MTU

Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Data Retention Policy

26th March 2021

Version: 1.0

www.mtu.ie/policies

Table of Contents

1. Overview

The University is responsible for the processing of a significant volume of information. These records are evidence of functions and activities performed across the University.

Good quality records are of value to any organisation, and their effective management is necessary to ensure that the records are retained in line with the university retention schedule. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

a) Comply with information management policies, legal and regulatory requirements (including the Freedom of Information Act 2014, the General Data Protection Regulation 2018), international standards, and best practices;
b) Are authentic, reliable and complete;
c) Are protected and preserved as evidence to support future actions;
d) Ensure current and future accountability;
e) The University has an appointed Data Protection Officer ('DPO') who is available to provide guidance and advice pertaining to this requirement; and,
f) All Staff must appropriately protect and handle information in accordance with University policies.

This document aims to inform the efficient management of records to a standard which meets accepted best practice. This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. Purpose

The purpose of this policy is to ensure that the University applies retention periods appropriately and retains data only for the period for which it is allowed. It sets out the roles and responsibilities in relation to data retention that are necessary to ensure that the University remains compliant with this policy.

3. Scope

The policy applies to:

a) all records created, received or maintained by the University;
b) all records, regardless of format;
c) Any person who is employed by the University who receives, handles or processes data in the course of their employment;
d) Any student of the University who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose; and,
e) Third party companies (data processors) that receive, handle, or process data on behalf of the University.

4. Definitions

Data	As used in this Policy shall mean information which either: a) is processed by means of equipment operating automatically in response to instructions given for that purpose; b) is recorded with the intention that it should be processed by means of such equipment; c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; d) Does not fall within any of the above, but forms part of a readily accessible record. Data therefore includes any digital data transferred by computer or automated equipment, and any non-digital data which is part of a relevant filing system.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any personal data are, or are to be, processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or processes personal data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the personal data. An employee of a Data Controller, or a School or Function within a University which is processing personal data for the University as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the processing of personal data would be a Data Processor. It is possible for one University or person to be both a Data Controller and a Data Processor, in respect of distinct sets of personal data. It should be noted however that, if you are uncertain as to whether the University is acting as a Data Processor or a Data Controller of personal data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by the University. Examples of personal data include, but are not limited to: a) Name, email, address, home phone number; b) The contents of an individual student file or HR file; c) A staff appraisal assessment; d) Details about lecture attendance or course work marks; e) Notes of personal supervision, including matters of behaviour and discipline.

Records	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Third Party	Means an entity, whether or not affiliated with the University, that is in a business arrangement with the University by contract, or otherwise, that warrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where the University has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third-Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to process personal data.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.

5. Roles & Responsibilities

The following roles and responsibilities apply in relation to this Policy:

Responsible Office/Person(s)	Role
Governing Body	• To review and approve the policy on a periodic basis.
President	• Ensure processes and procedures are in place within the University to facilitate adherence to the Data Retention Policy.
University Executive Team (UET)	• Implement the Data Retention policy and advocate a GDPR compliant culture.
Data Protection Officer (DPO)	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacy obligations.

	• To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to the University Executive Team and the Audit and Risk Committee. • To report directly on data protection risk and compliance to executive management.
Legal Services	• Review and provide policy input and related documentation, e.g. standards and guidelines. • Provide information retention and disposal legal advice to the University. • Assist with contract drafting relating to external service providers providing information retention and disposal services.
Head of Function (Academic/Administrative/Research)	• Implementing the Data Retention Policy in their areas of responsibility. • Ensuring ongoing compliance with this policy in their respective areas of responsibility. • Ensuring information required in relation to data retention activities is provided to the Data Protection Officer. • Manage University information, in compliance this policy and related standards.
IT Services	• Review and provide policy input and relevant related documentation, e.g., IT, policies, standards, and guidelines. • Allow appropriate access, where requested, to the Information Owner or their appointed representatives.
Staff/Students/External Parties	• Read and understand this policy document. • Manage information in compliance with this policy. • Contact their Head of Function. (Academic/Administrative/Research) or Data Protection Officer if in any doubt.

6. Policy

6.1 Ownership of Records

All records, irrespective of format, (i.e. both textual and electronic, including emails) created or received by University employees, students, contractors or other third parties in the course of their duties on behalf of the University, are the property of the University and subject to its overall control.

On resignation, retirement, or change of position, employees should transfer all relevant records to their successor or Head of Function.

6.2 Management of Records

All records are retained for as long as they are required to meet the legal, administrative, financial, and operational requirements of the University.

After this they are either destroyed or archived.

The final disposition of records is carried out according to the University's Record Retention Schedule.

