# Data Protection Procedural Guidelines

## Template Version Control

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>August 2019</td>
<td>Data Protection Officer</td>
<td></td>
</tr>
</tbody>
</table>
1. Introduction

Trinity College Dublin, The University of Dublin (hereinafter referred to as ‘Trinity’ or the ‘University’) processes personal data for a variety of purposes related to its core functions. This personal data relates to students, staff and other individuals who are associated with the University.

When processing personal data, Trinity must comply with Irish and European data protection legislation (the ‘legislation’) which seeks to safeguard the privacy rights of individuals.

Trinity fully respects an individual’s right to privacy and actively seeks to preserve the rights of those who share information with the University. Any personal information which is processed by Trinity will be treated with the highest standards of security and confidentiality, in accordance with the legislation.

Trinity has developed policies, procedures, controls and measures to ensure continued compliance with the legislation, including staff and student training, policy and procedure documents, processing records, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal data is a core priority of Trinity. The University is proud to operate a 'Privacy by Design' approach, assessing changes and their impact from the outset and designing systems and processes to protect personal data throughout the processing lifecycle.

2. Purpose

The purpose of the Trinity Data Protection Procedural Guidelines is to assist Trinity in meeting its legal, statutory and regulatory requirements under the legislation and to ensure that all personal data under the control of the University is processed in a compliant manner. These Guidelines set out responsibilities for Trinity staff, students, contractors and all other persons who process personal data in connection with their work for the University.

The aim of the Procedural Guidelines is to reduce the risk of personal data breaches and to ensure the protection of personal data. The Guidelines also serve as a reference document for staff, students and third parties on the responsibilities of processing personal data which is under the control of the University.

3. Scope

These Guidelines should be read and understood by students and staff within Trinity (including but not limited to permanent, fixed term, and temporary staff, third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with Trinity), and pertain to the processing of personal data on behalf of the University at all locations where Trinity-controlled personal data is processed, including working from home.
4. Data Protection Legislation

**EU General Data Protection Regulation 2016 (GDPR)**

**Data Protection Act 2018**

**S.I. No. 314 of 2018 - Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018**

**Universities Act, 1997**

**Data Sharing and Governance Act 2019**

**Higher Education Authority Act, 1971**

5. Definitions

**Personal data**

Any information relating to an identified or identifiable natural person ('data subject'). Personal data may be processed in paper and electronic form.

**Data subject**

An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**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 an individual.

This data is categorised under GDPR as:

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

Processing

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

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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data processor

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent of the data subject

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.

Data protection legislation

The collective description of the relevant Irish and EU data protection laws that Trinity complies with.

Supervisory Authority

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

Profiling

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a data subject, in particular to analyse or predict aspects concerning that person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Cross-border processing

Processing of personal data which takes place in more than one EEA Member State or which substantially affects or is likely to affect data subjects in more than one Member State.
6. Principles of Personal Data Processing

Trinity must adhere to the Principles of personal data processing, as set out under Article 5(1) GDPR:

*Personal data shall be:*

- **a)** processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

- **b)** collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) GDPR, not be considered to be incompatible with the initial purposes (‘purpose limitation’);

- **c)** adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

- **d)** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

- **e)** kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’); and

- **f)** 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’).

Article 5(2) GDPR requires that the controller shall be responsible for, and be able to demonstrate, compliance with the Principles of personal data processing (‘accountability’) and requires that controllers such as Trinity must demonstrate how they comply with the Principles, detailing and summarising the measures and controls that are in place to protect personal data and mitigate risk associated with processing.
7. Legal Basis for Processing (Lawfulness)

In order to process personal data lawfully, Trinity must have a legal basis for doing so. There are six legal bases for processing personal data. No single basis is preferred or regarded as more significant than another. Which basis is most appropriate to use will depend on the purpose of the processing and the University’s relationship with the individual.

