Data Protection Policy

8 December 2022

Version 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Policy Details	
Policy Title:	Data Protection 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

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

Contents

1. Introduction

South East Technological University (SETU) is responsible for the processing of a significant volume of personal information across the organisation. 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 personal information is processed in a manner compliant with data protection legislation and guidance;
- SETU has appointed a Data Protection Officer who is available to provide guidance and advice on data protection issues and concerns;
- All staff are responsible for protecting and handling personal information in accordance with the data inventory and schedule and the data retention policy.

This policy shall not give individuals additional rights greater than those which such person would be entitled to under applicable law and other binding agreements/ allowed for under the General Data Protection Regulation (GDPR) or Data Protection Act 2018.

The objective of this Data Protection Policy (Policy) is to set out the requirements of SETU relating to the protection of personal data where it acts as a data controller and / or data processor, and the measures SETU will take to protect the rights of data subjects, in line with GDPR legislation, and the Data Protection Act 2018.

Any person who is employed, is a student of SETU or any external third party is expected to:

- Acquaint themselves with, and abide by, the rules of Data Protection set out in this policy which is supported by the Data Governance Policy, the Data Retention Policy, the Data Inventory & Retention Schedule and the Data Protection Procedures document. These documents are all aligned to the Data Protection Act 1998 and the GDPR 2016;
- Understand what is meant by 'personal data' and 'sensitive personal data' and know how to handle such data; and
- Contact the appropriate person which may include a Head of Department/Function and/or the Data Protection Officer where there are data protection concerns.

Further information can be found in the *SETU's Data Protection Procedures* document which provides detailed guidance, templates and forms to enable staff to comply with GDPR.

2. Purpose

SETU is committed to complying with all applicable data protection, privacy and security laws and regulations (collectively referred to as requirements) in the locations in which it operates. In Europe, the data protection requirements have changed, with the key data protection requirement, the General Data Protection Regulation (GDPR), taking full effect on May 25, 2018.

SETU has adopted this Data Protection Policy, in addition to the Data Retention Policy, the Data Inventory and Retention Schedule and the Data Protection Procedures to create a common core set of values, principles and procedures which aim to achieve a standard set of universal compliance parameters based on GDPR.

3. Roles and Responsibilities

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

Governing Body	Responsible for reviewing and approving the policy on a periodic basis.
Executive Management Team	The Executive Management Team 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. The 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 TU's annual statement of internal control, signing a statement which provides assurance that their faculty/functional area is in compliance with GDPR; • Ensuring that their faculty/functional area is adhering to GDPR principles with regard to

	protection of personal data processing in line with the relevant policies, procedures and legislation requirements; • Ensuring oversight of data protection issues either through their own work or the 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 faculty/function 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/functions to assist them in achieving and retaining policy/standards compliance; • Monitor policy and procedural compliance and ensure that faculties/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 the Executive Management Team where appropriate.
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.
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.
Employees/Students/External 3rd 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/Department/Function and/or the Data Protection Officer.

If you have any queries on the contents of this Policy, please contact the Data Protection Officer by email dpo@SETU.ie.

4. Scope

This policy covers all processing activities involving personal data and sensitive personal data (special categories of personal data) whether in electronic or physical format.

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 that receive, handle, or process data on behalf of SETU.

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

5. Policy

It is the policy of SETU that all personal data is processed and controlled in line with the principles of GDPR and Data Protection Act 2018.

The SETU also embraces Privacy by Design and Privacy by Default principles in all its services and functions, both current and future. This ensures that the public can maintain a high level of trust in SETU's competence and confidentiality while handling data.

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

5.1 Personal Data Processing Principles

IMPORTANT NOTE: The following data protection requirements apply to all instances where personal data is stored, transmitted, processed or otherwise handled, regardless of geographic location.

SETU is required to adhere to the six principles of data protection as laid down in the GDPR, which state:

1. Personal data shall only be processed fairly, lawfully and in a transparent manner (Principles of Lawfulness, Fairness and Transparency);
2. Personal data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes (Principle of Purpose Limitation);
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Principle of Data Minimisation);
4. Personal data shall be accurate, and where necessary kept up to date (Principle of Accuracy);
5. Personal data shall not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which the Personal data are processed (Principle of Data Storage Limitation);

6. Personal data shall be processed in a secure manner, which includes having appropriate technical and organisational measures in place to:
   a. prevent and / or identify unauthorised or unlawful access to, or processing of, personal data; and
   b. prevent accidental loss or destruction of, or damage to, personal data (Principles of Integrity and Confidentiality);

SETU, whether serving as a data controller or a data processor, shall be responsible for, and be able to demonstrate compliance with, these key principles. (Principle of Accountability).

