personal data which is under the control of the University.

Comprehensive information on Trinity College IT Security provisions, including University IT Security policies, e-mail security, cloud computing, training, data backup and encryption is available from the Trinity College IT Security website.

Guidance on good housekeeping practices regarding manual data is contained within the Trinity College Records Management Policy.

7.8 Personal data breach notifications

Trinity College has implemented robust and documented controls for identifying, investigating, reviewing and reporting breaches or complaints. The University has developed Personal Data Breach Procedural Guidelines to assist staff and students in identifying and handling incidents involving personal data breaches.

Staff, students and associated entities who discover a personal data breach or incident should immediately inform the relevant Head of School / Unit and / or contact the Data Protection Officer immediately.

7.9 GDPR training for Trinity College staff and students

Trinity College has developed an online GDPR training module for staff This training is a mandatory requirement for all staff who process personal data as part of their duties.

The Data Protection Officer has developed training materials in data protection for students. Further information on training resources and material is available from the Trinity College Data Protection website.

7.10 Data Protection Officer

Pursuant to Article 37 GDPR Trinity College, as a public body, is required to appoint a Data Protection Officer.

Article 38 GDPR states that the Data Protection Officer must be consulted on all matters at Trinity College 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. Data subjects at Trinity College 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, pursuant to Article 39 GDPR, 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 data protection impact assessments; 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 for the Data Protection Officer are:

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 data subjects 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.

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

Contact details for the Data Protection Commission:
https://forms.dataprotection.ie/contact

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

8. Related Documents

- Data Protection Code of Practice
- Information Systems Security Policy
- Network Security Policy
- Internet Use Policy
- Email Use Policy
- Password Policy
- Virus and Spam Policy
- Software Security Policy
- Data Backup Policy
- Disaster Recovery Policy
- Remote Access Policy
- Third Party Access Policy
- Incident Response
- Misuse of IT Facilities Policy
- Legal Compliance Guidelines
- Records Management Policy
- Records Retention Schedule
- CCTV Policy

Data Protection Code of Practice

1. Introduction

Trinity College processes personal data for a variety of purposes related to its core functions. This personal data relates to Trinity College students, staff and other entities who are associated with the University.

When processing personal data in paper and electronic format, Trinity College must comply with Irish and European data protection legislation, specifically the EU General Data Protection Regulation (EU) 2016/679) ("**GDPR**") and the Data Protection Acts 1988 – 2018 ("**data protection law**") which seeks to safeguard the privacy rights of natural persons ("**data subjects**").

2. Purpose of the Code of Practice

The purpose of the Code of Practice is to provide a framework for implementing the University's Data Protection Policy.

The Code of Practice serves as a reference document for staff, students and third parties on the responsibilities for processing personal data which is under the control of Trinity College.

The Code of Practice will be reviewed and updated regularly, based on feedback from members of staff and other stakeholders.

3. Benefits

Ensuring and maintaining the security and confidentiality of personal data is a core priority for Trinity College.

The University has developed policies, procedures and control measures to ensure continued compliance with data protection law, including staff and student training, policy and procedure documents, processing records, audit measures and assessments.

Trinity College operates a *data protection by design and default* approach to processing, assessing the impact of processing personal data and designing systems and processes to safeguard personal data throughout the processing lifecycle.

Trinity College fully respects a data subject's fundamental right to privacy and actively seeks to preserve the rights of data subjects who share personal data with the University.

Any personal data which is processed by Trinity College will be treated with the highest standards of security and confidentiality, in accordance with data protection law.

4. Scope

Personal data may be processed in paper and electronic format or communicated verbally. It is the responsibility of Trinity College staff, students, contractors and all other persons who process personal data in connection with their work at the University to adhere to this Code of Practice.

- Staff employed or engaged by Trinity College who process personal data in the course of their employment or engagement with the University;
- Individuals who are not directly employed by Trinity College, but who are employed by contractors (or subcontractors) or are on secondment from a third party carrying out research, and who process personal data in the course of their duties for the University; and
- Students of Trinity College who process personal data in the course of their studies.

This Code of Practice applies to the processing of personal data on behalf of Trinity College at all locations where Trinity College-controlled personal data is processed, including working from home.

5. Definitions and Application

Article 4 GDPR provides the following definitions:

Personal data: Any information relating to an identified or identifiable natural person. Personal data may be processed in paper and electronic form (Examples of personal data are listed in Appendix 1.

Data subject: A living person who can be identified, directly or indirectly, from specific information, in particular by reference to an identifier such as a name, address, identification number or online identifier.

Data controller: The natural or legal person, public authority, agency or other body which, alone or jointly with others, 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.