The six legal bases as set out in Article 6(1) GDPR are:

1. **Consent**: The individual has (freely) given clear, specific and unambiguous consent for Trinity to process their personal data for a distinct purpose;
2. **Contractual basis**: The processing is necessary for a contract which Trinity has with the individual, or because they have asked the University to take specific steps before entering into a contract;
3. **Legal obligation**: The processing is necessary for Trinity to comply with Irish and EU law;
4. **Vital interests**: The processing is necessary to protect the life of an individual;
5. **Public interests**: The processing is necessary for Trinity to perform a task in the public interest or for the purpose of its statutory functions under the 1997 Universities Act; and
6. **Legitimate interests**: The processing is necessary for the legitimate interests of the University or a third party.

Trinity is required to determine the most appropriate legal basis before processing personal data in a specific context, and should document the legal basis in relevant Privacy Statements.

**Consent**

In cases where Trinity relies on consent as a lawful basis for processing personal data, the University must:

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

Where consent is obtained verbally, it is strongly recommended that staff / students utilise scripts and checklists to ensure that all necessary requirements have been met and that consent is obtained compliantly and can be evidenced.
Special categories of personal data

When processing special categories of data (sensitive data), it is necessary for the processing to be covered both by a legal basis under Article 6 GDPR and by a special category condition set out under Article 9 GDPR. Trinity must satisfy one of the Article 9 conditions listed below before processing sensitive data.

8. Records of Processing Activities

As an organisation with 250 or more employees, Trinity 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 and readily available to the Supervisory Authority upon request.

Acting in its capacity as a data controller, Trinity’s internal records of processing activities carried out under the control of the University, contain the following information:

- The University’s name and contact details, and the name and contact details of the University Data Protection Officer. Where applicable, Trinity also records joint controller details and / or details pertaining to the controller’s representative;
- The purposes of the processing;
- A description of the categories of data subjects and of the categories of personal data;
- The categories of recipients to whom the personal data has or will be disclosed (including any recipients in third countries or international organisations);
- Where applicable, transfers of personal data to a third country or an international organisation (including the identification of that third country or international organisation and where applicable, the documentation of suitable safeguards);
- Where possible, the envisaged time limits for erasure of the different categories of data; and
- A general description of the processing security measures pursuant to Article 32(1) GDPR.

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

Every Faculty 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 Data Protection website.
9. **External Data Processors**

Trinity utilises the services of third parties for certain processing activities. The University engages in due diligence when forming business relationships and uses information audits to identify, categorise and record personal data that is processed outside of Trinity’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
- Payroll

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

**International data transfers**

Trinity takes proportionate and effective measures to protect personal data held and processed by the University, including the disclosure and transfer of personal data. Data transfers within Ireland and the EEA are deemed less of a risk than transfers to a third country or an international organisation, due to the adequacy of relevant national and supranational data protection legislation.

The GDPR imposes restrictions on the transfer of personal data outside of the EEA, to third countries or international organisations. These restrictions are in place to ensure that the level of protection afforded by GDPR is not undermined. Personal data may only be transferred 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 Office for support.
10. Rights of Data Subjects

Under Chapter III GDPR Trinity is required to provide the following rights for individuals.

The Right To Be Informed

Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under GDPR. Where personal data is being collected directly from an individual, a Privacy Statement / Notice must be provided at the point at which the data is collected. This is a statement by an organisation which describes how it intends to process personal data, and must contain the following information:

- Who is collecting and processing the data (e.g. School or Business Unit)
- Why the data is being processed
- The legal basis used to justify the processing
- The format of the processing
- How long the data will be retained
- Who the data will be disclosed to
- Individuals’ rights under data protection law (access, erasure, objection etc.)

Information on Privacy Statements, how to complete a GDPR-compliant Privacy Statement and the Right to be Informed is available from the Trinity Data Protection website.

The Right of Access

Data subjects are entitled to make an access request for a copy of their personal data and for information relating to that data. This data must be complied-with within one month. Such information must be provided free of charge and in writing, or by other means where authorised by the data subject.

Individuals wishing to make a request to access their personal data are advised complete the Trinity Data Access Form, available from the Trinity Data Protection website. Access requests should be forwarded to the Trinity Data Protection Officer as soon as received and a record of the request should be noted.

Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay. Where Trinity does not comply with a request for data provision, the data subject must be informed within one month of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

Please refer to the Trinity Data Subject Rights Request Procedure for guidance on how an access request should be fulfilled.
The Right to Rectification

Under Article 5 (1)(d) GDPR, personal data processed by Trinity should be reviewed and verified as being accurate wherever possible. Where inconsistencies are identified by Trinity, or where a data subject or other party informs the University, every reasonable step 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 individuals 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 must respond to a request within one calendar month.

