Data Protection Policy

Version Number: 3

Revision date: 19/02/2024

Policy Owner: Information Compliance Manager and Corporate Secretary

Approved by: Governing Authority

Date approved: 30/04/2024

Policy Contents

1. INTRODUCTION

Data Protection ensures individuals' privacy rights are safeguarded when their personal data is processed. University College Cork ("the University") collects and uses personal data about its students, staff and other individuals who come into

contact with the University, referred to as "data subjects". To respect the privacy rights of these individuals, the University must comply with the EU General Data Protection Regulation ("GDPR") and the Irish Data Protection Acts, 1988 to 2018 (as amended) (the "DPA") – collectively referred to in this policy as "the Data Protection Acts". These Acts not only grant rights to individuals in respect of their own personal data but also impose responsibilities on those handling personal data.

2. PURPOSE

This policy is a statement of the University's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts. It sets out responsibilities for all managers, employees, students, contractors and anyone else who can access or use personal data in their work for or studies with the University.

3. PERSONAL DATA AND 'SPECIAL CATEGORIES' OF PERSONAL DATA

'**Personal data**' means any information that relates to an **identified or identifiable living individual**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. 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 a person can identify an individual or make them identifiable.

In practice, any data about a living person who can be identified from the data available (or potentially available) will count as personal data. This will include pseudonymised data i.e. replacing any identifying characteristics of data with a value which does not allow the data subject to be directly identified (pseudonym). Where a pseudonym is used, it is often possible to identify the data subject by analysing the underlying or related data. Examples of personal data can be found in Appendix F.

Stronger safeguards and requirements are required for '**special categories of data**' (previously known as 'sensitive personal data') under the GDPR. This refers to personal data falling under the following categories:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Data concerning a person's sex life or sexual orientation
- Genetic data
- Biometric data

Personal data falling under these categories can be processed ***only*** under specific circumstances, which are described in Article 9(2) of the GDPR (See Appendix B).

Personal data relating to criminal convictions and offences, while not included in the list of 'special categories' of personal data, have extra safeguards applied to processing them (see Appendix C).

Please see the Definitions section of this Policy for details on the terms used in this policy.

4. SCOPE

4.1 What information is included in this Policy?

This policy applies to all personal data created or received in the course of University business in all formats, of any age. Personal data may be held or transmitted in paper, physical and electronic formats.

4.2 To whom does this Policy apply?

This policy applies to:

- any person who is employed or engaged by the University; who processes personal data in the course of their employment or engagement;
- any student of the University who processes personal data not already in the public domain in the course of their studies or research activities;
- individuals who are not directly employed by the University, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the University;
- people on placement, visiting students and researchers, volunteers;
- members of UCC's Governing Authority in the course of their duties.

Hereinafter these are collectively referred to as "Members".

4.3 Where does the Policy apply?

This policy applies to all locations from which University personal data is accessed, including when working remotely.

5. DATA PROTECTION POLICY

The University undertakes to perform its responsibilities in accordance with the Data Protection Acts and the GDPR.

5.1 Data Protection Principles

The University is responsible for, and must be able to demonstrate, compliance ("accountability") with the following Data Protection Principles:

Personal data shall be:

- Processed lawfully, fairly and in a way that is transparent to the data subject **("lawfulness, fairness and transparency")**;
- Collected, created or processed only for one or more specified, explicit and lawful purpose **("purpose limitation")**;
- Adequate, relevant and limited to what is necessary for those purposes **("data minimisation");**
- Kept accurate and, where necessary, up-to-date **("accuracy");**
- Retained no longer than is necessary **("storage limitation");**
- Kept safe and secure **("integrity and confidentiality").**

These provisions are binding on **every** data controller, including the University. Any failure to observe them may be a breach of the Data Protection Acts. Further explanation of each principle is outlined below.

5.1.1 Process personal data lawfully, fairly and transparently

When the University collects personal data, it has to make certain information available to the person the data relates to. This applies whether the information is collected directly from the individual or from another source. This information must be provided via a **Data Protection Notice** (or Privacy Statement in the case of a website). In addition, the University must have a **legal basis** for processing the data. These legal bases are specifically defined in the Data Protection Acts and are set out below.

Data Protection Notices:

When is a Data Protection Notice required?

- Where information is being collected directly from an individual, a Data Protection Notice must be provided at the point at which the data is collected.

- Where information is obtained from another source, a Data Protection Notice must be provided:
    - within, at most, one month of obtaining the data;
    - if personal data is to be used to communicate with the data subject, at the latest, at the time of the first communication with the data subjects.
    - if disclosure to another recipient is envisaged, at the latest, when personal data are first disclosed.

What needs to be included in a Data Protection Notice?

