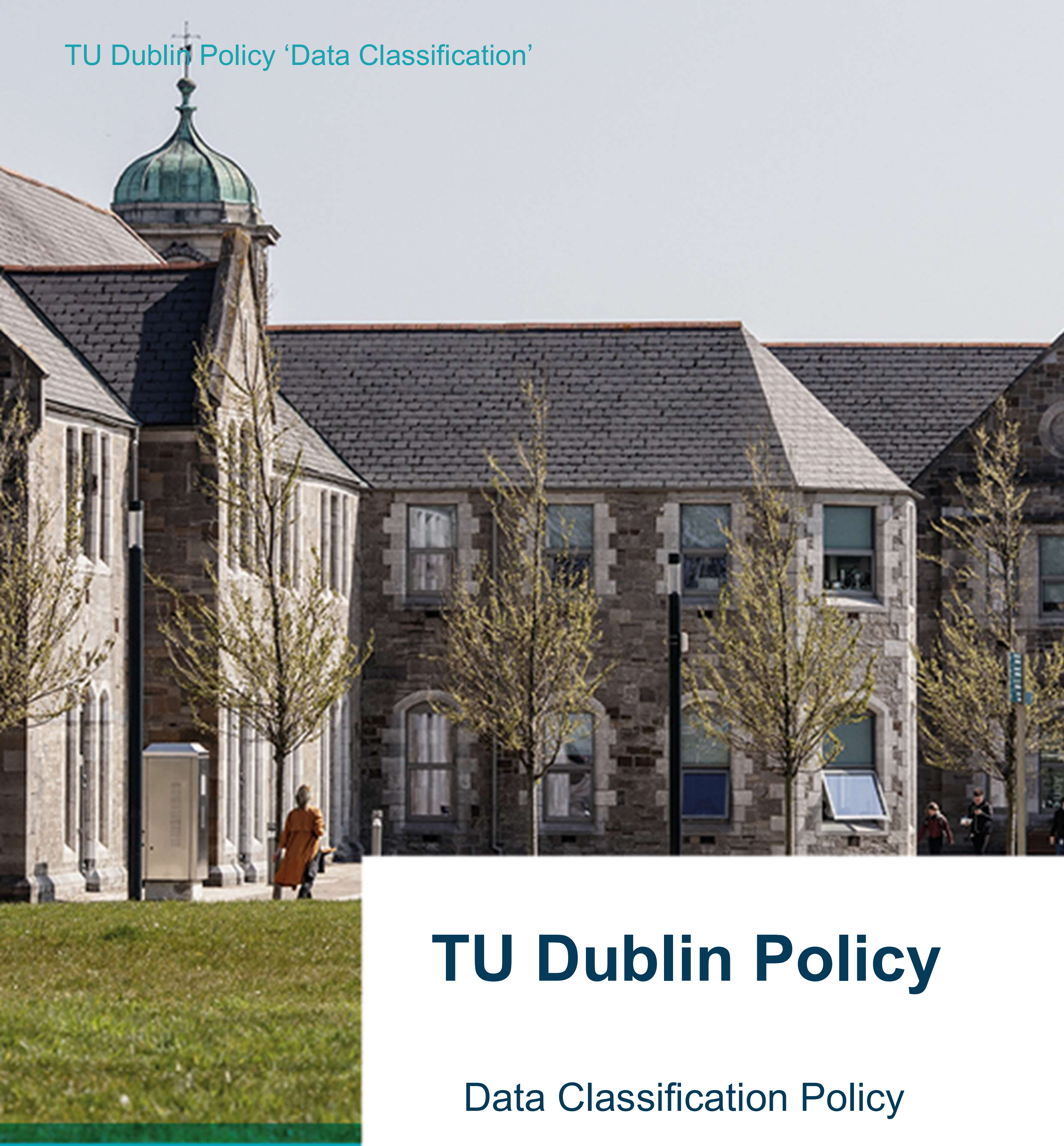

TU Dublin Policy

Data Classification Policy

Table of Contents

1. Document Control Summary

Area	Document Information
Author	Information Governance Office
Owner	Head of Governance and Compliance
UET Sponsor	*Denis Murphy, Chief Operations Officer*
Reference number	
Version	V1.1
Status	Approved
Pre-approval Body/Bodies	UET
Approved by / to be approved by	Governing Body
Approval date	30 November 2022 (electronic approval)
Next review date	August 2026
Document Classification	Public

2. Introduction / Context

The successful operation of TU Dublin involves the processing of a significant volume of information (hereafter referred to as data) across the University, both in the academic and professional services communities. As such, it is important that staff are aware of how different categories of data are to be treated. This TU Dublin Data Classification Policy provides a framework to ensure that there is a consistent approach in how authors classify data and that all staff appropriately protect and handle data in accordance with the data classification.
The introduction of the new General Data Protection Regulation (GDPR) in 2018 places additional responsibilities on data controllers.

