RECORDS MANAGEMENT POLICY

Contents

1 Introduction

1.1 Purpose

The purpose of this Policy is to ensure the management of complete, usable and reliable records within the University, which serve as evidence of the performance of University functions and activities, comprise a vital source of knowledge regarding how and why decisions were taken and ensure accountability for as long as is required.

Records of the University consist of recorded information created or received by the University, regardless of format.

Records Management is the systematic control of the creation, receipt, maintenance, use and disposal/archive of records and includes *inter alia*: classification, management of filing systems, retention scheduling; management of record conversion programmes, business continuity records planning, vital records protection and backup of files etc.

This Policy is implemented in conjunction with the University's Records Classification & Retention Schedule (available at www.ul.ie/recordsmanagement).

1.1.1 Objectives

The objectives of this Policy are to:

- Establish the framework for records management within the University;
- Assist and enable employees to adhere to University policies thereby meeting its regulatory compliance obligations, confidentiality requirements and business needs;
- Promote day-to-day efficiency and good office management;
- Ensure preservation of records of permanent value and to ensure continued and appropriate access to them;
- Ensure timely destruction of records that no longer need to be retained.

1.2 Scope

1.2.1 To whom does the policy apply?

All full or part time employees, casual workers, agency workers and work experience students of the University who access/use University records as part of their duties have a responsibility to ensure that they handle them in accordance with the conditions set down in this Policy, the University Records Classification & Retention Schedule and any other relevant University policies/regulations/procedures. For the purposes of this Policy, references to 'employees' throughout the remainder of this policy shall include the foregoing.

This Policy is relevant to all areas and locations of the University and includes all departments, faculties, offices, units, research centres, institutes and areas of work which form part of the University structure. For the purposes of this Policy, references to the above will be shortened to "Functional Area".

1.2.2 In what situations does the policy apply?

All records created, or received, and maintained in the course of its official business constitute the official records of the University of Limerick. This Policy applies to all records of the University.

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

It is the responsibility of all employees in each functional area to ensure that they manage University records in compliance with this Policy including the observation of appropriate security measures for maintaining records containing personal or other confidential information.

Responsibility for monitoring the implementation of this Policy rests with the Head of each functional area.

Where records are used by more than one functional area, the Heads of the respective functional areas are required to ensure there is clarity about which area has primary responsibility for their management. This should be established and documented between the relevant areas at the time the record(s) are created/received.

1.3 Definitions

1.3.1 Record

A record is defined as information/data held in any format, which is either created or received and maintained by the University in the course of its official business.

1.3.2 Personal Data

'Personal Data' means any information/data, irrespective of the format in which it is held, relating to an identified or identifiable living person

1.3.3 System

A hardware unit, software program and/or business process used by staff to help achieve a given business purpose (e.g. student records system, employee records system etc).

It is the responsibility of the System Owner (the Head of the functional area that utilises the system or their nominee) to monitor and ensure compliance with this Policy by employees involved in the use of the system.

2 Context

2.1 Legal and Regulatory Context

2.1.1 Data Protection Acts 1988-2018, EU General Data Protection Regulation (GDPR)

The University is required to take appropriate technical and organisational measures to ensure the safety and security of personal data it processes.

2.1.2 Freedom of Information (FOI) Act 2014

The University is required to comply with the obligations set out under the Freedom of Information (FOI) Act 2014.

2.2 Other Context

2.2.1 University Risk Management Framework

The University's Risk Appetite as approved by Governing Authority provides that the University has **no appetite** for any breaches in statute, regulation, professional standards, research ethics, bribery, or fraud. The lack of appropriate records management may lead to a breach of this nature.

3 Policy Statements

3.1 Records Management Principles

3.1.1 The University is committed to ensuring that a framework for records management is established and maintained within the University, to assist and enable employees to adhere to University policies and thereby meet regulatory compliance obligations, confidentiality requirements and business needs;

3.1.2 The University is committed to responsible collection, handling, retention and destruction/ archiving of records;

3.1.3 The University is committed to ensuring roles and responsibilities are clearly defined in relation to Records Management.