Data Protection Notices must contain specific information (set out in the legislation) which informs data subjects of:

- who is collecting the data (e.g. School of X, University College Cork);
- why the data is being collected (the purpose);
- what legal basis is being relied upon to process the data;
- what types of data will be processed and how;
- how long the data will be kept;
- who it will be disclosed to;
- the contact details of the Data Protection Officer;
- any intended transfer of personal data to a third country together with any relevant safeguards;
- Where data is obtained indirectly (i.e. not from the data subject themselves), the categories of personal data and its source/(s).

What rights do people have in relation to their own data? (see section 5.2 – Data Subject Rights below).

Individuals must also be made aware of:

- the right to lodge a complaint with the Data Protection Commission;
- the lawful basis for the processing and the consequences of failure by a data subject to provide the data;
- the existence of automated decision making, including profiling;
- in certain circumstances: the right to withdraw consent, to object to processing, to rectify personal data, the right to erasure of data, the right to data portability, the right to access, the right to restriction of processing.

Further details on what information is required in a Data Protection Notice is contained within UCC's Data Protection Notice Procedure.

Legal Basis for Processing

In order to collect and process personal data lawfully, the University must have a legal basis for doing so. There are six available legal bases for processing. No single

basis is ‘better’ or more important than the others – which basis is most appropriate to use will depend on the purpose and the relationship with the individual. The six legal bases, set out in Article 6(1) of the GDPR, are as follows:

- ***Consent**: the individual has given clear consent for the University to process their personal data for a specific purpose;
- **Contract**: the processing is necessary for a contract the University has with the individual, or because they have asked the University to take specific steps before entering into a contract;
- **Legal obligation**: the processing is necessary for the University to comply with the law;
- **Vital interests:** the processing is necessary to protect someone’s life;
- **Public task:** the processing is necessary for the University to perform a task in the public interest or for its official functions;
- ****Legitimate interests**: the processing is necessary for the legitimate interests of the University or a third party.

The University must determine its legal basis ***before*** beginning to process personal data, and should document it in its Data Protection Notices and in the University’s Record of Processing Activities

*In cases where the University relies on **consent** as a condition for processing personal data, it must:

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

**In cases where legitimate interests is being relied upon, it may be necessary to conduct a Legitimate Interests Assessment.

See Appendix A for further details of lawful bases. Further information on consent is documented in Appendix D.

In the case of personal data relating to special categories of data, it is necessary for the processing to be covered both by an Article 6 legal basis ***and*** by a special category condition set out in Article 9 of the GDPR (see Appendix B). In the case of personal data relating to criminal convictions and offences, it is necessary for the processing to be covered both by an Article 6 legal basis and by a separate condition for processing this data in compliance with Article 10 of the GDPR (see Appendix C). Both of these types of processing need to be documented to demonstrate accountability and compliance.

5.1.2 Process personal data only for one or more specified, explicit and LAWFUL purposes *("purpose limitation")*

Members must:

- only keep personal data for purposes that are specific, lawful and clearly stated (in a data protection notice);
- only process personal data in a manner which is compatible with these purposes;
- treat people fairly by using their personal data for purposes and in a way they would reasonably expect;
- ensure that the data is not reused for a different purpose that the individual did not agree to or would reasonably expect.
- ensure that the collection and processing of the data is lawful by meeting one or more of the lawful bases (See Appendix A).

5.1.3 Ensure that personal data being processed is adequate, relevant and not excessive *("data minimisation")*

Members should only collect the minimum amount of personal data from individuals that is needed for the purpose(s) for which it is kept (and referred to in the data protection notice).

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which the data are kept. Special attention should be paid to the protection of special categories of personal data, the disclosure of which would normally require explicit consent or one of the other specified lawful bases (see Appendix A).

5.1.4 Keep personal data accurate and, where necessary, up-to-date *("accuracy")*

Members must ensure that the personal data being processed is accurate and, where necessary, kept up-to-date. Members must ensure that local procedures are in place to ensure high levels of personal data accuracy, including periodic review and audit.

5.1.5 Retain personal data no longer than is necessary for the specified purpose or purposes *("storage limitation")*

Members must be clear about the length of time for which personal data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal data, then that data should be routinely deleted.

Members must comply with the University's Records Management Policy, and apply the University's Records Retention Schedules to keep records and information

containing personal data only so long as required for the purposes for which they were collected.

The legislation allows for data to be stored for longer periods kept insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of individuals.

5.1.6 Keep personal data safe and secure *("integrity and confidentiality")*

Members must take appropriate security measures to protect personal data from:

- unauthorised access;
- inappropriate access controls allowing unauthorised use of information;
- being altered, deleted or destroyed without authorisation by the "data owner";
- disclosure to unauthorised individuals;
- attempts to gain unauthorised access to computer systems e.g. hacking;
- viruses or other security attacks;
- loss or theft;
- unlawful forms of processing.