5.2 Lawfulness of Processing

GDPR requires data controllers & data processors to have one of six lawful bases on which to process personal data. These are article (6):

(a) Consent - The data subject has given clear consent to process their data;

(b) Contract – Processing the data is necessary to fulfil a contract;

(c) Legal obligation - The processing of the personal data is necessary to comply with legal requirements;

(d) Vital interests - The processing is necessary to protect a data subject's life;

(e) Public task - The processing is necessary to perform a task in interest of the public or to perform the functions of the organisation;

(f) Legitimate interests - The processing is necessary for the organisations legitimate interests or the legitimate interests of a third party.

SETU shall conduct all personal data processing in accordance with the most appropriate lawful basis above.

If consent is the basis for processing then Faculties and Functions must demonstrate that the data subject has provided appropriate consent for data processing. SETU must obtain a consent for any new processing activity outside of initial consent. It should be understood that anyone who has provided consent has the right to revoke their consent at any time and provision must be made for this as part of the consent process.

SETU will process personal data in accordance with the rights of data subjects. Moreover, the University will carry out communications with data subjects in a concise, transparent, intelligible and easily accessible form, using clear language.

SETU will only transfer personal data to another group or third parties outside of the European Economic Area (EEA) in accordance with this policy.

5.2.1 Special Categories of Personal Data Processing

SETU will not process Special Categories of Personal Data (see glossary for definition) unless;

- The data subject expressly consents and / or;
- It is necessary to carry out data controller's obligations or exercise data subject's specific rights in the field of employment and social security and social protection law and / or;
- It is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial functions.

SETU may only process such data where necessary to protect a data subject's vital interest in the event that this subject is physically or legally incapable of giving consent. For example this may apply where the data subject may require emergency medical care.

5.3 Transparency

To ensure fair and transparent processing activities, SETU is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data when directly collecting data. For a copy of a Privacy Notice Check List refer to *SETU's Data Protection Procedures* document.

These disclosures must be:

- Provided at the first contact point with the data subject or as soon as reasonably practicable;
- Provided in an easily accessible form;
- Written in clear language;
- Made in such a manner as to draw attention to the disclosure.

If consent is to be used as the most appropriate lawful basis then consent must be obtained at data collection point.

When collecting personal data Faculties and Functions and those acting on behalf of SETU will require a privacy notice to be provided at the time the personal data is collected or at the same time as consent is sought.

For further information and templates please refer to Section 4 (Data Protection Privacy Notices) of SETU's *Data Protection Procedures* document.

When SETU collects personal data from a third party (i.e. not directly from a data subject), SETU must ensure data subjects are aware of the indirect collection of data by including relevant details at the point where personal data is disclosed.

Faculties and Functions may not disclose personal data to third parties prior to informing the data subject of their rights. In addition to the above, SETU shall provide the data subject with the following information necessary to ensure fair and transparent processing of their personal data:

- The personal data collection and whether this was a public source;
- The personal data categories concerned.

The following are the only exceptions:

- If the data subject has already received the required information; or
- Notification would require disproportionate effort; or
- Where notification would be near impossible for example where systems used does not allow for this, or
- The law expressly provides for this personal data collection, processing or transfer.

5.4 Data Minimisation

Faculties and Functions should limit personal data collection to:

- What is directly relevant;
- What is necessary to accomplish a specified purpose.

Faculties and Functions should identify the minimum amount of personal data needed for a particular purpose, and then align collection volumes and associated retention to this purpose.

5.5 Data Use Limitation

Faculties and Functions must only collect personal data for specified, explicit and legitimate purposes. Faculties and Functions are prohibited from further processing unless legitimate processing conditions have been identified and documented as per Section 5.3 of this policy or if the personal data involved is appropriately anonymised and / or pseudonymised and used for statistical purposes only.

5.6 Data Accuracy

Each Faculty and Function must ensure that any collected personal data is complete and accurate and adequately protected from unauthorised access.

In addition, each Faculty and Function must maintain personal data in an accurate, complete and up-to-date form as its purpose requires.

Upon the discovery of incorrect, inaccurate, incomplete, ambiguous, misleading or outdated data each Faculty and Function must make every effort to correct without prejudice to:

- Fraud prevention based on historical record preservation;
- Legal Claim establishment, exercise or defence;
- Document Retention policy or other internal procedure.

5.7 Data Storage Limitation

Faculty and Functions must only keep personal data for the period necessary for permitted uses and as permitted under the SETU's approved *Data Retention Policy* and *Data Inventory & Retention Schedule*.

For further information and templates please refer to Section 8 (Data Storage Limitation) of SETU's *Data Protection Procedures* document.