Joint controller: An organisation is considered as a joint controller when together with one or more organisations it jointly determines the purposes and means of processing. Joint controllers must enter into an arrangement setting out their respective responsibilities for complying with data protection law. The main aspects of any such arrangement must be communicated to the relevant data subjects. In certain circumstances such as when carrying out collaborative research with other institutes or industry partners, Trinity College is a joint data controller .

Data processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. This does not include Trinity College staff or students who process personal data in the course of their employment or studies.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data.

Special categories of personal data: Categories of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, and which merit specific protection, as the context of their processing could create significant risks to the fundamental rights and freedoms of a data subject.

This data is categorised under GDPR as:

- Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade-union membership;
- The processing of genetic data for the purpose of uniquely identifying a natural person;
- The processing of biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of their personal data.

Supervisory Authority: An independent public authority which is established by a Member State. In Ireland, the relevant Supervisory Authority is the Data Protection Commission.

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 must adhere to the general principles of data protection when processing personal data. These principles are set out under Article 5 GDPR:

Lawfulness, Fairness and Transparency: Any processing of personal data should be lawful and fair. It should be transparent to data subjects as to how and to what extent their personal data is collected and processed. The principle of transparency requires that any information and communication relating to the processing of personal data is accessible and easy to understand, and that clear and plain language is used.

When Trinity College collects personal data directly or indirectly from data subjects, it must provide information regarding the intended processing to the relevant data subject. This information must be provided via a Privacy Statement. In addition, the University must have a legal basis as set out under Article 6 GDPR (see below) for processing personal data.

Purpose Limitation: Personal data should be processed by Trinity College for specified, explicit and legitimate purposes and not further processed by the University in a manner that is incompatible with those purposes.

Data Minimisation: Processing of personal data should be adequate, relevant, and limited to what is necessary. Trinity College staff and students should periodically review processing activities to check that the personal data that is retained is relevant and adequate for the intended purposes, and delete anything that is no longer required.

Accuracy: Trinity College must ensure that personal data is accurate and up to date; taking every reasonable step to ensure that inaccurate personal data is erased or rectified without delay.

Storage Limitation: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. Trinity College has implemented a Records Management Policy and Records Retention Schedule which set out the University's policy on the creation and management of records, including records containing personal data.

Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access, use or disclosure. Furthermore, Trinity College-controlled equipment which is used for the processing of personal data must be protected against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Trinity College has implemented an Information Security Policy and supporting policies which define security controls required to safeguard University Information Systems and ensure the security, confidentiality and integrity of data under the control of Trinity College.

Accountability: Trinity College is responsible for, and must be able to demonstrate, compliance with each of the principles of data protection when processing personal data. Accountability responsibilities should be regarded as perpetual, and will assist in mitigating data breaches and ensuring continual compliance with data protection law.

7. Legal basis for processing

In order to process personal data lawfully, Trinity College must rely upon a satisfactory legal basis for doing so. There are six legal bases set out under Article 6(1) GDPR for processing personal data.

University staff, students and associated individuals must determine the most appropriate legal basis before processing personal data in a specific context, and should document the legal basis in a relevant Privacy Statement and in their records of processing activities. The purpose of the processing and the University's relationship with the data subject will determine the appropriate basis for processing.

The legal bases for processing personal data are:

Consent**:** The data subject has freely given clear, specific and unambiguous consent for Trinity College to process their personal data for a distinct purpose. In cases where Trinity College relies on consent as a lawful basis for processing personal data, the University must:

- Obtain a data subject's specific, informed and freely given consent;
- Ensure that the data subject gives consent by a statement or a clear affirmative action and document the statement or affirmative action; and
- Allow a data subject to withdraw their consent at any time without detriment.

It is recommended that consent is obtained in writing or electronic format. However, where consent is obtained verbally it is recommended that staff and students utilise scripts and checklists to ensure that all necessary requirements have been met and that consent is obtained compliantly and can be evidenced.

Contractual basis**:** The processing is necessary for the performance of a contract which Trinity College has entered with the data subject or in order to take steps at the request of the data subject prior to entering into a contract.

Legal obligation**:** The processing is necessary for compliance with a legal obligation to which Trinity College is subject.

Vital interests**:** The processing is necessary to protect the vital interests of a data subject.

Public interest / Exercise of Official Authority**:** The processing is necessary for Trinity College to perform a task in the public interest or for the purpose of its statutory functions under the Universities Act, 1997 and Higher Education Authority Act, 1971.

Legitimate interests**:** The processing is necessary for the legitimate interests of Trinity College or a third party. This does not apply in instances where such interests are overridden by the interests or fundamental rights and freedoms of data subjects.

