MTU
Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Information Governance Policy

26th March 2021

Version: 1.0

www.mtu.ie/policies

Table of Contents

1. Purpose

The purpose of this policy is to provide direction on the classification, ownership, deletion and retention of data and information for the University as well as clarifying accountability for data and information. Data and information as pertaining to this policy includes electronic and non-electronic data.

The University is reliant upon the confidentiality, integrity, and availability of its data and information to successfully conduct its operations, meet student and staff/faculty expectations, and provide services. All staff, students, and external parties of the University have a responsibility to protect University data and information from unauthorized generation, access, modification, disclosure, transmission, or destruction and are expected to be familiar with and comply with this policy.

University data and information is an important asset and resource. All data and information is categorised according to appropriate needs for protection, handling and compliance with regulatory requirements. The purpose of classification is to ensure that data and information is managed in a manner appropriate to the risks associated with ensuring that it remains reliable, trustworthy and available for appropriate use.

It is also provided to make staff aware of their responsibilities for the protection of sensitive/confidential data and information and that access to such data and information should be restricted to appropriate authorised personal that require this access and that personal information is only disclosed to third parties as it applies as detailed in Appendix A.

2. Scope

This Information Governance Policy relates to all University data (paper, electronic, on-premise, cloud, backups, etc) including but not limited to:

a) University Student Data;
b) University Staff Data;
c) University Financial Data;
d) University Commercial Data;
e) University Intellectual Property;
f) Academic Data; and,
g) Research Data.

This policy also applies to any information created from University data. The University is committed to ensuring that all University data is clearly identified and an inventory of all important data is drawn up and maintained. The data inventory includes data held on all University data and information. Appendix A provides a template for the maintenance of a data inventory.

This policy applies to:

- Any person who is employed by the University who receives, handles or processes data in the course of their employment;
- Any student of the University who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose;
- Third party companies (data processors) that receive, handle, or process data on behalf of the University.

This applies whether you are working in the University, travelling or working remotely.

3. Definitions

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Confidential Data	Includes any data covered by General Data Protection Regulations under the category of personal data. This also includes information considered to be commercially sensitive to the University. Examples include strategic plans or intellectual property.
Data	As used in this Policy shall mean information which either: • Is processed by means of equipment operating automatically in response to instructions given for that purpose; • Is recorded with the intention that it should be processed by means of such equipment; • Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; • 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 manual information which is part of a relevant filing system.
Data Classification	A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately, and/or data being lost. The resulting data classification can be associated with a minimum level of control which then needs to be applied when handling data. It is the responsibility of data owners to classify their data.
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 Ownership	A process whereby information/data is assigned an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature. Refer to Information Security Policy on controls over creation, transmission, storage.
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. A staff member 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 Data Protection Officer or Legal team.
Data/Record Retention Schedule	The maximum period of time information/data should be retained by the University for legal and business purposes. It is the responsibility of data owners to define the retention period for their records/data and the eventual fate of the records/data on completion of this period of time.
Data Subject	Refers to the individual to whom personal data held relates, including: staff, students, customers and students.
Encryption	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. Refer to the Information Security Policy relating to information protection for further guidance on this area.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title and description; • Tags and categories; • Who created and when; • Who last modified and when; • Who can access or update.
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: • Name, email, address, home phone number;

	• The contents of an individual student file or Human Resources file; • A staff appraisal assessment; • Details about lecture attendance or course work marks; • Notes of personal supervision, including matters of behaviour and discipline.
Processing	Means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The terms 'process' and 'processed' should be construed accordingly.
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.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.
Strictly Confidential Data	Data covered by General Data Protection Regulations under the category of sensitive personal data or special categories of personal data. If this data were to be disclosed to an unauthorised party, it could result in the loss of public confidence, non-compliance with regulatory compliance, legal liabilities and/or additional costs. Special categories under General Data Protection Regulations include child data and health data.
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 General Data Protection Regulations, 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.