5.8 Security of Personal Data

5.8.1 Information Security

Each Faculty and Function shall ensure personal data security through appropriate physical, technical and organisational measures. These include but are not limited to, ensuring adherence to the clean desk procedures, regular reviews of computer account and systems and room access of staff. In addition, Faculties and Functions should ensure all staff are aware of SETU's data retention periods and of other appropriate policies and procedures of data protection. Security measures should prevent:

- Alteration
- Loss
- Damage

- Unauthorised processing
- Unauthorised access

5.8.2 Unauthorised Disclosure

Those covered by the scope of this policy as set out in section 4 above, shall not disclose data subject's confidential or strictly confidential information (including personal data or special categories of personal data), unless this policy allows such disclosures.

Suspected incidents of unauthorised access to personal data should be reported to the appropriate Head of Department, and/or the Data Protection Officer (for GDPR purposes only). Incidents include disclosure, loss, destruction or alteration of confidential or strictly confidential information, regardless of whether it is in paper or electronic form.

For further information and templates please refer to Section 9 (Security of Personal Data Procedures) of SETU's *Data Protection Procedures* document.

5.9 Privacy and Data Protection by Design and by Default

SETU 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.

Privacy by Design means that any system, process or project that collects or processes personal data must build privacy into the design at the outset and throughout the entire lifecycle.

Privacy by Default states that the strictest privacy settings should apply by default to any new service or process without requiring the data subject to make any changes.

5.10 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is designed to assist the University in assessing the risks associated with data processing activities that may pose a high risk to the rights and freedoms of individuals and is a requirement of the GDPR.

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues and risks are identified, examined and assessed to enable SETU to evaluate and address the likely impacts of new initiatives and put in place appropriate measures to minimise or reduce the risks (including non-implementation).

Data Protection Impact Assessments are required under GDPR under certain circumstances including:

- when the processing of personal data may result in a high risk to the rights and freedoms of a data subject;
- processing of large amounts of personal data;
- processing of special categories of personal data;
- where there is automatic processing/profiling.

DPIAs are mandatory for any new high risk processing projects. However, a DPIA is required as a standard practice in SETU and will serve as a useful tool to help comply with data protection law. The DPIA should be carried out prior to the processing of data.

For further information and templates please refer to Section 10 (Data Protection Impact Assessments) of SETU's *Data Protection Procedures* document.

5.11 Record of Processing Activities

SETU as a data controller is required under GDPR to maintain a record of processing activities under its responsibility (GDPR Data Processing Register). The record shall contain details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU.

New activities involving the use of personal data, and which is not covered by one of the existing records of processing activities, require consultation with the Data Protection Officer prior to the commencement of the activity.

The Data Protection Officer will review records of processing periodically and will put a monitor and review process in place in line with GDPR requirements. The Data Protection Officer is responsible for providing Data Processing Registers to the Data Protection Commission on request.

For further information and templates please refer to Section 11 (Data Processing Activity Inventory Procedures) of SETU's *Data Protection Procedures* document.

5.12 Data Sharing

5.12.1 Sharing with a Third Party or External Processor

As a general rule, personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible for example:

- SETU may disclose student's personal data and sensitive personal data/special category data to external agencies to which it has obligations or a legitimate reason. Such sharing should be noted in the Privacy Notice e.g. HEA;
- The data subject consents to the sharing;
- Where data is required under a statutory instrument;
- The Third Party is operating as a Data Processor and meets the requirements of GDPR.

Where a third party is engaged for processing activities, there must be a written contract, or equivalent in place which shall clearly set out respective parties responsibilities and must ensure compliance with relevant GDPR and Data Protection Act 2018 requirements and any other applicable legislation such as sharing for the purposes of prevention/detection or investigation of a crime.

The Data Protection Officer should be consulted where a new contract that involves the sharing or processing of personal data is being considered.

Requests for personal information from third parties should be dealt with in line with Sections 12 and 13 (Third Party Procedures) of SETU's *Data Protection Procedures* document.

5.12.2 Transfer of Personal Data outside the EEA

Transfers of personal data to third countries require certain safeguards. Personal data must not be transferred to a third country unless there are adequate

safeguards in place which will protect the rights and freedoms of the data subject. It is important to note that this also covers personal data stored in the cloud as infrastructure may be in part located outside of the EU.

Faculties / Functions must not transfer personal data to a third party outside of the EEA regardless of whether the university is acting as a data controller or data processor unless certain precautions are taken. It is the responsibility of the person or persons involved in the data processing and transfer of personal data to ensure that the third party outside of the EEA conforms to the rigorous data protection principles and conditions of GDPR and is covered under the 'adequacy decisions' made by the European Commission. An 'adequacy decision' refers to a decision by the commission as to the safety of transferring data to certain countries outside of the EEA.

For further information on Transfer of Personal Data, please refer to Section 12 of SETU's *Data Protection Procedures* document.

