



UCD Data Protection Policy

Purpose of this policy

This policy is a statement of University College Dublin's (UCD) commitment to protect the rights and privacy of individuals in accordance with the GDPR.

Scope of this policy

This policy applies to all personal data created or received in the course of University business in all formats and of any age. It applies to all locations where personal data is held by UCD. Personal data may be held or transmitted in paper, physical and electronic formats or communicated verbally in conversation or over the telephone. All staff, students, third parties engaged with UCD and processing personal data are all subject to the provisions of the Data Protection Policy.

Context

UCD needs to collect and use personal data (information) about its staff, students and other individuals who come into contact with the University. The purposes of processing personal data include the organisation and administration of courses, examinations, research activities, the recruitment and payment of staff, compliance with statutory obligations, etc. Data Protection law safeguards the privacy rights of individuals in relation to the processing of their personal data. The EU General Data Protection Regulation (GDPR), which came into force May 2018, confers rights on individuals as well as responsibilities on those persons processing personal data. Personal data, both automated and manual, are data relating to a living individual who is or can be identified, either from the data or from the data in conjunction with other information.

Definition of Personal Data

Personal data is any information that can identify an individual person. This includes a name, an ID number, location data (for example, location data collected by a mobile phone) or a postal address, online browsing history, images or anything relating to the physical, physiological, genetic, mental, economic, cultural or social identity of a person.

Special Categories of Data (previously also known as sensitive personal data) can only be processed under specific circumstances as outlined in Article 9 of the Regulations. The special categories are:

- personal data revealing racial or ethnic origin
- personal data revealing political opinions
- personal data revealing religious or philosophical beliefs
- personal data revealing trade union membership
- genetic data and biometric data (where used for identification purposes)
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation

Data Protection Principles

Principles are an important part of data protection law, and are, in fact, at the core of the General Data Protection Regulation (GDPR), which is often referred to as 'principles-based' regulation. UCD undertakes to perform its responsibilities under the legislation in accordance with Article 5 of the GDPR as follows:

- **Obtain and process information lawfully, fairly and in a transparent manner** UCD obtains and processes personal data fairly and in accordance with its statutory and other legal obligations
- **Keep it only for one or more specified, explicit and lawful purposes**
UCD keeps personal data for purposes that are specific, lawful and clearly stated. Personal data will only be processed in a manner compatible with these purposes

- **Use and disclosure only in ways compatible with these purposes**
UCD only uses and discloses personal data in circumstances that are necessary for the purposes for which it collects and keeps the data
- **Keep it safe and secure**
UCD takes appropriate security measures against unauthorised access to, or alteration, disclosure, or destruction of data and against accidental loss or destruction
- **Keep it accurate, complete, and up to date**
UCD operates procedures that ensure high levels of data accuracy, completeness, and consistency
- **Ensure it is adequate, relevant, and not excessive**
Personal data held by UCD are adequate, relevant, and not excessive in data retention terms
- **Retain for no longer than is necessary**
UCD has a policy on retention periods for personal data

Lawfulness of Processing

Each processing operation involving personal data needs to be based on one or more lawful basis. There are six available lawful bases for processing personal data under Article 6. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

The lawful bases for UCD are:

- **Consent:** UCD has an individual's freely given, specific, informed and unambiguous consent and indication of the data subject's wishes
- **Contract:** the processing is necessary for a contract UCD has with the individual, or because they have asked UCD to take specific steps before entering into a contract
- **Legal obligation:** the processing is necessary for UCD to comply with the law (not including contractual obligations).
- **Vital interests:** the processing is necessary to protect someone's life
- **Public task:** the processing is necessary for UCD to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law. UCD will rely primarily on this lawful base for processing personal data as necessary for and connected with the performance of its statutory functions under the Universities Act and related legislation
- **Legitimate interests:** the processing is necessary for UCD'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

UCD will decide which lawful basis applies depending on the specific purposes and the context of the processing. More than one basis may apply, however no one basis should be seen as better, safer or more important than the others; there is no hierarchy in the order of the list in the GDPR.

