Data Governance Policy

8 December 2022
Version 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Policy Details	
Policy Title:	Data Governance Policy
Version:	Version 1.0
Approved By:	Governing Body
Date Approved:	8.12.2022
Effective Date:	8.12.2022
Review Date:	7.12.2023
Policy Owner:	Vice Presidents of Corporate Affairs

Revision History		
Previous Version No.	Summary of Amendments	Reviewed Version No.
N/A	Initial Issue	0.1
0.1	Updates and amendments from consultation process	0.2
0.2	Final draft approved by EMT	0.3

A draft of this document was supplied to the following groups and all were requested to engage in consultation concerning the draft.

Consultation History		
Name	Date	Details of consultation
Academic union	February 2022	Comments and feedback incorporated where appropriate
PMSS	May 2022	Comments and feedback incorporated where appropriate

This policy must be available to all staff

Publication Details	
Where	**Date**
Sent by email to all staff	20.12.2022
Placed on SETU website	20.12.2022
Network Drive / Public / HR policies	

Feedback or issues arising on implementation of this policy should be communicated to the policy author.	
Policy Author	Risk & Compliance Officers and Data Protection Co-Ordinator

TABLE OF CONTENTS

1 Introduction

South East Technological University (SETU) is responsible for the processing of a significant volume of information across each of its Faculties 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 Faculty and Function to ensure this information is processed in a manner compliant with the relevant data protection legislation and guidance;
- SETU have appointed a Data Protection Officer ('DPO') who is available to provide guidance and advice pertaining to the protection of personal information;
- All staff must appropriately protect and handle information in accordance with the information's classification.

Confidential Information requires the greatest protection level (e.g. personal data).

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

SETU 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.

Therefore, all staff, faculty, students, and external parties of SETU have a responsibility to protect SETU data and information from unauthorised generation, access, modification, disclosure, transmission or destruction and are expected to be familiar with and comply with this policy.

3 Roles and Responsibilities

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

Governing Body	To review and approve the policy on a periodic basis
Executive Management Team	Executive Management Team (EMT) is responsible for the internal controls of SETU, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. EMT is responsible for: ● Reviewing and approving this policy and any updates to it as recommended by the Vice Presidents for Corporate Affairs; ● Ensuring ongoing compliance with the GDPR in their respective areas of responsibility; ● As part of the University's annual statement of internal control, signing a statement which provides assurance that their faculty/functional area is in compliance with the GDPR; ● Ensuring oversight of data protection issues either through their own work or a Data Protection Officer or other governance arrangement.
Data Protection Officer	The Data Protection Officer is available to provide support, assistance, advice and training to ensure compliance with data protection legislation. Responsibilities include: ● 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; ● Establish and maintain effective policies, standards and guidelines relevant to information retention and disposal; ● Distribute relevant documents to Faculties and Functions including policy or related standards/guidelines updates;

	• Periodically review relevant policies, procedures and related standards/guidelines for effectiveness; • Provide relevant advice and support to Faculties and Functions to assist them in achieving and retaining policy/standards compliance; • Monitor policy and procedure compliance and ensure that Faculties and Functions adhere to all data protection requirements; • 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 senior leadership team.
Staff/Students/External Parties	• To adhere to policy statements in this document; • To report suspected breaches of policy to the appropriate person which may include a Head of Faculty/Head of Department/Function and/or the Data Protection Officer.
Data Processor	The Data Processor shall be: • Contracted by the data controller to provide a service that involves the processing of personal data; • It is possible for SETU to be both a Data Controller and a Data Processor, in respect of distinct sets of personal data.
Data Controller	The Data Controller shall: • Determine the purpose(s) for which and the manner in which any Personal Data is, or is to be, processed. The Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.

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

4 Scope

This Data Governance Policy relates to all SETU data including but not limited to:

- SETU Student Data;
- SETU Staff Data;
- SETU Financial Data;
- SETU Commercial Data;
- SETU Intellectual Property;
- SETU Academic data.

SETU is committed to ensuring that all SETU data is clearly identified and an inventory of all-important data is drawn up and maintained. The data inventory includes data held on all IT resources and application types including Microsoft (MS) Excel spreadsheets, MS Access databases and other such end user applications. Please refer to the *SETU Data Inventory & Retention Schedule (link to follow)* for further information.

This policy applies to:

- Any person who is employed by SETU who receives, handles or processes data in the course of their employment;
- Any student of SETU 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 SETU.