While the Data Protection Acts do not specify the necessary security measures to be taken, they require that the state of technological developments, the nature of the data and the degree of harm that might result from unauthorised or unlawful processing should be taken into consideration.

The Data Protection Commission has issued a guidance note on this security obligation (which is available here) and the University has its own policies on security which must be adhered to at all times. See the University's IT Security Policy and Acceptable Use Policy.

Where transferring personal data to another country outside the European Union, appropriate agreements, and auditable security controls to maintain privacy rights must be put in place. See section 5.11 below.

Advice and guidance must be sought from the University's Information Compliance Manager where you are considering a transfer of data outside of the EEA.

5.1.7 Accountability

The GDPR states that the data controller shall be responsible for, and be able to demonstrate compliance with the above principles ("accountability"). This means that we must:

- maintain relevant documentation on all data processing activities, known as a Record of Processing Activities (ROPA) (see 5.2 below);
- implement appropriate technical and organisational measures that ensure and demonstrate that we comply;
- implement measures that meet the principles of privacy by design and by default (see 5.3 below), such as:
    - data minimisation;
    - pseudonymisation;
    - transparency; and
    - creating and improving security features on an ongoing basis.
- use data protection impact assessments (DPIAs) where appropriate.
- record all data security breaches (see 5.5 below).

5.2 Records of Processing Activities (ROPA)

In order to maintain documentation on processing activities, the University has created a central Record of Processing Activities (ROPA) which documents the categories of personal data we hold as a Data Controller, what we use it for, the legal basis we are relying on in order to process the data, who we may share it with, where it is held and how long we keep it.

The University is also required to hold a ROPA where the University acts as a **data processor** for another data controller.

Every school/discipline in the University is required to record the information that is needed to compile the ROPAs. This process is coordinated by the Information Compliance Manager. Nominated Data Protection Champions in each area are responsible for co-ordinating the compilation of the required information for their own area, in consultation with their Head of School/Discipline. Heads of School/Discipline must return the required information to the Information Compliance Manager. Heads must also notify the Information Compliance Manager with details of any changes to the processing of personal data carried out in their area.

5.3 Privacy by Design and by Default

Privacy by design and by default is written into Article 25 of the GDPR.

Privacy by Design states that any action an organisation undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. This includes internal projects, product development, software

development, IT systems, and much more. In practice, this means that the University must ensure that privacy is built into a system during the whole life cycle of the system or process.

Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. In addition, any personal data provided by the user to enable a product's optimal use should only be kept for the amount of time necessary to provide the product or service. If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

Members must apply the principles of Privacy by Design and by Default when processing any personal data by:

- Performing a Data Protection Impact Assessment (DPIA) – see section below – where data processing is likely to result in a **high risk** to the rights and freedoms of individuals, especially when a new data processing technology is being introduced.
- Performing a DPIA where systematic and extensive evaluation of individuals is to be carried out based on automated processing (profiling), large scale processing of special categories of data and personal data relating to criminal convictions.
- Collecting, disclosing, and retaining the minimum personal data for the minimum time necessary for the purpose.
- Anonymising personal data wherever necessary and appropriate.

5.4 Data Protection Impact Assessments (DPIA)

When members of the University process personal data, the individuals whose data we are processing are exposed to risks. A Data Protection Impact Assessment (DPIA) is the process of systematically identifying and minimising those risks as far and as early as possible. It allows the University to identify potential data protection issues before they arise, and to find ways to mitigate them.

Under the GDPR, a DPIA is mandatory where data processing “is likely to result in a high risk to the rights and freedoms of natural persons”. This is particularly relevant when a new data processing technology is being introduced or for high-risk research studies. In cases where it is not clear whether a DPIA is strictly mandatory, carrying out a DPIA is still good practice and a useful tool to help data controllers comply with data protection law.

For researchers who may need to conduct a DPIA as part of their research study, the University has developed a screening tool to help Members determine if a DPIA is required see Information Compliance info. For further information and guidance on the DPIA process, see here.

For the avoidance of doubt, the DPIA procedure is separate and distinct to the ethics application process and may be required in addition to that process.

5.5 Personal Data Security Breaches

In the event of a breach of personal data security occurring, it is vital to ensure that it is dealt with immediately and appropriately to minimise the impact of the breach and prevent a recurrence. If a member of the University becomes aware of an actual, potential or suspected breach of personal data security, they must report the incident to their Head of School/Discipline immediately. The Head of School/Discipline must then report the incident immediately to the Information Compliance Manager by completing the Data Breach Report Form and email it to gdpr@ucc.ie.

It is important that all Members act quickly and report any suspected incident without delay.