4 Related Procedures for Records Management

4.1 Creation/Receipt and Ownership

Records that are created and/or received by staff in the course of their duties are and remain the property of the University and are subject to the provisions of this Policy.

4.2 Responsibilities and Good Practice

All staff are required to employ the following best practice in the management of records and responsibility for monitoring implementation rests with the Head of each Functional Area:

- sensible and consistent naming of records and files;
- systematic set up and maintenance of filing systems to facilitate retrieval;
- ensure appropriate security measures are in place and storage of records in a manner that ensures access for authorised users only;
- protection of vital records and backup of appropriate files on a regular basis;
- the management of records held in off-site storage etc;
- business continuity planning;
- preservation of records of permanent value in order to ensure continued and appropriate access to them;
- regular, secure destruction of records (including email records) in accordance with the Classification & Retention Schedule;
- engaging with the University's Glucksman Library in the archiving of records;
- restrict access to record systems (eg by ensuring appropriate permissions are in place for all University systems, use of passwords, timed lock out of PCs etc.).

4.3 Classification

All University records belong to one of the classifications set out in Table 1, i.e**. 'Public', 'Protected' or 'Confidential'**.

The classification level applied to a record should take account of the organisational needs for sharing or restricting the record and the associated impacts and risks as a consequence of the record being handled inappropriately.

The University's Records Classification & Retention Schedule lists the major records types held by the University along with the retention time for each record type and the classification that applies.

In the event that a record has not yet been included in the Schedule, the default classification for University records shall be identified by the Functional Area based on the classification descriptions set out in Table 1 and steps will be taken to ensure the record type is added to a future iteration of the Schedule by contacting the Information & Compliance Officer at recordsmanagement@ul.ie.

When classifying a collection of records, the most restrictive classification of any of the individual elements of information in the records should be used. Please note however, that categorising information as protected/confidential does not exclude it from consideration for disclosure under the Freedom of Information Act or Data Protection legislation.

Table 1: Records Classification

Records Classification	**Public**	**Protected**	**Confidential**
Records description	Records which are available publicly and where confidentiality is of no significance.	Records intended for internal distribution within the University and where, in the event of disclosure/loss, there would be a low / moderate risk of embarrassment or reputational damage.	Inappropriate disclosure of records in this classification would result in one or more of the following: • adversely affect University reputation or operations, • cause serious distress to individuals / breach statutory restrictions on disclosure of information; • result in financial / legal penalties, • risk legal action or severe reputational damage to the University.
Examples include but are not limited to:	• *published Policies/ Procedures, Annual Reports etc;* • *campus Maps;* • *course brochures;* • *job advertisements* • *public web pages* • *press releases* • *semester dates etc.*	• *internal telephone directory;* • *user manuals;* • *staff newsletters etc.*	• *personal data;* • *secret / confidential business information eg, certain financial data, legal advice etc* • *commercially sensitive information;* • *information that is part of a deliberative process.*

4.4 Handling

All University records belong to one of the classifications set out in Table 1, e.g. **'Public', 'Protected' or ''Confidential'** and are subject to the handling practices and where applicable, handling restrictions, set out in Table 2. All employees must take care to ensure that confidential records as indicated in the Retention Schedule are handled in accordance with these handling practices.