All requests for erasure of personal data should be notified to the Data Protection Officer without delay.

The Right to Restrict Processing

There may arise certain circumstances whereby Trinity may be required to restrict the processing of personal data, to validate, verify or comply with a legal requirement of a data subject’s request. 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 must respond to a request within one calendar month.

All requests for restriction of processing should be notified to the Data Protection Officer without delay.

The Right to Object to Processing

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 provides opt-out options on all direct marketing material, whether conducted by Trinity or by third parties on the University’s behalf.

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 statistics.

Where Trinity processes personal data for the performance of a legal task, in relation to the legitimate interests of the University or for research purposes, a data subject’s objection will only be considered
where it is on grounds relating to their particular situation. Trinity reserves the right to continue processing such personal data where:

- The University can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- The processing is for the establishment, exercise or defense of legal claims.

Where a data subject objects to processing on valid grounds, Trinity will cease the processing for that purpose and advise the data subject of cessation in writing within one month of the objection being received.

In the event that Trinity uses automated decision-making processes, the University must inform the individual of same, and advise them of their rights. Trinity must also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

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

The Right to Data Portability

The right to data portability allows data subjects to manage their personal data for their own purposes across different platforms and services. Data portability facilitates data subjects to transmit personal data from one IT environment to another without hindrance to usability.

The right to data portability is not absolute and applies in the following circumstances only:

- To personal data that a data subject has provided directly to a controller;
- Where the processing is based on consent or for the performance of a contract; and
- When processing is carried out by automated means.

All transmission requests under the portability right should be assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the data subject requesting the transmission to another controller, this is always to be effected without prejudice to the rights and freedoms of the other data subjects.

All requests received regarding data portability should be forwarded to the Data Protection Officer.
11. Data Security

Under Article 32 GDPR, individuals processing personal data on behalf of Trinity 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.

Examples of breaches of security include:

- Unauthorised access to or use of Trinity-controlled personal data
- Inappropriate access controls facilitating unauthorised use or disclosure of the data
- Loss of data
- Theft of data
- Data being altered, deleted or destroyed without authorisation
- Attempts to gain unauthorised access to Trinity-controlled computer networks and systems; e.g. Hacking
- Computer viruses or other security attacks; e.g. Ransomware, phishing, malware

GDPR requires that the following technical and organisational measures are 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

In addition, GDPR requires that “in assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing”.

The Data Protection Commission has published extensive guidance on data security.

Comprehensive information on Trinity IT Security provisions, including University IT Security policies, email security, Cloud computing, training, backups and encryption is available from the College IT Security website.
12. Breaches of Personal Data Security

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

University staff are required to take all necessary steps to reduce the impact of incidents involving personal data by following the Procedural Guidelines. Where a data breach is likely to result in a risk to the rights and freedoms of data subject, the Data Protection Officer will liaise with the Data Protection Commission and report the breach within 72 hours of discovery, per Article 33 GDPR requirements. The DPO will also recommend, where appropriate, actions to inform data subjects and reduce risks to their privacy arising from the breach, pursuant to Article 34 of the Regulation.

Staff, students and contractors who discover a personal data breach or incident should immediately inform their Head of School / Unit who should contact the Data Protection Officer, in line with procedure.

13. Data Protection by Design and by Default

Article 25 GDPR provides for two crucial concepts for future project planning: Data Protection By Design and Data Protection By Default.

Data Protection by Design: controllers must ensure that privacy-enhancing considerations and technologies are considered from the outset, and for the entirety of the lifecycle thereafter, of a system, project or process. This will help to ensure stronger protection for individual data privacy when processing personal data.

Data Protection by Default: controllers must apply privacy settings as standard to a particular process, product or service from the outset of availability to individuals, without any manual input from the end user.

