UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

DATA PROTECTION POLICY

Approved by Governing Authority
December 2018

1. Purpose of Data Protection Policy

1.1 The purpose of this Policy is to assist University of Limerick employees in adhering to the University's Privacy Notices and the Data Protection Acts 1988 & 2018 and the EU General Data Protection Regulation, 2016/679 (GDPR) ("the Legislation"). This Policy combined with the University's Privacy Notices (available at www.ul.ie/dataprotection) affirms the University's commitment to protecting the privacy rights of individuals in accordance with the Legislation.

2. Responsibilities of University Employees

2.1 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, the 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.

2.2 While the University as a whole has the overall responsibility for ensuring compliance with the 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.

3. Explanation of terms:

- **Personal Data**: means any information, irrespective of the format in which it is held, relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The legislation also differentiates between 'Personal Data' and **'Special Category Personal Data';**

1 Principal Investigator: An 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 who is assigned to a postgraduate research candidate at the time of their commencement of a postgraduate research project. The supervisor has 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 (Research Postgraduate Academic Regulations).

- **Special Category Personal Data** (previously known as "Sensitive" Personal Data) relates to the processing of personal data, irrespective of the format in which it 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 The Legislation requires that additional conditions be met for the processing of such data;

- **Data Subject**: a living individual to whom personal data relates;

- **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. Please refer to the University's Privacy Notices for further details in relation to the University's obligations (www.ul.ie/dataprotection).

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

- **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.

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

4. Role of Data Protection Commission ("DPC")

4.1 The DPC oversees compliance, monitors and enforces the Legislation. The Commission has a wide range of enforcement powers, including investigation of University records and record-keeping practices as well as the issuing of warnings, reprimands, corrective actions and administrative fines.

5. The University's Obligations under Data Protection and the Data Protection Principles:

5.1 This Policy aims to enable the University's compliance with GDPR. The University undertakes to perform its responsibilities under the legislation in accordance with the data protection principles outlined in the GDPR and the Data Protection Act 2018 as follows:

1	**Process personal data lawfully**, fairly and in a transparent manner in relation to the data subject;
2	**Collect for specified, explicit and legitimate** purposes and do not further process in a manner that is incompatible with those purposes;
3	**Ensure personal data is adequate, relevant and limited** to what is necessary in relation to the purposes for which it is processed;
4	**Keep 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 they are processed, is erased or rectified without delay;
5	**Keep 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;
6	**Process 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;
7	The University as a data controller is responsible for and must be able to **demonstrate compliance** with the Data Protection Principles.

5.2 **Processed in a way that is lawful, fair and transparent:**

- 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 www.ul.ie/dataprotection): to ensure their awareness of:

    - the identity and contact details of data controller;
    - the purpose and legal basis for processing personal data;
    - provide the information on whether it is necessary to enter into a contract or whether there is an obligation to provide information and the possible consequences of failure;
    - where legitimate interests are relied upon (article 6.1.f), the legitimate interests pursued by the data controller of 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 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 www.ul.ie/dataprotection):

  - 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 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.

- 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 affective action;
  - document that statement/affirmative action;
  - allow data subjects to withdraw their consent at any time.

5.3 **Collected for specified, explicit and legitimate purposes 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.

5.4 **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.

5.5 **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 must have local procedures established for same.

5.6 **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:**

- Personal data should be held for the periods specified in the University's Records Management & Retention Policy (www.ul.ie/recordsmanagement). The retention and confidential destruction of personal data must be carried out in accordance with that policy.

5.7 **Processed in a manner that ensures appropriate security of the data.**

- Use, storage and transfer of personal data in electronic format must be subject to stringent controls (e.g. use of password protection, timed log-out of systems, encryption of PC folders and portable devices, regular backup, use of anonymisation software; avoiding storage of a laptop in one's car or allowing unauthorised individuals to view computer screens displaying special category data etc);
- 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, always ensure the contents of the hard drive of your old PC 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 cabinets in locked rooms;
- Subject to the schedules set out in the University's Records Management & Retention Policy (www.ul.ie/recordsmanagement), personal data held 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 (e.g. if required for the purpose of preventing, detecting or investigating offences, required urgently to prevent damage to health or serious loss/damage to property, required under law etc.);
- Personal data relating to a data subject must not be disclosed to any third party, even if they identify themselves as a parent, current/potential employer, professional body, sponsor, etc. Such disclosures must only be 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.

6. Accountability

6.1 GDPR obliges organisations to demonstrate that their Processing activities are compliant with the Data Protection Principles that includes the following:

- All functional areas that process personal data must maintain a personal data register which must include details on personal data collected, held or processed. All such local personal data registers must be communicated to the Data Protection Unit of the University (dataprotection@ul.ie) when updated by the functional area;
- Upon request, these registers will be disclosed to the Office of the Data Protection Commissioner.

The University's personal data registers will contain the following information:

- contact details of the Head of functional area/their nominee;
- list of personal data being processed;
- categories of data subjects;
- Processing activities;
- Categories of recipients with whom the data will be shared;
- Retention periods;
- Descriptions of the security measures implemented in respect of the processed data;
- Deletion authorisation and methods;

6.2 Any international transfers must have measures in place to ensure that such transfers are lawful through liaison with the Data Protection Unit (dataprotection@ul.ie).

7 Training and Development

7.1 Data Protection training will be provided through online training, presentations, attendance at Data Protection specific training events and seminars where appropriate, employee briefings and information notices.

8 Procedure in the event of a Personal Data breach

8.1 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.

8.2 All data breaches or suspected data breaches must be reported to the University's Data Protection Unit without delay for assessment. The University's Data Breach Procedure and Data Breach Report Form are available at www.ul.ie/dataprotection. The Corporate Secretary's Office will ensure, where appropriate and required, that the data subjects and the Data Protection Commission are notified

8.3 Breaches of the terms and conditions of this Policy and the University's Privacy Notices (available at www.ul.ie/dataprotection) could result in major reputational and financial damage to the University and may result in Statute No. 4 of the University of Limerick: 'Employee Disciplinary Matters & Termination of Employment' being invoked.

9 Data Subject rights and access requests

9.1 Under the Data Protection legislation, data subjects are entitled to make a request for their personal data held by the University. Where an access 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. See the University's Privacy Notices for further details on subject access requests and Data Subjects' rights (www.ul.ie/dataprotection).

10 Contact Details of the Data Protection Officer

10.1 The Data Protection Officer of the University may be contacted at dataprotection@ul.ie; Address: Corporate Secretary's Office, University of Limerick, V94, T9PX, Ireland.

11 Further information

11.1 This Policy sets out key areas of work at the University where data protection issues may arise and outline best practice in dealing with them. However, it is not envisaged that this Policy contains an exhaustive list of all areas of work to which Data Protection principles apply and employees should refer to the additional resources available at www.ul.ie/dataprotection or contact the Data Protection Unit within the Corporate Secretary's Office by email to dataprotection@ul.ie.

11.2 Extensive information is also available from the Data Protection Commissioner's website, www.dataprotection.ie or from the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois.

12 Review

12.1 This Policy will be reviewed regularly and at least on a biennial basis.

13 Related Policies

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

- University of Limerick Records Management & Retention Policy;
- University of Limerick Code of Conduct for Employees;
- Data Protection Privacy Notices;
- University of Limerick Research Integrity Policy
- Clinical Research Policy for UL Sponsored Regulated Clinical Trials;
- Risk Management Policy;
- Information Technology Division Policies and Regulations available at https://ulsites.ul.ie/itd/policies-regulations