Table 2: Handling Practices and Restrictions for University Records

Classification	Public	Protected	Confidential
Access control	No restrictions specified	Restrict access to UL employees	Access restricted to authorised UL employees on a 'need to know' basis
Physical Storage	No restrictions specified	Filing cabinet or equivalent in a locked or attended office	
Electronic Storage *(e.g. on Sharepoint, MS OneDrive for Business, UL provided Sharedrive etc)*	No restrictions specified	On University managed IT facilities that are in compliance with the UL IT Security Policy & the UL Acceptable Usage Policy and have appropriate access controls implemented	
Storage on University Mobile Devices *(e.g. UL laptops, tablets, mobile phones etc)*	No restrictions specified	Permitted in compliance with the UL IT Security Policy, UL Acceptable Usage Policy and relevant ITD Procedures	
Storage on Personal Devices *(e.g. non-UL laptops & tablets, non-UL mobile phones etc)*	No restrictions specified	Permitted	Not Permitted
Use of portable/removable media *(e.g. USBs, Hard Drives, CDs etc)*	No restrictions specified	Use of portable/removable devices is strongly discouraged. Microsoft OneDrive for Business/Sharepoint should be used as an alternative to the use of removable media wherever possible. If there is absolutely no alternative, removable media must be encrypted & used in compliance with the UL IT Security Policy and relevant ITD Procedures	
Sharing *(e.g. Transmission via UL-managed/approved systems HEANET File Sender etc)*	No restrictions specified	Share records on a 'need to know' basis via University managed IT facilities that are in compliance with the UL IT Security Policy, the UL Acceptable Usage Policy and relevant ITD Procedures	
Email	No restrictions specified	Permitted – utilise official UL email account only	Permitted – utilise official UL email account only where alternative approved sharing methods are unsuitable. Password protect attachments prior to sending
Post	No restrictions specified	Sealed envelope, with return address clearly marked on envelope and sent via An Post	Use either of the following: • Securely sealed envelope, marked *Confidential*, with return address clearly marked on envelope & sent via An Post; or • Recorded courier / An Post Registered delivery
Marking	Not required	Not required	Recommended that records/files be marked "Confidential" so it is apparent to the user that appropriate extra care must be taken

4.5 Retention

Records should be retained for as long as required to meet the legal, administrative, financial and operational requirements of the University during which time, they should be managed appropriately. Following a period of time, as set out in the University of Limerick Records Classification & Retention Schedule, records should be either archived or destroyed appropriately.

4.5.1 Retention Schedule

The Records Classification & Retention Schedule prescribes the retention period for a range of records held by the University (available at www.ul.ie/recordsmanagement).

Any Functional Area which considers that records should be retained for a longer or shorter period than that set down in the University Classification & Retention Schedule is required to consult with the Information & Compliance Officer (recordsmanagement@ul.ie) to ensure that reasonable justification exists for their retention. In the case of records which contain personal data, to ensure compliance with the GDPR and the Data Protection Acts (1988-2018) they are required to consult with the Data Protection Officer (dataprotection@ul.ie).

4.6 Destruction

Once records have been retained (in situ or off-site storage) for the requisite time as stipulated in the Records Classification & Retention Schedule, they must be securely destroyed or archived for permanent retention as set out in the schedule.

When scheduled for destruction, records must be shredded, pulped or otherwise disposed of securely. For in-house destruction, the relevant Functional Area should document and retain the date and manner of destruction of records. In the case of third-party destruction, a certificate or docket confirming destruction should be received and retained as proof of destruction.

4.7 Archiving

Records with lasting historic and business value will be identified primarily through the University's Classification & Retention Schedule. Records which are identified for indefinite retention must be retained within the Functional Area for as long as they continue to be in active use. Following this, they shall be appraised by the Functional Area in consultation with the University Archivist and transferred to the University Archive.

These records will become part of the University's Archive and will provide an enduring record of the conduct of University functions and operations.

5 Related Documents

University of Limerick Records Classification & Retention Schedule
University of Limerick IT Security Policy
University of Limerick Acceptable Usage Policy
ITD Disaster Recovery Procedure
ITD Network Access Procedure
ITD Access Control Procedure
University of Limerick Data Protection Policy
University of Limerick Data Protection Impact Assessment Process
University of Limerick Risk Management Policy
University of Limerick Signing Authority Policy

6 Document Control

Document Version	Version 3.0 Records Management Statement & retention schedules (v.1) were formally put in place in 2002. Records Management & Retention Policy (v.2) superseded this in 2012.
Document Owner	Corporate Secretary
Approved by	Executive Committee
Date	15 September 2021
Approved by	Audit & Risk Committee
Date	8 February 2022
Approved by	Governing Authority
Date	24 February 2022
Effective Date:	24 February 2022
Scheduled Review Date:	24 February 2025