Trinity staff must apply the principles of Data Protection by Design and by Default when processing personal data. This can be attained by:
Performing a Data Protection Impact Assessment (DPIA) in instances where processing is likely to result in a high risk to the rights and freedoms of individuals, particularly when new technologies are being used to process data

Performing a DPIA where systematic and extensive evaluation of individuals is to be carried out based on automated processing, including profiling, or where the processing relates to large scale processing of special categories of data / personal data relating to criminal convictions

Performing a DPIA when processing involves the large-scale systematic monitoring of individuals of a publicly accessible area (e.g. Trinity Campus Security CCTV systems)

Processing the minimum amount of required personal data for the minimum amount of time necessary for the purpose

Pseudonymising or anonymising personal data where necessary and appropriate

**Data Protection Impact Assessment (DPIA)**

**DPIA - General**

The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation. A DPIA is the process of systematically identifying and minimising potential privacy risks as early as possible, and devise suitable mitigation measures.

The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals. The DPIA should assess the activity to be carried out against the Principles of data protection and determine whether the processing of personal data is both necessary and proportionate, or whether changes to the process or additional controls are required.

The DPIA methodology enables controllers to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either:

- Eliminated
- Reduced
- Accepted

The **Trinity DPIA Template** is available to download [here](#).
DPIA - Research

A completed DPIA is required for research studies conducted at St. James’s Hospital, Tallaght University Hospital and all clinical sites in which Trinity researchers are active. Moreover, under Regulation 3(1)(c) of the Health Research Regulations 2018 a DPIA is required where the processing represents a high risk to the rights and freedoms of individuals.

It is the responsibility of the Project Supervisor to ensure the required controls are put in place and to sign off on any risks arising from the processing.

The DPIA should be updated to reflect any material changes to the processing as the project or activity progresses.

The Trinity DPIA Template (Research) is available to download here.

14. CCTV

Closed Circuit Television (CCTV) systems are installed on University premises to provide for the protection, safety & security of Trinity students and staff and all visitors to University property.

In addition, the purpose of CCTV at the University is to facilitate proceedings in the context of criminal or legal issues, including the investigation of major staff, student or visitor disciplinary offences. CCTV cameras may also be used for purposes other than security, for example as part of a research project, for the purpose of recording the progress of a large building project or for monitoring the performance of important items of equipment or machinery.

When using CCTV systems, Trinity will have the greatest possible regard for the protection of the fundamental right to privacy enjoyed by each staff and student member of the College as well as visiting members of the public, and their rights of free association and free expression within the law. CCTV cameras will not be used with the intention of monitoring or recording student union or trade union activities at Trinity. Those charged with the operation of the various CCTV systems at the University must exercise the greatest possible care and ensure that the systems are not used in any unauthorised or inappropriate manner.

Before installing a CCTV system at the University, staff must consult with Estates and Facilities, the Data Protection Officer, and a DPIA must be undertaken.

See the Trinity CCTV Policy for further information on operation of CCTV at University-controlled sites.

Further guidance on the use of CCTV systems is available from the Data Protection Commission.
15. Retention and Destruction

Trinity adheres to the GDPR requirement to process personal data for as long as is necessary. In so doing, the University has defined procedures for adhering to statutory retention periods as set out by legislation, as well as those periods stipulated under contractual requirements.

Personal data should be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritises the protection of the personal data in all instances.

Please refer to the Trinity Records Management Policy and Records Retention Schedule for full information on University’s defined retention periods and archiving and destruction processes.

16. GDPR Training for Trinity Staff

Trinity has developed an online GDPR training session which takes approximately 35 minutes to complete and includes a short assessment which staff must pass in order to successfully complete the training. This training is now a mandatory requirement for all staff at the College. The pass mark for this training session is set at 80/100.

On completion of the session staff should be able to:

- Describe personal data
- Explain the importance of protecting personal data
- Outline the key principles of GDPR
- Recognise the rights of an individual and explain how to implement them
- Locate where to go for GDPR information and support, for individuals and organisations

The GDPR training session can be accessed [here](#).

17. Data Protection Officer

As a public authority the University is required to appoint a Data Protection Officer. The role of the Data Protection Officer is:

- To advise the University and its staff what their responsibilities are under data protection legislation
- To monitor compliance with data protection legislation and relevant policies
- To provide training and increase awareness among staff
- To provide guidance on the completion of Data Protection Impact Assessments
- To co-operate and act as the contact point with the Data Protection Commission in relation to complaints, investigations, audits and consultations and any other matter relevant to the legislation

Contact details for the Data Protection Officer are:

By email:

dataprotection@tcd.ie

By post:

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.

