MTU

Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Data Handling and Clean Desk 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 personal information across each of its Schools, Departments and Functions. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- It is the responsibility of each School, Department and Function to ensure this personal information is processed in a manner compliant with the relevant data protection legislation and guidance.
- The University has an appointed Data Protection Officer ('DPO') who are available to Schools, Departments and Functions to provide guidance and advice pertaining to this requirement.
- All Staff must appropriately protect and handle information in accordance with the information's classification.
- Personal Data is considered Confidential Information and requires the greatest protection level.

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 security and protection of University assets, facilities and personnel are fundamental to the efficient and effective operations of the University. This policy is to establish the minimum requirements for handling data and maintaining a "Clean desk" - where sensitive/critical information about University employees, students, University intellectual property, and University vendors is handled correctly, is secure in locked areas and out of sight.

3. Scope

This policy applies to:

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

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

4. Definitions

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
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 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.
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 organise, 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 HR file; • A staff appraisal assessment; • Details about lecture attendance or course work marks; • 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.
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.
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 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 Data Handling & Clean Desk Policy.
University Executive Team	• Implement the Data Handling & Clean Desk 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. • To report directly on data protection risk and compliance to executive management.
Head of Function (Academic/Administrative/Research)	• Implementing the Data Handling & Clean Desk Policy in their areas of responsibility • Ensuring ongoing compliance with this policy in their respective areas of responsibility.
Staff/Students/External Parties	• To adhere to policy statements in this document.

	• To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.

If you have any queries on the contents of this Policy, please contact the Data Protection Officer.

6. Policy

This policy should not be viewed in isolation. Rather, it should be considered as part of the University suite of Data Protection policies and procedures (see Document Control).

6.1 Policy Requirements

Protecting the integrity of confidential data that resides within the University is critical. To comply with GDPR regulations, Heads of Schools/Departments/Function (Academic/Administrative/Research) are encouraged to strive to implement a Data Handling & Clean Desk Policy where appropriate and practicable.

The below requirements must be followed by all staff:

a) You should never leave confidential documents unattended at your desk or when working remotely.
b) You should never leave confidential documents at printers, in meeting rooms or other such public/semi-public places.
c) You should check that no sensitive documents are sitting in your mail slot/post-box waiting to be collected and not leave 'Post-it' notes on your desk. These notes often contain personal details such as telephone numbers which ought to remain confidential at all times.
d) Information stored in filing cabinets should be reviewed regularly and disposed of in line with the Data Retention Policy.
e) If you notice a colleague has left confidential documents unattended, you should put these documents in safekeeping and return to the person concerned as soon as possible.
f) Do not bring confidential documentation out of the office unless in accordance with approved business requirements or leave same unattended.
g) Always lock your computer screen if away from your desk.
h) Always lock away all data carriers, such as files, documents, USB keys, etc. when not required.
i) Always secure your paper-based files in a locked press/filing cabinet.
j) Always shred confidential documents or dispose of these in the provided confidential bins.
k) Always secure your portable IT equipment when unattended by using a cable lock, locked drawer or locking your office.
l) Users shall not leave laptops and other portable computing devices, unattended and in plain sight (for example, in public areas or conference rooms).

m) Users must log off or otherwise lock systems or initiate a password protected screensaver before leaving a workstation unattended (for example, Ctrl+Alt+Del or Windows logo key+L on Microsoft Windows systems).
n) While travelling, the University's assets shall not be left in plain sight. Car boots, hotel safes and laptop encryption must be utilised to secure assets.[1]

6.2 Data Handling

The University's documents should be managed in a systematic, structured manner, and information security requirements should be maintained throughout the document lifecycle (i.e., creation, transmission, storage, modification, retention, and destruction). The table below publishes the data management requirements for the four data classification levels with the treatment of Confidential and Strictly Confidential data largely the same. Please refer to Data Governance Policy for information on data classification.

Data Management – EXAMPLE			
Category	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Access Controls	• No restrictions	• Access limited to those with a need to know, at the discretion of the data owner or custodian • Viewing and modification restricted to authorised individuals as needed for University-related roles • Authentication and authorisation required for access	• Viewing and modification restricted to authorised individuals as needed for University-related roles • Authentication and authorisation required for access • Data Owner required to grant permission for access
Copying/ Printing (both hard and soft copy)	• No restrictions	• Data should only be printed when there is a legitimate business need • Physical copies are prohibited from being left unattended on a printer/fax machine • Physical copies are required to be labeled using 'Restricted' watermark or footer or similar	• Data should only be printed when there is a legitimate business need • Physical copies are prohibited from being left unattended on a printer/fax machine • Physical copies are required to be labeled using 'Confidential' watermark or footer or similar

[1] If you are unsure whether your laptop is encrypted or not, please contact your local IT support.

Data Management – EXAMPLE			
Category	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Storage	• Electronic copies are recommended to be stored on a secure server/location (e.g., publicly posted press release)	• Electronic data is recommended to be stored on a secure server/location • Encryption of restricted information is at discretion of the owner or custodian of the information	• Electronic data is required to be stored on a secure server/location • Physical copies are required to be stored in a locked drawer, locked room, or any other area with controlled access • Electronic data is prohibited from being stored on a workstation or mobile device, unless the device is fully encrypted • Storage of regulated confidential data must meet the applicable regulatory requirements • Electronic data is prohibited from being permanently stored on portable media devices (e.g. USB drive)
Transmission	• No restrictions	• Disclosure to parties outside the University is required to be authorised by the data owner • Encryption is required when transmitting information electronically	• Encryption is required during transmission (e.g. SSL, secure file transfer protocols, Filesender with password) when transmitting information electronically. Confidential numbers/data may be masked instead of encrypted • Disclosure to parties outside the University is required to be authorised by the data owner • Transmission via fax is required to be authorized by the data owner • Transmission of regulated confidential data must meet the applicable regulatory requirements
Modification	• Modification is restricted to authorised users with a valid business need	• Modification is restricted to authorised users with a valid business need	• Modification is restricted to authorised users with a valid business need • An audit log where relevant, and dependent on the type of data, is required to be maintained in order to track changes made to the data

Category	Data Management – EXAMPLE		
	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Destruction	• No restrictions	• Physical copies are required to be shredded • Electronic media containing restricted data is required to be wiped/erased	• Physical copies are required to be shredded • Electronic portable media containing confidential data is required to be physically destroyed so that data on the media cannot be recovered or reconstructed

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 Handling and Clean Desk Policy
Owner(s):	Vice Presidents for Finance & Administration/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	Yes	
0.2	09/02/2021	Final review by DPOs	Yes	
0.3	18/02/2021	Review by IT Managers	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 Protection Breach Response Policy
Data Protection Policy
Data Retention 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