The University will take all necessary steps to reduce the impact of incidents involving personal data by following the University's Personal Data Security Breach Management Procedure. Where a data breach is likely to result in a risk to the rights and freedoms of a data subject, the Information Compliance Manager will liaise with the Data Protection Commission and report the breach within 72 hours of becoming aware of the breach. The Information Compliance Manager will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

5.6 Data Subject Rights

The GDPR provides the following rights for individuals:

5.6.1 The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. See section above on Data Protection Notices.

5.6.2 The right of access

Data subjects are entitled to make an access request under the Data Protection Acts for a copy of their personal data and for certain information relating to that data. This must be complied with within one calendar month.

If a data access request is received by the University, the recipient should forward it immediately to the University's Information Compliance Manager (email: gdpr@ucc.ie) who will respond to the request on behalf of the University, consulting with staff in relevant offices/departments and taking into account the narrow exemptions set out in the legislation.

Please refer to the University's Data Subject Right's Procedure.

In certain circumstances, the information may be exempt from disclosure in accordance with the restrictions in the Data Protection Acts (e.g. disclosure required

by law). Such exemptions are subject to strict conditions, and should only be availed of where authorised by the University's Information Compliance Manager.

The personal information of a data subject must not be disclosed to a third party, be they parent, potential employer, employer, professional body, etc. without the consent of the individual concerned or an alternative appropriate legal basis (e.g. vital interests).

5.6.3 The right to rectification

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete. An individual can make a request for rectification verbally or in writing. The University must respond to a request within one calendar month. In certain circumstances, the University can refuse a request for rectification.

All requests for rectification of personal data should be notified without delay to the Information Compliance Manager who will advise further on the steps to be taken to respond to the request.

5.6.4 The right to erasure

The GDPR introduced a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. Individuals can make a request for erasure verbally or in writing. The University must respond to a request within one calendar month. The right to erasure is not absolute and only applies in certain circumstances.

All requests for erasure of personal data should be notified without delay to the Information Compliance Manager who will advise further on the steps to be taken to respond to the request.

5.6.5 The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, the University is permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing and the University must respond within one calendar month.

All requests to restrict the processing of personal data should be notified without delay to the Information Compliance Manager who will advise further on the steps to be taken to respond to the request.

5.6.6 The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or

transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

All requests in relation to portability of personal data should be notified to the Information Compliance Manager (gdpr@ucc.ie).

5.6.7 The right to object

Individuals have the right to object to:

- **processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling):**
  - Individuals must have an objection on "grounds relating to his or her particular situation".
  - You must stop processing the personal data unless:
    - you 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 defence of legal claims.

  You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.

  This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".
- **direct marketing (including profiling)**
  - You must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse.
  - You must deal with an objection to processing for direct marketing at any time and free of charge.
  - You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
  - This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".
  - Data subjects must be given the option to opt out of further communications each and every time they are contacted. They must also be given the opportunity to segment their preferences.

- **processing for purposes of scientific/historical research and statistics.**

  Individuals must have “grounds relating to his or her particular situation” in order to exercise their right to object to processing for research purposes. This applies to processing based on public interest or legitimate interest unless processing is for scientific purposes and necessary for the performance of a task carried out for reasons of public interest in which case you are not required to comply with an objection to the processing.

5.6.8 Rights in relation to automated decision making and profiling

You must offer a way for individuals to object online. An individual has the right not to be subjected to automated decision-making that has significant effect, legal or otherwise, on them unless they have explicitly consented **or** it is necessary for contract purposes **or** is authorised by law.

5.7 External Data Processors and Joint Data Controllership

It is occasionally necessary for the University to engage the services of external suppliers (data processors). If the service involves the external hosting of personal data (such as staff and student data) by the supplier on behalf of the University, a number of steps must be taken before any personal data can be disclosed to the supplier. See the IT Supplier Procurement Procedure.

As a data controller, the University is responsible for determining the purpose and the manner in which personal data in its control is processed e.g. student data, staff data, alumni data. The University must not only ensure its own adherence to the data protection regulations but also take measures to ensure that any third party suppliers it engages are compliant as well.

There may also be occasions when the University acts as a joint data controller with a third party or external party to jointly control the data. In such circumstances University shall enter into a formal agreement that sets out the duties and obligations each party owes to each other and to data subjects in regard to the processing of personal data.

5.8 Transfers of Personal Data Outside of the E.U.

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

Personal data may be transferred where the organisation receiving the personal data has provided assurance of adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies;
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group);
- standard data protection clauses in the form of template transfer clauses adopted by the Commission;
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission;
- compliance with an approved code of conduct approved by a supervisory authority;
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority; or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

If you intend to transfer personal data outside of the E.U., contact the Information Compliance Manager in the first instance, who will seek the appropriate legal advice where required. An assessment of the data protection regime of the third country may need to be carried out.

