Data Retention Policy

8 December 2022

Version 1.0

setu.ie

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Policy Details	
Policy Title:	**Data Retention Policy**
Version:	Version 1.0
Approved By:	Governing Body
Date Approved:	08.12.2022
Effective Date:	08.12.2022
Review Date:	07.12.2023
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 & feedback incorporated where appropriate

PMSS	May 2022	Comments & 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 has an appointed Data Protection Officer ('DPO') who is available to Faculties and Functions to provide guidance and advice pertaining to this requirement.;
- All Staff and other persons charged with maintaining information on behalf of SETU must appropriately protect and handle information in accordance with the information's classification;
- Personal Data is considered confidential Information which 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 purpose of this policy is to ensure that SETU applies retention periods appropriately and retains data only for the period for which it is allowed under these retention periods. It sets out the procedures that should be in place and puts responsibility on each Faculty and Function to ensure that SETU remains compliant with this area of the regulation.

3. Scope

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.

4. 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 Data Protection Officer; ● 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 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 procedural 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 compliance to Executive Management Team where appropriate.
Data owners	● Define appropriate data management processes; ● Define appropriate retention schedules to support SETU business, regulatory or disposal requirements; ● Use and maintain appropriate and durable information retention/retrieval mechanisms to prevent damage, degradation or unauthorised alteration and ensure retrieval at any time; ● Use appropriate security measures as laid out in the SETU's Information Security policy, appropriate to the classification level of the data.
ICT Department	● Review and provide policy input and relevant related documentation e.g. IT, policies, standards & guidelines; ● Ensure that the technical aspects of the information retention and disposal requirements, as defined by the data owner are met, including monitoring of the service provided; ● Support the data owner or their representative with those aspects of the Data Inventory & Retention Schedule which relate to electronic information; ● Ensure that all copies made of information, within the scope of this policy, whether for development or test purposes, or for internal or external use, are subject to, as a minimum, the same controls as the original information; ● Manage University information, in compliance with this policy and related standards; ● Monitor the supporting processes to ensure ongoing compliance; ● Ensure that ICT staff or agents acting on their behalf are fully familiar with and trained on all of the relevant policies and procedures and that they are aware of their responsibilities; ● Provide supporting evidence of compliance on request to the data owner and DPO; ● Allow appropriate access to the data owner or their appointed representatives; ● Notify the data owner or his/her nominated representative of any non-compliance discovered.

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.

5. Policy

This policy should not be viewed in isolation. Rather, it should be considered in conjunction with the documents referred to in Appendix A.

University policy is to retain and dispose of information in compliance with legal and regulatory requirements together with this Data Retention Policy and related policies.

Data Protection legislation only applies to a living individual's personal information, e.g. student or staff information (potential, current or past). Commercial requirements may drive disposal of other information, not covered by Data Protection legislation.

Data Protection legislation is not the only body of legislation which prescribes minimum retention periods for certain types of information. Other legislation or regulations should also be considered when defining minimum retention requirements (e.g. legislation requiring retention of employee records or financial information). Faculties and Functions must confirm which retention requirement takes precedence in these instances

This policy only deals with those parts of Data Protection Legislation which relate to information retention, disposal and retrieval.

Information Retention and Disposal

Faculties, Functions and information owners must define appropriate data management processes to comply with legal and regulatory requirements, international standards and best practises.

These processes must:

- Be based on the information owner's approval of these information use processes;
- Be sufficiently flexible to cope with temporary changes to retention requirements for example if information is required for investigations or potential litigation;
- Be cognisant of other faculties / functions' dependence on any retained or disposed information;
- Use appropriate security requirements;
- Include appropriate retention mechanisms such as archiving, facilitating reasonable retrieval times in order to prevent damage, degradation and unauthorised alteration of data;
- Use and maintain appropriate and durable information retention / retrieval mechanisms to prevent damage, degradation or unauthorised alteration and ensure retrieval at any time.

Please refer to SETU Data Protection Policy for GDPR Principles.

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

Each Faculty/Function and Information Owners must manage the information, including assessment, storage, retrieval and disposal in accordance with this policy and related policies in order to ensure that the information is retained for the appropriate period of time, in a manner which befits its sensitivity and value.

Faculties and Functions shall also ensure that all retained information, within their area of responsibility is:

- Identified, recorded and assessed to ensure that it is appropriately managed throughout the retention and disposal life-cycle.
- Subject to appropriate information management procedures throughout the retention and disposal life cycle.
- Subject to periodic procedure effectiveness reviews.

SETU must also:

- Communicate all procedural changes for retention of data to relevant parties;
- Ensure that all students, staff, vendors, independent contractors, consultants and other resource users, charged with managing retained information, are familiar with and trained on all relevant procedures and aware of their responsibilities;
- Provide timely notification to students, staff, vendors, independent contractors, consultants or entities that use SETU IT resources, when information is required to be retrieved (e.g. to support investigations or litigation, to prevent data from being destroyed);
- Retrospectively assess existing information, stored prior to this policy implementation to ensure appropriate documentation, management and disposal;
- Report any inability to comply with this policy via the regular Risk Management processes.

Each Campus, Faculty and Function must complete a data inventory, documenting all information categories required for retention within its responsibility (See SETU Data Inventory Retention Schedule). In particular:

- Establish appropriate retention requirements for each category;
- Review and update this inventory regularly or post significant change introduction.

Faculties and Functions must refer all retention period inconsistencies to the DPO and/or Legal Services before any action is taken to dispose of the data. When deciding upon an acceptable retention period, the decision

should be grounded on an appropriate legal basis. Faculties and Functions should not hold data for longer than is necessary.

Faculties and Functions must contractually ensure that all contractors and external service providers manage information retention services in such a manner as to:

- Minimise risk to SETU, its employees and its (potential, past, or current) students;
- Ensure that contractors or external service providers allow reasonable audits and inspections access;
- 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;
- Ensure that SETU information and related records, on which SETU is reliant, are available and appropriately protected until the period of reliance has elapsed.

Faculties and Functions must report non-compliance instances to the:

- Data Protection Officer
- Vice Presidents/Deans/Heads of School responsible for a Faculty/Function.

6. Policy Compliance

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.

Compliance Exceptions

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

Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the 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 additional documents that may be used in conjunction with this policy.

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

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

Appendix B – Glossary of Terms

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 record. Data, therefore, includes any digital data transferred by computer or automated equipment, and any manual information (information which is not processed by computer) which is gathered by employees/those representing the University.
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 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 the 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 the University or a 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 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).
Function	Where function is mentioned it is intended to include Departments, Faculties and all other functional units in SETU including Research Centres
Information	Facts, details or knowledge obtained or processed about person, product, company, etc.
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.
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.

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 shall have the same meaning as the GDPR.