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

5 Policy

This policy should not be viewed in isolation. Rather, it should be considered as part of the SETU suite of Data Protection policies and procedures (see Appendix A). In particular, please refer to data handling & clean desk procedures (see section 5 of the Data Protection procedures) for further information on the minimum requirements for handling data and maintaining a "clean desk."

5.1 Information Governance

5.1.1 Data Ownership

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 SETU and implies authority as well as responsibility and control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, but also the right to assign these access privileges to others.

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

- HR;
- Payroll processes;
- Student Administration Processes/services;
- Information Systems;
- Financial processes;
- Resource Planning;
- Research, Innovation & Graduate Studies.

Data ownership responsibilities include:

- Approval of user access;
- Approval of user roles/profiles/classes;
- Review of access including application data held in network directory locations;
- Data classification;
- Data retention rules and definition;
- Master data changes authorisation;
- Ensuring availability of information;
- Data restoration testing;
- Service level management and monitoring.

5.1.2 Information / Data Classification

The purpose of information classification is to ensure that information/data receives an appropriate level of protection.

Following on from this, SETU 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:

Impact Level	Types of Classification
High	Confidential data (+ Strictly Confidential Data)
Medium	Internal Use Only data
Low	Public 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:

Risk	*IMPACT IS CONSIDERED FROM FIVE MAIN PERSPECTIVES- STRATEGIC, LEGAL, REPUTATIONAL, FINANCIAL, AND OPERATIONAL*		
Inappropriate access causing breach of confidentiality/data protection rules	Serious	Moderate	Minor
Inappropriate access resulting in unauthorised amendments	Serious	Moderate	Minor
Data loss	Serious	Moderate	Minor
UNAUTHORISED DISCLOSURE	Serious	Moderate	Minor
RESULTING DATA CLASSIFICATION	*Confidential Data (+ Strictly Confidential Data)*	*Internal Use Only*	*Public Data*



DATA CLASSIFICATION EXAMPLES	• Finance Data relating to students and personnel. • HR Data. • Commercially Sensitive Data • Personal Data (under GDPR Legislation). **Strictly Confidential** • Special Categories of Personal Data (under GDPR Legislation).	• Intranet / Extranet data. • Internal telephone books and directories. • Financial Budgets.	• Public Websites. • Campus Maps. • Staff Directory

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

Confidential Data

Confidential data is information or data protected by statutes, regulations, SETU policies or contractual obligation. Personal data is considered to be **confidential or strictly confidential** data (see distinction below). Prior to the distribution or transmission of confidential data, it is required that reference is made to relevant legislation, (which at this time is the General Data Protection Legislation or GDPR) 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:

- Medical records **(SC)**;
- Student records and other non-public student data **(C)** or **(SC)** (see Special Categories of Personal Data under GDPR);
- PPS Numbers **(C)**;
- Personnel and payroll records **(C)**;
- Bank account numbers and other personal financial information **(C)**;
- Financial budgets [Commercially Sensitive – **(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.

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 SETU 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;
- Internal telephone books and directories.

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

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 SETU community and to all individuals and entities external to the SETU 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 SETU maps, newsletters, newspapers and magazines.

5.1.3 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 SETU.

Please refer to the *SETU Data Retention Policy* and *SETU Data Inventory & Retention Schedule (link to follow)* for information on retention periods.

6 Policy Compliance

6.1 Compliance

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

6.2 Compliance Exceptions

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

6.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with SETU's disciplinary procedures. Non-compliance shall be reported to the DPC and Data Protection Officer for the purposes of GDPR only and should the need to instigate the disciplinary procedures arise, it should be dealt with by the appropriate manager.

Failure of a third party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Appendix A – Supporting Documents

The below is a list of a suite of policies and procedures that may be used in conjunction with this policy.

- Data Protection Policy
- Data Protection Procedures
- Data Retention Policy
- Data Inventory & Retention Schedule

The above list is not exhaustive and other SETU policies, procedures and standards and documents may also be relevant.

Appendix B – Glossary of Terms

Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to the SETU including intellectual property.
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 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.
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 Faculty or Function within an SETU which is Processing Personal Data for the SETU 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 SETU 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 SETU 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).
Data/Record Retention Schedule	The maximum period of time information/data should be retained by the SETU 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: employees, 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.
Information	Facts, details or knowledge obtained or processed about person, product, company, etc.
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 SETU. 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.

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 organisation 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 GDPR 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 GDPR include child data and health data.
Third Party	Means an entity, whether or not affiliated with SETU, that is in a business arrangement with SETU 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 SETU 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, and shall have the same meaning as the GDPR and/or local requirements.