5.9 Marketing / Mailing Lists / Electronic Privacy Regulations

The Electronic Privacy Regulations 2011 (SI 336 of 2011) sit alongside the Data Protection Acts. They give people specific privacy rights in relation to electronic communications and contain specific rules on:

- Marketing calls, emails, texts and faxes;
- Cookies (and similar technologies);
- Keeping communications services secure; and
- Customer privacy regarding traffic and location data, itemised billing, line identification, and directory listings.

While primarily aimed at electronic communications companies (telecommunications companies and internet services providers), the Regulations also apply to any entity (such as the University) using such communications and electronic communications networks to communicate with customers

Unsolicited direct marketing is one of the main sources of complaint from individuals to the Data Protection Commissioner and anyone who fails to comply with the E-Privacy Regulations can be prosecuted as each unlawful marketing message or call constitutes a separate offence.

It is imperative that the necessary marketing opt-ins and opt-outs (via a data protection notice or otherwise) are in place before using personal data for marketing purposes. The Data Protection Commissioner's guidance note is available here.

Where Members process personal data to keep people informed about University activities and events they must provide in each communication a simple way of opting out of further communications.

Members are required to follow the Guide to Direct Marketing when seeking to send out marketing communications on behalf of the University.

5.10 Personal Data relating to Criminal Convictions/Offences (incl. Garda Vetting)

To process personal data about criminal convictions or offences, the University must have both a lawful basis under Article 6 of the GDPR and either legal authority or official authority for the processing under Article 10. This must be established before processing begins and must be documented. See Appendix C for further information.

Garda vetting disclosures made to the University must be stored securely with access restricted to a small number of authorised personnel. The University's Garda Vetting Policy is available here.

Advice and guidance on profiling can be sought from the University's Information Compliance Manager.

5.11 Profiling and/or Automated Decision Making

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning their performance at work or studies, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

There is a distinction between the concepts of profiling and automated decision-making. There are three ways in which profiling can be used in practice:

- general 'profiling' (which is defined in Article 4(4) GDPR)

- human decision-making based on profiling (i.e. the ultimate decision is made by a human who bases that decision on a profile produced by purely automated means); and
- purely automated decision-making (i.e. decisions made by technological means without human involvement) under Article 22 GDPR, which includes profiling and which produces legal effects for or significantly affects the data subject.

While the law recognises profiling and automated decision-making can be useful for individuals and organisations, GDPR restricts profiling and gives data subject rights around profiling-based decisions. There is a general prohibition on 'solely' automated processing producing 'legal' or 'similarly significant' effects unless permitted by law and the transparency requirements (set out in section 1 above) are complied with.

Advice and guidance on profiling can be sought from the University's Information Compliance Manager.

5.12 CCTV

All usage of CCTV other than in a purely domestic context must be undertaken in compliance with the requirements of the Data Protection Acts. Extensive guidance on this issue is available on the Data Protection Commissioner's website.

In summary, all uses of CCTV must be **proportionate** and **for a specific purpose/s**. As CCTV impacts the privacy of the persons captured in the images, there must be a genuine reason for installing such a system. If installing a CCTV system, the **purpose** for its use must be displayed in a prominent position.

Before installing a CCTV system in the University, Members must consult with the Office of Corporate & Legal Affairs (Information Compliance Manager) and a Data Protection Impact Assessment must be undertaken.

5.13 CHILDREN'S PERSONAL DATA

Children are identified in the GDPR as "vulnerable individuals" and deserving of "specific protection". Guidelines on the use of personal data relating to children are outlined in Appendix E.

6. ROLES AND RESPONSIBILITIES

The University has overall responsibility for ensuring compliance with the Data Protection Acts. However, all employees who process personal data in the course of their employment, those on placements or seconded to the University and students of the University who process personal data in the course of their studies, or where

they are employed by the University, are also responsible for ensuring compliance with the Data Protection Acts.

The University will provide support, assistance, advice and training to all relevant schools, disciplines and staff to ensure they are in a position to comply with the legislation. The University's Information Compliance Manager (contact details below) will assist the University and its staff in complying with the Data Protection legislation.

Specifically, the following roles and responsibilities apply in relation to this Policy:

All users of University information:

- Must complete relevant training and awareness activities provided by the University to support compliance with this policy;
- Should take all necessary steps to ensure that no breaches of information security result from their actions;
- Must report all suspected and actual data security breaches to their head of school/discipline who must in turn report the incident immediately to the Information Compliance Manager, so that appropriate action can be taken to minimise harm;
- Must inform the University of any changes to the personal information that they have provided to the University in connection with their employment or studies (e.g. changes of address or bank account details).

