

DATA PROTECTION POLICY

Contents

1 Introduction 3

1.1 Purpose 3

1.2 Scope 3

1.2.1 To whom does the policy apply? 3

1.2.2 In what situations does the policy apply? 3

1.2.3 Who is responsible for ensuring that the policy (and any associated procedure) is implemented and monitored? 3

1.3 Definitions 4

2 Context 5

2.1 Legal and Regulatory Context 5

2.2 University Risk Management Framework 5

3 Policy Statements 5

3.1 Data Protection Principles 5

3.1.1 Processed lawfully, fairly and in a transparent manner: 6

3.1.2 Collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes 7

3.1.3 Adequate, relevant and is limited to what is necessary: 7

3.1.4 Accurate and kept up to date: 7

3.1.5 Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose for which the Personal Data is processed; 7

3.1.6 Processed in a manner that ensures appropriate security of the data ... 8

3.1.7 Accountability 8

3.2 Training and Development 9

4 Related Procedures for Data Protection 9

4.1 Procedure in the event of a Personal Data breach 9

4.2 Data Subject rights and requests 9

4.3 Further Information 10

5 Review 10

6 Related Documents 10

7 Document Control 10

1 Introduction

1.1 Purpose

In carrying out its functions, the University processes a large amount of personal data relating to students, staff and other individuals with whom we interact. Where the University processes personal data, it is subject to the obligations set out in the Data Protection Acts 1988 - 2018 and the EU General Data Protection Regulation, 2016/679 ("GDPR").

This purpose of this Policy is to provide information to University of Limerick employees to assist them in complying with Data Protection Legislation. The Policy affirms the University's commitment to protecting the personal data of individuals and to uphold the privacy rights of individuals in accordance with the Legislation.

1.2 Scope

1.2.1 To whom does the policy apply?

This Policy applies to all departments, offices, units, research centres and areas of work that form part of the University structure and applies to all personal data processed by the University. All full or part time employees, casual workers, agency workers and work experience students of the University who collect or use personal data as part of their duties, have a responsibility to ensure that they process personal data in accordance with the conditions set down in this Policy, the University's Privacy Notices, Data Protection Legislation and any other relevant University policies/regulations/procedures. For the purposes of this Policy, references to 'employee' throughout the remainder of this Policy shall include the foregoing.

1.2.2 In what situations does the policy apply?

The policy applies to any processing which is performed on personal data or on sets of personal data, by an employee of the University.

1.2.3 Who is responsible for ensuring that the policy (and any associated procedure) is implemented and monitored?

While the University as a whole has the overall responsibility for ensuring compliance with Data Protection Legislation, responsibility for the implementation of this Policy rests with the Head of each Academic / Administrative area / Principal Investigators[1] / Supervisors[2] to ensure good data handling practices are in place in order to uphold the privacy of personal data within their respective areas of responsibility.

[1] Principal Investigator: Employee of the University who has primary responsibility for the design, implementation, completion and management of a research project.

[2] Supervisor: An employee of the University in accordance with their responsibilities relating to the postgraduate's academic and research activities as described in Section 5 of the University of Limerick's Handbook of Academic Regulations and Procedures (Postgraduate Research Academic Regulations).

1.3 Definitions

1.3.1 **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. The University is a data controller and must adhere to its responsibilities under the Legislation.

1.3.2 **Data minimisation**: the collection and processing of personal data to the extent that is adequate, relevant and limited to what is necessary in order to achieve the given purpose and no more.

1.3.3 **Data Processor**: natural or legal person, public authority, agency or other body that processes personal data on behalf of a data controller.

1.3.4 **Data Protection Commission**: the supervisory authority with responsibility for monitoring the application of Data Protection Legislation.

1.3.5 **Data Protection Legislation**: the Data Protection Acts 1988 - 2018 and the EU General Data Protection Regulation, 2016/679 ("GDPR") as well as related guidance issued by supervisory authorities, including the Data Protection Commission and the European Data Protection Board.

1.3.6 **Data Protection Officer:** An individual appointed by the University to inform and advise on obligations under Data Protection Legislation and to act as the point of contact with the Data Protection Commission.

1.3.7 **Data Subject**: a living individual to whom personal data relates.

1.3.8 **Personal Data**: means any information, irrespective of the format in which it is held, relating to an identified or identifiable natural person.

1.3.9 **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, comprising:

- Collecting, obtaining, assembling, organising or storing personal data;
- Recording and structuring of personal data;
- Using, consulting and retrieving personal data;
- Altering, adapting, erasing, restricting, combining, aligning or destroying personal data;
- Disclosing personal data by transmission, dissemination or otherwise making available.

1.3.10 **Special Category Personal Data**: relates to the processing of personal data, irrespective of the format in which it is held, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Data Protection Legislation requires that additional conditions be met for the processing of such data.