Rights of Data Subjects

Individuals have the following rights over the way UCD process their personal data:

Right of Access by the data subject

Individuals have the right to request a copy of their personal data UCD are processing about them and to exercise that right easily and at reasonable intervals. UCD has procedures in place to ensure that data subjects can exercise their rights under the GDPR, see www.ucd.ie/dataprotection

Right of rectification

Individuals have the right to have inaccuracies in personal data that UCD hold about them rectified.

Right to erasure

Individuals have the right to have their personal data deleted where UCD no longer has any justification

for retaining it, subject to legal obligations or exemptions such as the use of pseudonymised data for scientific research.

Right to restriction of processing

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

Right to data portability

Where it is technically feasible, Individuals have the right to have a readily accessible machine readable copy of their personal data transferred or moved to another data controller where UCD are processing their data based on their consent and if that processing is carried out by automated means.

Right to object

Individuals have the right to object to processing or restrict the processing of their personal data if:

- The processing is based on public interest; or in order to pursue a legitimate interest of the controller or a third party
- The personal data was processed unlawfully
- The personal data cannot be deleted in order to comply with a legal obligation

Right not to be subject to automated individual decision-making, including profiling

In certain circumstances individuals can object to profiling and automated decision making.

Transferring Personal Data outside the EEA

Flows of personal data to and from the European Union (the “EU”) are necessary for international collaboration and research. However, the transfer of such personal data from the EU to controllers and processors located outside the EU in third countries should not undermine the level of protection of the individuals concerned, with a third country being any country outside the European Economic Area (the “EEA”). Therefore, any UCD transfers to third countries or international organisations should be done in full compliance with the GDPR. Depending on the circumstances and nature of the data sets, a number of transfer mechanisms have to be explored, in line with [DPC Guidance](#). In most instances, transfers will also require contractual agreements between UCD and a receiving controller or processor, which specify roles and responsibilities of all parties involved regarding data protection obligations and the handling of personal data.

Information Technology and Data Protection

The University has established [IT policies and procedures](#) to safeguard essential services, protect the privacy of students and staff, and comply with contractual requirements and legislation.

Personal Data Security Breaches

A data security breach is any event that has the potential to affect the confidentiality, integrity or availability of data held by the University in any format. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Under the GDPR, where UCD is in control of *why* and *how* personal data sets are processed, the University, as data controller, is required to report relevant personal data breaches concerning those data sets to the Data Protection Commission (DPC) within 72 hours from the time of becoming aware of it. This reporting to the DPC is done through the Office of the DPO. In the event of any actual, potential or suspected personal breach of data security or confidentiality, to avoid the risk of harm to individuals, damage to operational business or severe financial, legal and reputational costs to the University, it is vital for anyone processing personal data on behalf of UCD, to take prompt action and to inform the Office of the DPO (gdpr@ucd.ie).

UCD, as data controller of the affected personal data sets, is expected to respond promptly and appropriately

to personal data breaches, including not only all relevant reporting obligations, but also, where appropriate, informing individuals affected. This can be necessary so that individuals affected can take preventative measures to reduce potential negative impacts.

UCD has developed a [Personal Data Incident Report Form](#) and [Guidance Document](#) to deal with these situations efficiently and effectively and to minimise the consequences of any personal breach occurring to the rights and freedoms of those data subjects.

Responsibility

UCD has overall responsibility for ensuring compliance with GDPR legislation when it is the data controller of personal data sets, or when it acts as processor of personal data on behalf of another controller. The Office of the DPO provides support, advice, and training to all UCD Units and employees to ensure that they are in a position to comply with GDPR, whenever they are processing personal data on behalf of the University.

However, all employees and students of UCD, who *separately*, i.e. not on behalf of UCD, collect and/or control the content and use of personal data, are individually responsible for compliance with the legislation.

Procedures and Guidelines

UCD is firmly committed to ensuring personal privacy and compliance with GDPR, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection. More information is available at www.ucd.ie/gdpr.

Review of Policy

This Policy will be reviewed regularly in light of any legislative or other relevant developments.

Contact

Office of the DPO

University College Dublin
Roebuck Castle
Belfield, Dublin 4, Ireland
Website: <http://www.ucd.ie/gdpr/contact/>
Email: gdpr@ucd.ie
Data Subject Access Requests: data.protection@ucd.ie