University Leadership Team – Operations (ULT):

- the ULT is responsible for reviewing and approving this Policy as recommended by the Corporate Secretary;
- each member of ULT is responsible for ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility;
- members of ULT must, as part of the University's Annual Statement of Internal Control, sign a statement which provides assurance that their functional area is in compliance with the Data Protection Acts.

Corporate Secretary:

The Corporate Secretary is the Senior Officer within the University, with accountability for compliance with the Data Protection Acts and for:

- ensuring that this Policy is reviewed and approved by the ULT as appropriate;
- ensuring that appropriate policies and procedures are in place to support this Policy;
- liaising with the ULT as appropriate;

- ensuring that any data security breaches are properly dealt with.

Heads of School/Discipline:

Heads of School/Discipline are responsible for:

- ensuring compliance with the Data Protection Acts and this policy in their respective areas of responsibility;
- nominating a suitable member of staff to be responsible for coordinating Data Protection compliance matters within each of the areas under their remit;
- enabling the Information Compliance Manager to maintain a Record of Processing Activities (ROPA) by compiling (along with the Data Protection Champions for their areas of responsibility), approving and returning the information required for the compilation of the ROPA to the Information Compliance Manager.

Information Compliance Manager:

The Information Compliance Manager is responsible for administrative matters at an institutional level in relation to data protection. The principal data protection duties of the Information Compliance Manager are to:

- process and respond to formal Data Access Requests;
- respond to requests for rectification, erasure of data and restrictions or objections to processing of data;
- initiate regular reviews of data protection policies and procedures and ensure documentation is updated as appropriate;
- provide advice to staff in relation to the completion of and outcome of Data Protection Impact Assessments;
- acting as the contact point for and cooperating/liaising with the Data Protection Commission where necessary/appropriate, including in the event of a data security breach;
- maintain a record of all personal data security breaches;
- organise targeted training and briefing sessions for the University's staff as required;
- provide advice and guidance to the University's staff on data protection matters;
- maintain a centrally-held register of the categories of personal data held by UCC (ROPA);
- maintain records of the University's compliance with the Data Protection Acts.

Nominated Data Protection Champions within Schools/Disciplines:

Every School/Discipline within the University which processes personal data is asked to nominate a suitable member of staff to be responsible for coordinating Data Protection compliance matters within their respective area, such matters to include:

- being a point of contact for the Information Compliance Manager regarding Data Protection;
- compiling and maintaining the information required from their area for the University's Register of Personal Data;
- bringing relevant Data Protection/IT security matters to the attention of relevant staff in his/her area;
- participating in training in data protection/IT security where appropriate.

Staff, students and other Members of the University:

All staff, students and other Members are expected to:

- acquaint themselves with, and abide by, the rules of Data Protection set out in this Policy;
- read and understand this policy document;
- understand what is meant by 'personal data' and 'special categories of personal data' and know how to handle such data;
- understand the lawful basis for processing personal data;
- not jeopardise individuals' rights or risk a contravention of the Act;
- report all data security breaches to their manager immediately;
- contact the Information Compliance Manager if in any doubt.

7. BREACH OF THIS POLICY

If any breach of this Policy is observed, then disciplinary action may be taken in accordance with the University's disciplinary procedures (Principal Statute for staff) and Student Rules as amended or updated from time to time.

8. SUPPORTING POLICIES, PROCEDURES & GUIDELINES

This policy supports the provision of a structure to assist in the University's compliance with the Data Protection Acts. The policy is not a definitive statement of Data Protection law. If you have any specific questions or concerns in relation to any matters pertaining to personal data, please contact the University's Information Compliance Manager (see contact details below).

The Policy should be read in conjunction with the following University policies, procedures and guidelines:

- Data Impact Assessment procedure
- Data Protection Notice Procedure
- Records Management Policy
- IT Security Policy
- Acceptable Use Policy
- Guidelines for Portable Devices
- Guidelines for Smartphone Users
- Guidelines for the Disposal of Devices Containing Confidential Data
- Personal Data Security Breach Management procedures
- Web and Social Media Policy
- Code of Research Conduct

In addition, the following legislation must be considered in conjunction with this policy:

- Electronic Privacy Regulations 2011 (SI 336/2011)

9. DEFINITIONS

The GDPR and Data Protection Acts govern the processing of personal data. As with any legislation, these and other terms used in the GDPR and Data Protection Acts have a specific meaning. The following are some important definitions used in this policy, taken from the legislation, with additional comments provided where appropriate:

Personal data

Personal data means information relating to-

a. an identified living individual

b. a living individual who can be identified from the data, directly or indirectly, in particular by reference to

- an identifier such as a name, an identification number, location data or online identifier, or
- one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

This can be a very wide definition depending on the circumstances.