Whilst the GDPR does not specify a requirement for data classification labels, Article 25 Data protection by design and by default, does outline the principles of Data Protection by design and by default.

As stated in the TU Dublin Data Protection Policy, the University has an obligation under GDPR to consider Data Privacy throughout all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to Personal Data. This is of particular importance when considering new processing activities or setting up new procedures or systems that involve Personal Data. GDPR imposes a ‘privacy by design’ requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

3. Purpose

This policy provides a framework for classifying and handling data to ensure that the appropriate degree of protection is applied to all data held by the University. The classification of data will help determine how the data should be accessed and handled and ensures that sensitive and confidential data remains secure.
The correct classification of data is important in order to reduce the risk of data breaches and minimising the impact of such breaches if they do occur.
The University intends to meet all relevant Data Protection, privacy and security requirements. This policy serves to assure students, staff and other stakeholders of data privacy and confidentiality. This policy should not be viewed in isolation, rather it should be considered as part of the TU Dublin suite of Data Protection policies and procedures.

4. Scope

This policy covers all data or information held, on paper or in electronic format, by the University including documents, spreadsheets and other paper and electronic data and should be applied by all staff and other members of the University as described below. Section 5 of the policy includes a definition of data.

This policy is also applicable to staff working with the University, students accessing University data as part of their programme of study, data processors, third parties and collaborators working with the University. Data Owners are responsible for assessing and classifying the data they work with and applying appropriate controls. Members of staff working with third parties or collaborators have a responsibility to bring this policy to their attention.

5. Definitions

- **Data** - This covers all data (personal and non-personal) held by the University, on paper or in electronic format, including documents, spreadsheets and other data. It includes data held on systems and databases, produced by systems and data to be uploaded to systems, as well as email content.

- **Process data** - 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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- **Public Data**- May be viewed by all members of TU Dublin and the public. Data should be classified as Public when the disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Such data is often made available to the public via the TU Dublin website. This data will not cause harm to any individual, group, or to the University if made public.

- **Internal Data** – Information that can be used and shared within TU Dublin but would not be appropriate to be known to people outside the University.

- **Confidential Data** - Accessible only to relevant members of staff of TU Dublin or designated third parties who require it to perform their duties.

- **Data Owners** - 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.

- **Personal Data -** In Article 4 (1) of GDPR personal data means any information 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;
  - Examples of personal data include, but are not limited to:
  - Name, email, address, home phone number
  - The contents of a student file or an employee HR file
  - Details about lecture attendance or course work marks
  - Notes of personal supervision, including matters of behaviour and discipline.

- **Special Category Personal Data** (or Sensitive 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; trade union membership; criminal convictions or the alleged commission of an offence.

6. Policy Details:

6.1 Policy Details

When users process data in the University it should be organised into a category of classification.

The University’s data will be classified into three categories of classification depending on their levels of risk and importance to provide a basis for understanding and managing the University’s data. The majority of data processed by the University will fall within the categories Public and Internal. The minority of data will be categorised as Confidential.

The table below details the types of data that falls within each category of classification and the data management requirements that should be maintained throughout the data lifecycle (from collection to destruction).