4. Roles and 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 Information Governance Policy.
University Executive Team	• Implement the Information Governance Policy and advocate a General Data Protection Regulations compliant culture.
Heads of Schools & Support Functions, Directors of Research Centres	• Implementing the Information Governance Policy in their areas of responsibility. • Ensuring ongoing compliance with the General Data Protection Regulations in their respective areas of responsibility. • Ensuring information required for the record of processing activities is provided to the Data Protection Officer.
Data Owner	• Accept responsibility and are accountable for relevant sets of information/data in accordance with the principles of data ownership set out in this document. • Data owners are responsible for the stewardship of information assets.
Data Processors	• Management and staff within the University who take responsibility for processing, storing and/or archiving University data. • Data processors take responsibility to apply the relevant information handling controls required per the classification of data set out in this document.
Data Protection Officer	• 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 General Data Protection Regulations. • 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.

Data Users	• All users of the University information and data must be aware of the University classifications of data and the appropriate handling requirements of data linked to each classification. • Read and understand this policy document. • Adhere to the policy statements in this document.
Audit & Risk Committee	• To oversee all aspects of data protection and privacy obligations.

5. Policy

5.1 Data Ownership

As per ISO 27002 all information and assets associated with information processing facilities (applications) should be owned by a designated part of the organisation. Therefore, data ownership to key sets of information and data (and associated applications) must be formally assigned.

Ownership of data resides with the University and implies authority as well as responsibility and control. The control of information includes not just the ability to access, create, modify, delete, package, derive benefit from, but also the right to assign or remove these access privileges to or from others.

In the context of the University, data ownership responsibility will be formally assigned for the following functional domains/process but is not limited to these functions:

a) Human Resources;
b) Payroll processes;
c) Student Administration processes/services;
d) Information Systems;
e) Financial processes;
f) Resource planning;
g) Research.

Data ownership responsibilities include:

a) Approval of user access;
b) Approval of user roles/profiles/classes;
c) Review of access including application data held in network & cloud directory locations;
d) Data classification;
e) Data retention rules and definition;
f) Master data changes authorisation;
g) Ensuring availability of information;
h) Data restoration testing;
i) Deletion of data;
j) Service level management and monitoring.

5.2 Data Classification

All existing administrative data belongs to one of the classifications in the Data Classification Guide below and in Appendix B.

All information assets should be categorised & labelled for handling as per guidance in the Data Handling & Clean Desk Policy.

Controls must be implemented by the Data Controller according to the classification to which the data belongs. Data is classified, and may be reclassified, by the Data Owner.

Note: Categorising information does not exclude it from consideration for disclosure under Freedom of Information or Data Protection legislation.

As per ISO 27002 the purpose of information classification is to ensure that information/data receives an appropriate level of protection.

Following on from this, the University classifies its data based on the level of impact that would be caused by inappropriate access and/or data loss.

There are three classifications as follows:

1. Public data
2. Internal Use Only/ Restricted data
3. Confidential data

Classification of data is independent of its format.

The following table provides an indication of how classifications get assigned through considering the impact of various risks (Refer to Appendix B for Further Guidance):

Risk ↓	**IMPACT IS CONSIDERED FROM FOUR MAIN PERSPECTIVES - LEGAL, REPUTATIONAL, FINANCIAL, AND OPERATIONAL (REFER TO APPENDIX B FOR FURTHER GUIDANCE)**		
Inappropriate access causing breach of confidentiality/data protection rules	Minor	Moderate	Serious
Inappropriate access resulting in unauthorised amendments	Minor	Moderate	Serious
Data loss	Minor	Moderate	Serious
UNAUTHORISED DISCLOSURE	Minor	Moderate	Serious
Resulting Data Classification	**Public Data**	**Internal Use Only/ Restricted**	**Confidential Data**
DATA CLASSIFICATION EXAMPLES	• Public Websites • Campus Maps • Staff Directory	• Intranet / Extranet data • Financial Budgets	• Finance Data relating to students and personnel. • Human Resources Data. • Commercially Sensitive Data • Personal Data and Special Categories of Personal Data (General Data Protection Regulation)

Data that is not yet been classified should be considered confidential until the owner assigns the classification.