2 Context

2.1 Legal and Regulatory Context

Where the University processes personal data, it is subject to the obligations set out in the Data Protection Acts 1988 - 2018 and the EU General Data Protection Regulation, 2016/679 ("GDPR") as well as related guidance issued by supervisory authorities, including the Data Protection Commission and the European Data Protection Board ("Data Protection Legislation").

2.2 University Risk Management Framework

The University's Risk Appetite Statement, as approved by Governing Authority, provides that the University has no appetite for any breaches in statute, regulation and professional standards. Failure to comply with this Policy could lead to such a breach.

3 Policy Statements

3.1 Data Protection Principles

The University undertakes to perform its responsibilities under Data Protection Legislation in accordance with the Data Protection Principles set out in Data Protection Legislation as follows:

Personal Data must be:

- **Processed lawfully**, **fairly and in a transparent manner** in relation to the data subject;
- **Collected for specified, explicit and legitimate** purposes and not further processed in a manner that is incompatible with those purposes;
- **Adequate, relevant and limited** to what is necessary in relation to the purposes for which it is processed;
- **Kept accurate and where necessary, kept up to date**: every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
- **Kept in a form which permits identification** of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- **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;

- The University as a data controller is responsible for and must be able to **demonstrate compliance** with the Data Protection Principles.

3.1.1 Processed lawfully, fairly and in a transparent manner:

- Personal data is obtained fairly and in a transparent manner if the data is obtained in accordance with the relevant privacy notice provided to the individual (available at https://www.ul.ie/corporatesecretary/data-protection) to ensure their awareness of:

    - the identity and contact details of the data controller;
    - the purpose and legal basis for processing personal data;
    - whether it is necessary to enter into a contract or whether there is an obligation to provide information and the possible consequences of failure to provide this information;
    - where legitimate interests are relied upon, the legitimate interests pursued by the data controller or third party;
    - recipients or categories of recipients of the personal data;
    - details of transfers to third countries, the fact of same and the details of the relevant safeguards and the means to obtain a copy of them or where they have been made available;
    - the storage period /criteria used to determine that period;
    - the rights of the data subject (access, rectification, erasure, restriction, objection and portability);
    - where processing is based on consent, the right to withdraw consent at any time;
    - the right to lodge a complaint with the Data Protection Commission;
    - where relevant, the existence of automated decision making;
    - contact details for the Data Protection Officer.

- Personal data is obtained lawfully where at least one of the following applies: (please refer to Privacy Notices available at https://www.ul.ie/corporatesecretary/data-protection):

    - The data subject has given **consent** to the processing of his /her personal data for one or more specific purposes;
    - Processing is necessary for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
    - Processing is necessary for **compliance with a legal obligation** to which the controller is subject;
    - Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
    - Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; or
    - Processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal

data, in particular where the data subject is a child. In all cases where the University seeks to rely on legitimate interests as a lawful basis, a legitimate interest assessment must be carried out and reviewed by the Data Protection Unit;
    - Special category personal data must only be processed where there is a lawful basis under Article 9 of GDPR.

- Where the University relies solely on consent as a condition of processing personal data, it must:
    - Obtain the data subject's specific, informed and freely given consent;
    - Ensure the data subject gives consent by a statement or clear affirmative action;
    - Document that statement/affirmative action;
    - Allow data subjects to withdraw their consent at any time.

3.1.2 Collected for a specified, explicit and legitimate purpose and not further processed in a manner that is incompatible with those purposes

- Personal data already collected for a specific, explicit and legitimate purpose may not be used for further processing if the secondary purpose is not compatible with the original purpose;
- Personal data must only be accessed in order to complete official functions of the University;
- Personal data must only be disclosed to work colleagues where the data is required to fulfil an official function of the University.

3.1.3 Adequate, relevant and is limited to what is necessary:

- The University follows the *"data minimisation principle"* whereby personal data held by the University should be adequate to enable the University achieve its purposes, and no more. Personal data must not be collected or held on a 'just in case' basis.

3.1.4 Accurate and kept up to date:

- An employee must seek to ensure that all personal data which is collected and processed by them on behalf of the University is kept accurate and up to date. Where any inaccurate or out of date data is identified, reasonable steps must be taken to have the data amended or erased as appropriate and local procedures established for same.

3.1.5 Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purpose for which the Personal Data is processed;

- Personal data should be held for the periods specified in the University's Records Classification and Retention Schedule (available at https://www.ul.ie/corporatesecretary/information-and-compliance/records-management). The retention and confidential destruction of personal data must be carried out in accordance with that Schedule.

3.1.6 Processed in a manner that ensures appropriate security of the data

The University will process personal data in a manner that ensures appropriate security and confidentiality, including protection against unauthorised or unlawful access, use, loss, alteration or disclosure.