Special categories of personal data

Special categories of personal data (formerly known as “sensitive personal data”) receive greater protection under the Data Protection Acts and refer to the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data for the purpose of uniquely identifying a person;
- data concerning health;
- data concerning a person’s sex life or sexual orientation.

Data subjects have additional protections under Article 9 of the GDPR in relation to the processing of any such data.

Whilst criminal convictions and offences are not classed as special categories of personal data, the Data Protection Acts also provide additional protections to data subjects in this regard.

Data concerning health

Data concerning health means personal data relating to the physical or mental health of an individual, including the provision of health care services to the individual, that reveal information about the status of his or her health.

Data subject

Data subject is a living person who is the subject of personal data.

Data controller

Data controller means 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. The University, for example, is a data controller in relation to personal data relating to its own staff and students.

Data owner

Data owner means the most senior person in the department/school/college/administrative unit/research unit within which the data is created. An exception can be made if this role has been explicitly and formally

delegated to someone else by the most senior person in the aforementioned areas. Data owners have overall responsibility for the quality and integrity of the data held in their area.

Data processor

Data processor means a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller. Note: the term 'Data Processor' does not include an employee of a data controller who processes such data in the course of their employment. Such processing is considered to be performed by the Controller. Examples of data processors include payroll companies, accountants, and market research companies, all of which could hold or process personal information on behalf of someone else.

Direct marketing

Direct marketing is defined as:

"the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals".

This covers all advertising or promotional material, including that promoting the aims or ideals of not-for-profit organisations – for example, it covers a charity or political party campaigning for support or funds.

The marketing must be directed to particular individuals. In practice, all relevant electronic messages (e.g. calls, faxes, texts and emails) are directed to someone, so they fall within this definition.

Genuine market research does not count as direct marketing. However, if a survey includes any promotional material or collects details to use in future marketing campaigns, the survey is for direct marketing purposes and the rules apply.

An unsolicited message is any message that has not been specifically requested. So even if the customer has 'opted in' to receiving marketing from you, it still counts as unsolicited marketing. An opt-in means the customer agrees to future messages (and is likely to mean that the marketing complies with the Electronic Privacy Regulations) but this is not the same as someone specifically contacting you to ask for particular information.

Members

In this Policy, '**Members'** is used to refer to:

- any person who is employed or engaged by the University who processes personal data in the course of their employment or engagement;
- any student of the University who processes personal data in the course of their studies or work carried out on behalf of the University;

- individuals who are not directly employed by the University, but who are employed by contractors (or subcontractors) and who process personal data in the course of their duties for the University.

Processing

Processing is widely defined under the Data Protection Acts and means performing any operation or set of operations on personal data, whether or not by automated means, including-

- the collection, recording, organisation, structuring or storing of the data;
- the adaptation or alteration of the data;
- the retrieval, consultation or use of the data;
- the disclosure of the data by their transmission, dissemination or otherwise making the data available;
- the alignment or combination of the data; or
- the restriction, erasure or destruction of the data.

Pseudonymisation

Pseudonymisation means 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 information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. The Data Protection Acts still apply to personal data which has been pseudonymised.

10. POLICY REVIEW AND APPROVAL

This policy has been approved by the University Leadership Team (ULT). Any additions or amendments to this or related policies will be submitted by the Corporate Secretary to the ULT for approval or to whatever authority the ULT may delegate this role.

The policy will be reviewed periodically by the Information Compliance Manager and Corporate Secretary in light of any legislative or other relevant developments.

This policy will be reviewed every two years by the Information Compliance Manager and Corporate Secretary. Changes will be made in line with any legislative or other relevant developments.

11. FURTHER INFORMATION

If you have any queries in relation to this policy, please contact:

Catriona O'Sullivan
Information Compliance Manager
Office of Corporate & Legal Affairs
University College Cork

Tel: 021 4903949

Email: gdpr@ucc.ie

12. MISCELLANEOUS

The University reserves the right to amend or revoke this policy at any time without notice and in any manner in which the University sees fit at the absolute discretion of the University or the President of the University.

This policy will be reviewed every two years by the Information Compliance Manager and the Director of Legal & Information Compliance in light of any legislative or other relevant developments.

APPENDIX A: LAWFUL BASES FOR PROCESSING

It is necessary under Article 6 of the GDPR to have a legal basis for processing ALL personal data. There are six legal bases set out in the legislation:

Consent from the individual

The individual must give consent at the outset. Inferred consent is not enough. Their consent must be freely given and the withdrawal of their consent should not have any adverse consequences for the individual.

Necessary for the performance of a contract

The contract must be between the controller and the data subject and the data must be necessary for the performance of that contract or necessary in order to take steps to enter a contract with the data subject. For example, processing data relating to an individual's qualifications and work history when considering entering into an employment contract.