5.2.1 Public Data

Public data is information that may be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data can be made available to all members of the University community and to all individuals and entities external to the University community.

By way of illustration only, some examples of public data include:

- Publicly posted content on all external facing web sites;
- Publicly posted press release;
- Publicly posted schedules of classes;
- Publicly posed interactive University maps, newsletters, newspapers and magazines.

5.2.2 Internal Use Only Data

Internal only data is confidential information that must be protected due to proprietary, ethical, or privacy considerations, and must be protected from unauthorised access, modification, transmission, storage or other use. Internal use data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of official use data include:

- Intranet / Extranet data; and,
- Internal telephone books and directories.

Internal Use only data must be protected to prevent loss, theft, unauthorised access and/or unauthorised disclosure.

Unauthorised disclosure of this information, particularly if taken out of context, could adversely impact the University, individuals or affiliates.

Note: While some forms of Internal Use Only data can be made available to the public, it is not freely disseminated without appropriate authorisation.

5.2.3 Confidential Data

Confidential data is information or data protected by statutes, regulations, University policies or contractual obligation. Personal data is considered to be confidential or strictly confidential data. Prior to the distribution or transmission of confidential data, it is required that reference is made to relevant legislation (e.g. General Data Protection Regulation) to ensure such distribution or transmission is not in breach of same. Confidential data should only be disclosed to authorised individuals on a need-to-know basis and in accordance with the relevant legislation. By way of illustration only, some examples of confidential (C) and strictly confidential (SC) data include:

- CCTV footage; (C)
- Medical records; (SC)
- Student records and other non-public student data; (C) or (SC)
- PPS Numbers; (C)
- Personnel and payroll records; (C)
- Bank account numbers and other personal financial information. (C)

Confidential data, when stored in an electronic format, must be protected with strong passwords and stored on servers that have appropriate access control measures in order to protect against loss, theft, unauthorised access and unauthorised disclosure.

Confidential data must not be disclosed to parties without explicit management authorisation. Confidential data must only be used for the purpose for which it was originally gathered. If, for legitimate teaching, learning and/or research activities confidential data is used for a purpose other than that of which it was originally gathered the data must be anonymised.

5.2.4 Classification Record

The data inventory as per the template in Appendix A should clearly indicate the data classification assigned to individual data sets for University processes. It is the responsibility of individual data owners to input into the data inventory. It is the responsibility of the Data Protection Officer to coordinate and update this data inventory.

5.3 Retention of Data

It is the responsibility of data owners to clearly indicate the maximum period of time information/data should be retained by the University. Refer to Appendix A for the data inventory which should indicate the data retention period. This period of time needs to be agreed in the context of relevant legislation including Data Protection guidelines.

It is the responsibility of the data processor to implement the appropriate storage, archiving and purging rules to match agreed data retention period. When the retention period expires, the information shall be destroyed in such a way that the information cannot be retrieved. Particular care shall be taken where the information is categorised as restricted or highly restricted. All data being purged should be purged in a complete and secure manner. Copies of data must be included in the purging process and data deleted must be done so that it's not recoverable from any devices or media prior to disposal.

Please refer to the Data Retention Policy for more detail in relation to data retention.

6. 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 staff or other relevant third parties.

6.1 Compliance Exceptions

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

6.2 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University's disciplinary procedures unless you are granted privileges to monitor equipment, systems, or network traffic as part of your duties to ensure compliance with additional relevant University policies. 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.