- Use, storage and transfer of personal data in electronic format must be subject to stringent controls including those set out in University policies such as the IT Security Policy and Acceptable Usage Policy and associated procedures;
- Employees must ensure that personal data they have access to as part of their duties is kept securely at all times and is protected from inadvertent disclosure, loss, destruction, alteration or corruption;
- When upgrading/changing a PC, laptop or other electronic device, always ensure the contents of the hard drive are irrevocably deleted by an authorised ITD employee;
- Screens, printouts, documents, and files showing personal data must not be accessible to unauthorised persons;
- Personal data held in paper format must be stored securely in l o c k e d cabinets in locked rooms;
- Subject to the schedules set out in the University's Records Management Policy, personal data must be destroyed by confidential shredding/secure deletion when the retention period has expired;
- Personal data must be kept confidentially and must never be discussed with/disclosed to any unauthorised third party, either internal or external to the University, without the prior consent of the data subject, except where there is a statutory obligation to do so or there is another lawful basis in accordance with Data Protection Legislation;
- Personal data relating to a data subject must not be disclosed to any third party (except where required by law), even if they identify themselves as a parent, current/potential employer, professional body, sponsor, etc. Such disclosures must only be made with the consent of the individual concerned. This includes requests for contact details (e.g. address, mobile phone number) or even a request to confirm a person's attendance at the University;
- Where individuals (the data subjects) wish to discuss personal data relevant to themselves, the employee must confirm one or more facts that should be known only to the data subjects such as their date of birth, student number, mother's maiden name etc prior to any disclosure.

3.1.7 Accountability

GDPR obliges organisations to demonstrate that their processing activities are compliant with the Data Protection Principles. This includes the following:

- All functional areas that process personal data must maintain a personal data inventory to include details of personal data processed as required by Data Protection Legislation. All such local personal data inventories must be submitted annually to the Data Protection Unit of the University (dataprotection@ul.ie) by the functional area. Upon request, these inventories will be disclosed to the Data Protection Commission.

- Where personal data is shared with third parties, the appropriate data sharing or processing agreement must be put in place and reviewed with the Data Protection Unit. Such agreements must be signed in accordance with the UL Contract Signing Policy.

- Any international transfers of personal data must have measures in place to ensure that such transfers are lawful under Data Protection Legislation. All proposed international transfers of personal data must be reviewed by the Data Protection Unit (dataprotection@ul.ie).

- Where the processing of personal data may involve a high risk to Data Subjects, a DPIA screening questionnaire can be used to assess the risk. Where a high risk is indicated, a Data Protection Impact Assessment ("DPIA") must be carried out by the employee responsible for the processing. The DPIA should be submitted to the Data Protection Unit for review.

3.2 Training and Development

All employees must complete Data Protection training. Training will be provided through online training and webinars as well as in-person events.

4 Related Procedures for Data Protection

4.1 Procedure in the event of a Personal Data breach

4.1.1 A Personal Data breach may be defined as an incident where there is an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data through, for example, loss or theft of a portable device, accidental disclosure via email/other electronic system, loss of hard copy records etc.

4.1.2 All data breaches or suspected data breaches must be reported to the University's Data Protection Unit without delay for assessment. The Data Protection Officer will ensure, where appropriate and required, that the data subjects and the Data Protection Commission are notified. Where notification to the DPC is required, this will be done within 72 hours of the University becoming aware of the personal data breach.

4.2 Data Subject rights and requests

Under Data Protection Legislation, data subjects have a number of rights including those relating to obtaining access to their personal data, to rectification, erasure and to object to the processing of their personal data. Where a request is received, it should be directed to the University's Data Protection Officer immediately so

that it can be processed as efficiently as possible and within the timeframe specified in the legislation.

4.3 Further Information

Further information relating to data protection matters for employees is available on the University Data Protection Sharepoint site https://ulcampus.sharepoint.com/sites/CSCPLDataProtection.

5 Review

This Policy will be reviewed every three years in line with the University Policy Management Framework.

6 Related Documents

Related policies that should be read in conjunction with this Data Protection Policy include:

- University of Limerick Code of Conduct for Employees
- Data Protection Privacy Notices
- University of Limerick Records Management Policy
- University of Limerick Records Classification & Retention Schedule
- University of Limerick IT Security Policy
- University of Limerick Acceptable Usage Policy
- Information Technology Division Procedures
- University of Limerick Enterprise Risk Management Policy
- University of Limerick Contract Signing Policy

7 Document Control

Document Version	Version 2.0
Document Owner	Data Protection Officer
Approved by	Executive Committee
Date	28/01/2026
Approved by	Audit & Risk Committee
Date	06/03/2026
Approved by	Governing Authority
Date	26/03/2026
Effective Date:	26/03/2026
Scheduled Review Date:	26/03/2029