Necessary for compliance with a legal obligation

The University is required by statute to retain certain records, for example employment records, health & safety records, student data. This lawful basis will cover a lot of the University's data processing.

Necessary to protect the vital interests of the individual or another natural person

This ground is applied in essentially "life and death" situations, for example where it is necessary to provide personal data to the emergency services in the case of an emergency situation.

Necessary for the performance of a task carried out in the public interest

This may occur where the University carries out a task in the public interest or in an exercise where official authority has been invested in the University as a data controller. However, a data subject can object to this lawful basis and challenge whether the grounds for the processing override their interests, rights and freedoms.

Necessary for the legitimate interests of the controller or a third party

The processing is necessary for the University's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests

In the case of personal data relating to criminal convictions and offences, it must be covered by a lawful basis set out in the DPA.

If you have any questions in relation to the application of a lawful basis, please contact University's Information Compliance Manager.

APPENDIX B: CONDITIONS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA (Article 9)

The GDPR sets out conditions for processing Special Categories of personal data. The University requires a lawful basis for processing personal data under Article 6 of the GDPR as well as one of the bases in Article 9 in order to process these categories of data.

- the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the data subject cannot consent to the processing;
- 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;
- 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;
- 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 subjects;

- processing relates to personal data which are manifestly made public by the data subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- 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;
- 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 provided those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies;
- 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 the data subject, in particular professional secrecy;
- 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.

Note: Part 3, Chapter 2 of the Data Protection Act 2018 set out some additional grounds for processing ‘special categories of personal data’ (such as health data) under Irish law, in addition to those contained in Article 9 of the GDPR. Notably, these include a legal basis to process health data for insurance, pension or mortgage purposes.

APPENDIX C: CONDITIONS FOR PROCESSING PERSONAL DATA ABOUT CRIMINAL CONVICTIONS OR OFFENCES (Article 10)

The GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings or convictions. Instead, there are separate

safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

To process personal data about criminal convictions or offences, you must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. You must determine your condition for lawful processing of offence data (or identify your official authority for the processing) before you begin the processing, and you should document this.

The Data Protection Act 2018 (section 55) deals with this type of data in a similar way to special category data, and sets out specific conditions providing lawful authority for processing it.

Article 10 also specifies that you can only keep a comprehensive register of criminal convictions if you are doing so under the control of official authority.

APPENDIX D: CONDITIONS FOR CONSENT

Article 7 of the GDPR outlines the conditions for consent:

1. Where processing is based on consent, the University must be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

APPENDIX E: GUIDELINES ON PROCESSING PERSONAL DATA RELATING TO CHILDREN

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all of your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 16 or over are able provide their own consent.
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.
- You should refer to the following Data Protection Commission publication for further guidance: Fundamentals for a Child-Oriented Approach to Data Processing

APPENDIX F: EXAMPLES OF PERSONAL DATA*

The following is a list of the types of data which would be considered to be 'Personal Data'. Please note: this list is not exhaustive.

People's names	Contact Details (incl. Home address, home phone/mobile nos., email addresses)
Date of Birth/Age	Birthplace/citizenship/nationality

Gender	Marital Status
PPS Numbers	Student/Staff Nos.
National ID Card details/Nos.	Next of kin / dependent / family details
Photographs	CVs
Personal financial data (e.g. Bank account details, credit card Nos.)	Details of gifts/donations made
Income / salary	Blood samples (linked to identifiable individuals)
Fingerprints/biometric data	CCTV images
Video images containing identifiable individuals	Voice recordings
Employment History	Sick leave details/medical certificates
Other leave data (excl. sick leave)	Qualifications/Education Details
Work performance	References for staff/students
Grievance/Disciplinary Details	Examination/assignment results
Membership of Professional Associations	Signatures (incl. Electronic)
Passwords & PINS	Continuous Professional Development (CPD) records
Car registration details	Clinical files relating to research participants

Online identifiers (e.g. IP address)	Location data
Data relating to children	Research subject consent forms

SPECIAL CATEGORIES OF PERSONAL DATA:	
Racial or Ethnic origin	Biometric data for the purpose of uniquely identifying a natural person
Political opinions	Data Concerning health
Religious or philosophical beliefs	Data concerning a person's sex life or sexual orientation
Membership of a trade union	Genetic data
Data relating to the commission or alleged commission of any offence (incl. Garda vetting data)	**Any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings**

*While the Data Protection legislation only applies to data relating to LIVING individuals, due care and attention should also be given to personal/sensitive data relating to deceased individuals.

**Whilst criminal offences are no longer included in the definition of Special Categories of Personal Data, the collection and processing of criminal offence data is given special protection in the GDPR.