Records containing personal information should be stored in accordance with the University's Data Protection Policy and in line with national and European Data Protection legislation. Any area which considers that such records should be retained for a longer period than that set down in the Records Retention Schedule is required to consult the Data Protection Officer to ensure that reasonable justification exists for their retention and compliance with the General Data Protection Regulation.

The University must define appropriate Management Processes to comply with information management policy, legal and regulatory requirements, international standards, and best practices.

These processes must be:

a) Based on the information owner's approval of these information use processes;
b) Sufficiently flexible to cope with temporary changes to retention requirements for example if information is required for investigations or potential litigation;
c) Cognisant of other department's dependence on any retained or disposed information;
d) Use appropriate security requirements based on School and Function information classification levels as laid out in the Information Security Policy;
e) Include appropriate retention mechanisms facilitating reasonable retrieval times to support University business, regulatory or disposal requirements; and,
f) Use and maintain appropriate and durable information retention/retrieval mechanisms to prevent damage, degradation or unauthorised alteration and ensure retrieval at any time.

The University must develop, maintain, procure and manage information retention and disposal procedures, mechanisms, facilities and services to ensure that they are effective.

6.3 Implementation

Operational responsibility for the implementation of this policy rests with the Head of Function (Academic/Administrative/Research).

Each Head of Function must:

a) Ensure that all records, within their area of responsibility, which must be retained, has been identified, recorded, and assessed to ensure that it is appropriately managed through-out the retention and disposal lifecycle in accordance with the University's Data Retention Schedule;
b) Ensure that appropriate procedures are in place to manage this information effectively through all stages of the retention and disposal lifecycle, and that these procedures are reviewed periodically to assess their effectiveness and changes are communicated to all relevant parties;
c) Ensure that all students, staff (permanent and temporary), vendors, independent contractors, consultants and other persons or entities that use the University resources, charged with managing retained information are fully familiar with and trained on all of the relevant procedures and that they are aware of their responsibilities;
d) Where applicable, ensure that contractual or other agreements are in place with external third parties participating in the design and/or provision of information retention and disposal services, in order to protect the interests of the University, its staff and its students and to minimise risk to the University, its employees and its (potential, past, or current) students. This must include, as a minimum, provisions for non-compliance with defined policies and standards, malicious or negligent activities by their employees or agents, and termination of agreement. Agreements must ensure that University information and related records, on which the University is reliant, are available and appropriately protected until the period of reliance has elapsed and ensure that contractors or external service providers allow reasonable audits and inspections access;
e) Provide timely notification, where applicable to students, staff (permanent and temporary), vendors, independent contractors, consultants and other persons or entities that use University resources, when information is required to be retrieved, e.g. to support investigations or litigation, to prevent this information from being destroyed;
f) Ensure that procedures are in place to retrospectively assess existing information, stored prior to the implementation of this policy, to ensure that it is appropriately documented, managed and disposed of as required. Any inability to comply with this policy in a timely manner must be risk assessed and residual risks must be reported via the regular Risk Management processes; and,
g) Report all serious breaches of compliance, including those which may have legal or regulatory implications, to the DPO.

7. Policy Compliance

7.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to the University and an infringement of the rights of employees or other relevant third parties.

7.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer in advance.

7.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the Data Protection Officer.

Document Control

A. Document Details

Title:	Data Retention Policy
Owner(s):	Vice Presidents for Finance & Administration and Corporate Affairs
Author(s):	Data Protection Officers
This Version Number:	1.0
Status:	Approved
Effective Date:	26/03/2021
Review Date:	03/2022

Important Note: If the 'Status' of this document reads 'Draft', it has not been finalised and should not be relied upon. An existing approved policy is deemed relevant until such time as an updated policy has been approved by the relevant approval authority and becomes the new binding policy.

B. Revision History

Version Number	Revision Date	Summary of Changes	Changes tracked?	Proposed Revision Date
0.1	30/10/2020	Initial Draft of Policy based on Cork and Tralee policies.	Yes	
0.2	09/02/2021	Updated based on feedback from DPOs – Overview section, Roles & Responsibilities of DPOs.	Yes	
0.3	18/02/2021	Review by IT Managers, updated roles and responsibilities section.	Yes	

C. Relevant/Related Existing Internal/External Documents

Data Protection Policy
Data Protection Procedures
Information Governance Policy
Information Security Policy
Data Access Management and Privileged User Policy
Data Handling & Clean Desk Policy
Data Protection Breach Response Policy

The above list is not exhaustive and other University documents may also be relevant.

D. Consultation History

This document has been prepared in consultation with the following bodies:

E. Approvals

This document requires following approvals (in order where applicable):

Name	Date	Details of Approval Required
Governing Body	26/03/2021	Approved by Governing Body

F. Responsible for Communication and Implementation

The Manager/Functional Area responsible for communication and implementation of the policy:

Title	Functional Area	Date Implemented
Data Protection Officer	Corporate Affairs	26/03/2021