7. Appendices

Appendix A – Data Inventory

Munster Technological University (MTU) Data Inventory								
Process Name	Data Set	Data Owner Name	Data Storage Location (Application /database; Network Directory location, Cloud Storage)	Data Processor Name	Data Classification: (Public Data; Sensitive Data) Confidential Data)	Data Retention Period (Months or Years)	Data Disposal technique (Purge or archive)	Data Recovery Time (How long can MTU Survive without system/data)
Finance								
Human Resources								
Student Administration								
Health and Safety								
Research								

Appendix B – Guidance on Impact Criteria

To ensure consistency across the University the following method will be used in assessing risk.

Risk Impact Criteria

Option B - Risk Impact Criteria for a 5x5 score model						
Description	**Strategic Risk**	**Reputational risk**	**Compliance Risk**	**Operational Risk**	**Financial Risk**	**Score**
Extreme	Non completion of capital project. Non-recruitment of key personnel.	Prominent coverage of Institute in national media and / or political reaction	Breach in laws and regulations e.g. resulting in material fines, penalties being levied on the Institute or funding being withheld	Serious impact on objectives e.g. closure of Institute for >2 days. Serious debilitating injury/loss of life.	>€1m or X% of Turnover	5
Major	Failure to meet quality standards	Embarrassment within a department/function leading to adverse media or a significant number of student complaints	Breach in laws and regulations e.g. resulting in substantial fines and consequences	Significant impact on objectives Short to medium damage. e.g. unavailability of a department /function for up to 2 days. Injury requiring hospitalisation.	<€500-€1m or X% of Turnover	4
Moderate	Significant delay in the delivery of new programmes. Significant delay in the completion of capital project	Reputational impact in local/specialist area covered in the media or some student complaints	Breach in laws and regulations with no fine, and no regulatory investigation	Moderate impact on objectives. Some short term damage. e.g. disruption to departments / function for a day. Injury requiring attendance at medical facility	<€100-€500k or X% of Turnover	3
Minor	Minor delay in achievement of departmental goals	Potential damage evident to those close to the event/area of interest	Breach in laws and regulations noted but no consequences identified	Minimal impact on objectives. Minor Damage e.g. non delivery of several classes during one day.	<€100k or X% of Turnover	2
Insignificant	No impact	No impact on reputation	No impact on compliance	Consequences can be absorbed under normal operating conditions	<€5k or X% of Turnover	1

Risk Likelihood Criteria

Option B - Risk likelihood criteria for a 5x5 Score Model

Assessed likelihood	Description	Score
Very Probable	Estimated >90% chance of occurence one year. Almost certain to occur.	5
Probable	Estimated 60%-89% chance of occurrence one year. Probable or likely to occur.	4
Possible	Estimated 30% - 59% chance of occurrence one year. Potential to occur.	3
Improbable	Estimated 10%-29% chance of occurrence one year. Improbable but not impossible to occur.	2
Very Improbable	Estimated <10% chance of occurrence one year. Remote chance of occurrence.	1

Risk Rating Criteria

Option B - Risk Rating Criteria for 5x5 score model

		Likelihood				
		Very Improbable (1)	*Improbable (2)*	*Possible (3)*	*Probable (4)*	*Very Probable (5)*
Impact	*Extreme (5)*	5	10	15	20	25
	Major (4)	4	8	12	16	20
	Moderate (3)	3	6	9	12	15
	Minor (2)	2	4	6	8	10
	Insignificant (1)	1	2	3	4	5

Document Control

A. Document Details

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

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	29/09/2020	Initial Draft with content taken from CIT & ITT policies.	Yes	
0.2	30/10/2020	Review of Policy Draft by DPOs.	Yes	
0.3	10/11/2020	Review and update by IT Managers.	Yes	
0.4	09/02/2021	Final review by DPOs.	Yes	

C. Relevant/Related Existing Internal/External Documents

Acceptable Usage Policy
Information Security Policy
Data Retention Policy
Third Party IT Engagement Policy
Data Protection Policy
Data Handling & Clean Desk 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