8. Rights of data subjects

Under Chapter III GDPR Trinity College is required to provide the following rights for data subjects:

The right to be informed

Data subjects have the right to be informed about the processing of their personal data. Where personal data is being collected directly from a data subject, a Privacy Statement must be provided at the point at which the data is collected. The Privacy Statement must contain the following information:

- Who is collecting and processing the data (e.g. Trinity College School or

Business Unit);

- Why the data is being processed;
- The legal basis (*per* Articles 6 and 9 GDPR) used to justify the processing;
- The format of the processing;
- How long the data will be retained;
- Who the data will be disclosed to;
- Where applicable, the fact that Trinity College intends to transfer the personal data to a non-EEA country or international organisation; and
- How data subjects can exercise their rights under data protection law (access, erasure, objection etc.)

Guidance on how to complete a GDPR-compliant Privacy Statement is available from the Trinity College Data Protection website.

The right of access

Data subjects are entitled to make an access request for a copy of their personal data. This data must be provided to the requestor free of charge within one month and in writing. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the initial one-month period may be extended by two further months. However, this extension applies in exceptional circumstances only and the data subject must be notified of the reason for delay during the initial one-month period.

Data subjects wishing to make a request to access their personal data are advised to complete the Trinity College Data Access Form. Access requests received by University Schools and Business Units should be forwarded to the Data Protection Officer as soon as received.

The right to access one's own personal data is not absolute and is subject to restrictions. Where Trinity College does not comply with an access request the data subject must be informed during the initial one-month period of the reason(s) for the refusal and their right to lodge a complaint with the Data Protection Commission. Guidance on how an access request should be fulfilled is available via the Trinity College Data Subject Rights Request Procedure.

The right to rectification

Personal data processed by Trinity College should be reviewed and verified as being accurate wherever possible. Where inconsistencies are identified by Trinity College, or

where a data subject or other party informs the University of same, actions should be taken to ensure that such inaccuracies are corrected with immediate effect. All requests for rectification of personal data should be forwarded to the Data Protection Officer without delay.

The right to erasure

The right to erasure, whereby data subjects can petition an organisation to have their data erased from its systems, is also known as 'the right to be forgotten'. The right to erasure is not absolute and only applies in certain circumstances.

Trinity College must respond to an erasure request as soon as possible. All requests for erasure of personal data should be forwarded to the Data Protection Officer without delay.

The right to restrict processing

Trinity College may be required to restrict the processing of personal data under certain circumstances. Restricted data should be removed from the normal flow of information and recorded as such. The right to restrict processing is not absolute and only applies in certain circumstances. Trinity College must respond to a restriction of processing request as soon as possible. All requests for restriction of processing should be notified to the Data Protection Officer without delay.

The right to data portability

This right allows data subjects to manage their personal data for their own purposes across different digital platforms and services. Data portability facilitates data subjects to transmit personal data between digital environments without hindrance to usability. All requests received regarding data portability should be forwarded to the Data Protection Officer.

The right to object

Data subjects have the right to object to:

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistical purposes.

Data subjects should be informed of their right to object to processing in University Privacy Statements and at the point of first communication, in a clear and legible form and separate from other information.

In addition, Trinity College should provide opt-out options on all direct marketing material, whether conducted by Trinity College or by third parties on the University's behalf.

All requests regarding an objection to processing should be notified to the Data Protection Officer without delay.

9. Records of Processing Activities

Trinity College is required under Article 30 GDPR to maintain records of processing activities involving personal data and maintain such records (in writing) in a clear and easy to read format.

Trinity College is also required to hold a register of personal data which it processes in its capacity as a data processor.

Every School and Business Unit at the University is required to record its specific processing activities in accordance with Article 30 requirements. Further information on Article 30 requirements, including relevant templates, is available from the Trinity College Data Protection website.

10. Third party data processors

Trinity College engages the services of third parties for certain processing activities.

The University carries out due diligence when forming business relationships and utilises information security audits to identify, categorise and record personal data that is processed outside of Trinity College's direct control, so that the data, processing activity, processor and legal basis are recorded, reviewed and easily accessible.

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

- IT Systems and Services
- Legal Services
- HR Services
- Payroll Services
- Timekeeping and attendance records
- Student and staff surveys

The continued protection of data subject rights and the security of personal data is prioritised when choosing a processor.

Trinity College recognises the importance of adequate and reliable outsourcing for processing activities as well as the University's continued obligations under data protection law for data processed by a third party.

Trinity College staff and students must ensure that processing is limited to third parties operating under formal agreements which satisfy the requirements of Article 28 GDPR.

Staff and students intending to engage the services of third party processors should contact the Data Protection Officer for support.

11. International data transfers

The GDPR imposes restrictions on the transfer of personal data to third countries or international organisations located outside of the European Economic Area. These restrictions are in place to ensure that the level of protection and accountability afforded by GDPR is not undermined.

Personal data may only be transferred from Trinity College to entities situated outside of the EEA in compliance with the conditions for transfer as set out under Chapter V GDPR.