18. Data Protection Commission

The Data Protection Commission is the national independent authority responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. The Commission is the Irish supervisory authority for the GDPR and also has functions and powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the Health Research Regulations 2018.

Further information on how the DPC safeguards and 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/.

Contact details for the Data Protection Commission:

21 Fitzwilliam Square South,
Dublin 2,
D02 RD28,
Ireland

Phone: +353 761 104 800

Webform: https://forms.dataprotection.ie/contact
Appendix 1 – Examples of Personal Data

<table>
<thead>
<tr>
<th>People's names</th>
<th>Contact details (incl. Home address, home phone/mobile numbers, email addresses)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Birth / Age</td>
<td>Birthplace/citizenship/nationality</td>
</tr>
<tr>
<td>Gender</td>
<td>Marital status</td>
</tr>
<tr>
<td>PPS numbers</td>
<td>Student / Staff numbers</td>
</tr>
<tr>
<td>National ID Card details</td>
<td>Next of kin / dependent / family details</td>
</tr>
<tr>
<td>Photographs</td>
<td>CVs</td>
</tr>
<tr>
<td>Personal financial data (e.g. Bank account details, credit card numbers)</td>
<td>Details of gifts / donations made</td>
</tr>
<tr>
<td>Income / salary</td>
<td>Blood samples (linked to identifiable individuals)</td>
</tr>
<tr>
<td>Fingerprints / biometric data</td>
<td>CCTV images</td>
</tr>
<tr>
<td>Video images containing identifiable individuals</td>
<td>Voice recordings</td>
</tr>
<tr>
<td>Employment history</td>
<td>Sick leave details / medical certificates</td>
</tr>
<tr>
<td>Other leave data (excl. sick leave)</td>
<td>Qualifications/Education Details</td>
</tr>
<tr>
<td>Work performance</td>
<td>References for staff / students</td>
</tr>
<tr>
<td>Grievance / Disciplinary details</td>
<td>Examination / assignment results</td>
</tr>
<tr>
<td>Membership of professional associations</td>
<td>Signatures (incl. Electronic)</td>
</tr>
<tr>
<td>Passwords &amp; Pin numbers</td>
<td>Continuous Professional Development (CPD) records</td>
</tr>
<tr>
<td>Car registration details</td>
<td>Clinical files relating to research participants</td>
</tr>
<tr>
<td>Online identifiers (e.g. IP address)</td>
<td>Location data</td>
</tr>
<tr>
<td>Data relating to children</td>
<td>Research subject consent forms</td>
</tr>
</tbody>
</table>
Appendix 2 – Processing of 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 an individual. When processing special categories of data (sensitive data), it is necessary for the processing to be covered both by a legal basis under Article 6 GDPR and by a special category condition set out under Article 9 GDPR. Trinity must satisfy one of the Article 9 conditions listed below before processing sensitive data.

### Sensitive Data

<table>
<thead>
<tr>
<th>Sensitive Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, trade-union membership</td>
</tr>
<tr>
<td>The processing of genetic data for the purpose of uniquely identifying a data subject</td>
</tr>
<tr>
<td>The processing of biometric data for the purpose of uniquely identifying a data subject</td>
</tr>
<tr>
<td>Data concerning health</td>
</tr>
<tr>
<td>Data concerning a data subject’s sex life or sexual orientation</td>
</tr>
</tbody>
</table>

### Article 9 GDPR conditions for processing sensitive data

<table>
<thead>
<tr>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>An individual has given explicit consent to the processing of their sensitive data for one or more specified purposes</td>
</tr>
<tr>
<td>The processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the individual 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 individual;</td>
</tr>
<tr>
<td>The processing is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent;</td>
</tr>
<tr>
<td>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</td>
</tr>
</tbody>
</table>
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 individual(s);

The processing relates to personal data which are manifestly made public by the individual;

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 individual;

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 individuals, in particular professional secrecy; and

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 individual.