	Public	Internal	Confidential
Level of Access Or Guidance	May be viewed by all members of the University and the public. No access restrictions.	May be seen by all members of the University but would not normally be available to people outside the University This data could be released to the public under Freedom of Information legislation.	Accessible only to relevant members of staff or designated third parties who require it to perform their duty, due to its potential impact on the University (including financial or reputational damage). Refer to the TU Dublin Information Security Policy and Password Policy for guidelines on security of data.
Level Of Risk	Low	Medium	High
Security and Storage (refer to Information Security Policy for appropriate security measures.)	Can be stored on any device and placed on the internet. There are no restrictions on printing and copying this data, subject to copyright restrictions.	Should be stored on TU Dublin managed storage resources or intranet. Caution should be exercised if data is transferred to any non-TU Dublin ICT managed storage or devices. See TU Dublin Information Security Policy Physical copies or copies stored on portable devices should not be left unattended.	Electronic data should be stored on TU Dublin managed storage resources in locations with restricted access and appropriate security. Data should not be transferred to external storage or mobile devices but if essential then appropriate security must be used (e.g. encryption, user permissions, etc). Electronic data is prohibited from being permanently stored on a portable media device (e.g. USB drive). Data should only be printed when there is a legitimate business need and, when not being referred to, held in a locked storage location. Physical copies or copies stored on portable devices are prohibited from being left unattended. Physical copies are required to be labelled ‘Confidential’
Transmission	No restrictions	Data may be placed in shared folders and sent via approved internal communication channels (e.g. internal mail, MS Teams, VLEs).	Disclosure to parties outside the University should be sent via approved secure method (e.g. HEANet filesender) Encryption is required when transmitting information through a network (e.g. emails with attachments to third parties) Items sent via internal mail should be placed in a sealed envelope. External postage should be signed for.
Modification	Modification is restricted to authorised users with a valid business need identified by the data owner.	Modification is restricted to authorised users with a valid business need identified by the data owner.	Modification is restricted to authorised users with a valid business need identified by the data owner An audit log (e.g. version control) is required to be maintained to track changes made to the data
Destruction/Disposal	No restrictions. Recycle where possible. Dispose in line with TU	Most physical documents can be placed in paper recycling or confidential shredding as	Delete electronic data in accordance with Record

	Dublin Record Management, Retention and Destruction Policy	appropriate. Delete electronic data in accordance with record Management, Retention and Destruction Policy.	Management Retention and Destruction Policy. Shred or use confidential waste bins for paper documents.
Examples of Data	**Public** • Information contained within the FOI Publication Scheme • Information for prospective and current students • Publications – flyers, prospectus • Press releases • Published research report • Audited Financial Statements • Annual Report • Course Names • Module Names • Staff names and internal phone number extensions	**Internal** • Internal policies and procedures • Internal operating procedures • Operational manuals • Technical documents, such as system configurations • Purchase orders • Budgets (excluding individual salaries) • Annonymised Alumni data • Organisational charts with names	**Confidential** • Confidential commercial contracts • Passwords • Disciplinary proceedings • Security information • Legally privileged information • Medical records • Documents containing sensitive personal data • HR data, • Employment contracts • Appointment letters • Individual salary & benefits • Financial Aid records • Student data, including Student applications, transcripts and grades • Reserved committee business • Draft reports, papers, policies • Financial information (not disclosed in Financial Statements) • Databases and spreadsheets containing personal data • Data on research participants

7. Related Documents

This policy should not be viewed in isolation. This policy supports the following compliance and IT security policies;

1. TU Dublin Data Management, Retention and Destruction Policy
2. TU Dublin Information Security Policy

8. Conclusions

All staff working with the University, students accessing University data as part of their programme of study, data processors, third parties and collaborators working with the University e University are expected to:

- ensure they classify data based on the information provided in this policy;
- acquaint themselves with, and abide by, the rules of the full suite of compliance policies;
- read and understand all data protection documentation;
- understand what is meant by ‘personal data’ and ‘sensitive category personal data’ and know how to handle such data;
- not jeopardise individuals’ rights or risk a contravention of data protection legislation;
- contact their Head of School/Service Area or the Information Governance Office if in any doubt regarding their responsibilities under this policy.

9. Document Management

9.1 Version Control

VERSION NUMBER	VERSION DESCRIPTIN / CHANGES MADE	AUTHOR	DATE
1.0	*Initial Policy*	*Information Governance Team*	*10/01/2022*
1.1	*Review and Update*	*Information Governance Team*	*26/04/2024*

9.2 Document Approval

VERSION NUMBER	APPROVAL DATE	APPROVED BY (NAME AND ROLE)
1.0	*30/11/2022*	*Governing Body*
1.1	*June 2024*	*Update noted by UET*

9.3 Document Ownership

Document Owner – Head of Governance and Compliance
Document Update - Information Governance Senior Manager

9.4 Document Classification

Document is classified as Public and is available to all staff, students and members of the public who wish to view it.