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

12. Data security

Under Article 32 GDPR, third parties (data processors) processing personal data on behalf of Trinity College must take appropriate measures to preserve data security and mitigate risk in order to safeguard personal data which is under the control of the University.

Article 32 requires that "in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed ".

The following technical and organisational measures should be implemented as appropriate:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- The implementation of processes to regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of the processing.

Comprehensive information on Trinity College IT Security provisions, including University IT Security policies, e-mail security, cloud computing, training, data backup and encryption is available from the Trinity College IT Security website.

Guidance on good housekeeping practices regarding manual data is contained within the Trinity College Records Management Policy.

13. Personal data breach notifications

Under GDPR, a personal data breach is defined 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*." This definition extends to breaches which result from, malicious conduct, lack of appropriate security controls, system or human failure, or error.

Trinity College has implemented robust and documented controls for identifying, investigating, reviewing and reporting breaches or complaints. The University has developed Personal Data Breach Procedural Guidelines to assist staff and students in identifying and handling incidents involving personal data breaches.

University staff and students are required to take all necessary steps to reduce the impact of incidents involving personal data by following the Personal Data Breach Procedural Guidelines.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the Data Protection Officer will report the breach to the Data Protection Commission within 72 hours of discovery, *per* Article 33 GDPR requirements. Where appropriate, actions to inform data subjects and reduce risks to their privacy arising from the breach will be implemented without delay, pursuant to Article 34 GDPR.

Staff, students and associated entities who discover a personal data breach or incident should immediately inform the relevant Head of School / Unit and / or contact the Data Protection Officer immediately.

GDPR training for Trinity College staff and students

Trinity College has developed a compulsory online GDPR training module for staff which includes a short assessment which participants must successfully complete as evidence of compliance. Completion of this training module is a mandatory requirement for all staff who process personal data. The pass mark for the module is set at 80%.

Trinity College has developed a compulsory online module for PhD students; CA7000: Research Integrity and Impact in an Open Scholarship Era, which includes sections on data protection, data management and research data security. The pass mark for this module is set at 100%.

The Data Protection Officer has developed training materials in data protection for students. Further information on training resources and material is available from the Trinity College Data Protection website.

14. Data Protection Officer

Pursuant to Article 37 GDPR Trinity College, as a public body, is required to appoint a Data Protection Officer.

Article 38 GDPR states that the Data Protection Officer must be consulted on all matters at Trinity College 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. Data subjects at Trinity College 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, pursuant to Article 39 GDPR, 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 data protection impact

assessments; 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 for the Data Protection Officer are:

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

15. Data Protection Commission

The Data Protection Commission is the Irish Supervisory Authority responsible for upholding the fundamental right of data subjects 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.

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

Contact details for the Data Protection Commission:
https://forms.dataprotection.ie/contact

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

16. Related Documents

- Data Protection Policy
- Information Systems Security Policy
- Network Security Policy
- Internet Use Policy
- Email Use Policy
- Password Policy
- Virus and Spam Policy
- Software Security Policy
- Data Backup Policy
- Disaster Recovery Policy
- Remote Access Policy
- Third Party Access Policy
- Incident Response
- Misuse of IT Facilities Policy
- Legal Compliance Guidelines
- Records Management Policy
- Records Retention Schedule
- CCTV Policy

17. Responsibility

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

18. Document Control

Approved by:

Date Code of Practice approved:

Date of next review:

Appendix 1 – Examples of Personal Data

Names of data subjects	Voice recordings
Student/staff numbers	Employment history
Contact details (incl. Home address, home phone/mobile numbers, email addresses)	Sick leave details/medical certificates
Personal financial data (e.g. Bank account details, credit card numbers)	Other leave data (excl. sick leave)
Photographs/CCTV images of data subjects	Qualifications/Education Details
Video images of data subjects	Work performance
PPS numbers	References for staff/students
Date of birth/Age	Grievance/Disciplinary details
Birthplace/citizenship/nationality	Examination/assignment results
Gender	Membership of professional associations
Marital status	Signatures (including E-signatures)
National ID Card details	Passwords & PIN numbers
Next of kin/dependent/family details	Continuous Professional Development (CPD) records
CVs	Research participant Consent Forms
Details of gifts/donations made	Clinical files relating to research participants
Income/salary	Online identifiers (e.g. IP address)
Blood samples (linked to identifiable data subjects)	Location data
Fingerprints/biometric data	Data relating to children

Appendix 2 – Article 9 GDPR Conditions for Processing of Special Categories of Personal Data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, **unless one of the following conditions apply**:

- The data subject has given explicit consent to the processing of their special category personal data for one or more specified purposes;
- The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject(s);
- The processing relates to personal data which are manifestly made public by the data subject;
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and

specific measures to safeguard the fundamental rights and the interests of the data subject;

- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to certain conditions and safeguards;

- The processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects, in particular professional secrecy;

- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.