5.13 Education and Awareness of Data Protection

SETU is committed to the provision of data protection training on a mandatory basis as well as necessary in addition to on an opt-in basis to ensure all individuals are aware of their respective obligations under data protection regulation. This is especially important for staff who handle personal data and / or sensitive personal data in the course of their everyday business.

Faculties and Functions must ensure that all staff are trained on relevant privacy, data protection and information security requirements periodically. In addition to General Data Protection Regulation training, staff may receive additional training when applicable to their duties or position. SETU will be responsible for maintaining employee training completion records in order to comply with GDPR requirements.

5.14 Data Subjects Rights

Data subjects have a number of rights under GDPR. These include:

- Data subjects will be able to request to access the data SETU holds on them through a Subject Access Rights Request (SAR) (Right of Access);
- Data subjects can request to change or correct any inaccurate data (Right to Rectification);

- Data subjects can request to delete data that SETU holds (Right to Erasure (sometimes referred to as the Right to be Forgotten));
- Data subjects have the right to object to having their data processed (Right to Restriction of Processing);
- Data subjects can request to have their data moved outside of SETU if it is in an electronic format (Right to Data Portability);
- Data subjects can object to a decision made by automated processing and request that any decision made by automated processes have some human element (Right to Object to Automated Decision Making, including Profiling).

5.15 Subject Access Request (SAR)

SETU processes certain personal data relevant to the nature of the employment of its employees, students and, where necessary, to protect its legitimate business interests. As such, SETU is the data controller for such personal data.

Data subjects have the right to access personal information held by SETU. Data subjects can request to see any information that SETU holds about them. This may include both electronic and non-electronic records (including e-mails, spreadsheets etc.) and for records held on formal files, temporary folders or in any other manner.

Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month of receiving the request (20 working days). Employees should consult the Data Protection Officer for all data requests.

Requests for personal information will normally be free of charge, however, SETU reserves the right where requests from a data subject are manifestly unfounded or excessive in nature to either:

- Charge a fee to cover the administrative costs of providing the personal data;
- Refuse to act upon the request.

SETU may also refuse to act upon a subject access request under GDPR in the following circumstances:

- Where it would breach the rights of someone else;
- Where it is the subject of an ongoing legal case;
- It would be illegal to do so;
- The identity of the requester cannot be determined;

For further information please refer to Section 14 of SETU's *Data Protection Procedures* document.

6. Data Breaches

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

SETU is committed to ensuring that a standard management approach is implemented throughout the organisation in the event of a personal information/data breach.

The following breach management plan should be adhered to in the event that a personal data breach occurs. There are a number of elements to the plan:

- 6.1 Reporting, Identification and Classification
- 6.2 Containment and Recovery
- 6.3 Risk Assessment and Investigation
- 6.4 Notification
- 6.5 Evaluation and Response

6.1 Reporting, Identification and Classification

6.1.1 Reporting

Any individual who accesses, uses or manages personal data is responsible for reporting data breach incidents to the Head of Function/Head of Faculty/Head of Department and/or Data Protection Officer as soon as it is detected. The urgency of reporting a breach, or suspected breach, to the Data Protection Officer is due to a regulatory requirement of the need to report breaches to the Data Protection Commission within 72 hours as per GDPR regulations as outlined in Section 6.4 of this policy.

Early recognition and reporting is vital to ensure the breach can be dealt with swiftly and appropriately.

A "GDPR Data Breach Report" form should be completed and a copy forwarded to the appropriate Head of Function/Head of Faculty/Head of Department and the Data Protection Officer directly (see Appendix F of Data Protection Proceduresfor a copy of the template GDPR Data Breach Reporting form). The report should

include full and accurate details of the incident, the date and time of the breach, when it was detected and by whom, the nature of the data and a detailed description of the breach.

6.1.2 Identification and Classification

GDPR identifies three categorisations of breaches:

- Confidentiality Breach – there is unauthorised or accidental disclosure of or access to personal data;
- Availability Breach – there is unauthorised or accidental loss of access to or destruction of personal data:
- Integrity Breach – there is unauthorised or accidental alteration of personal data.

A breach can fall into all or a combination of these categories depending on the circumstances.

A breach incident includes but is not restricted to the following:

- Loss or theft of confidential or sensitive personal data or the equipment used to store the data (laptop, USB key, tablet, paper record);
- Failure of equipment;
- Unauthorised use of access to or modification of personal data or IT systems;
- Attempts to gain unauthorised access to information or IT systems;
- Unauthorised disclosure of personal data (e.g. email/document sent to the incorrect recipient);
- Human Error;
- Cyber hacking attack.

6.2 Containment and Recovery

This involves limiting the scope and impact of the breach of personal data following consultation with the appropriate Head of Function/Head of Faculty/Head of Department and in conjunction with the Data Protection Officer. Where a data breach has taken place you should:

- Take the appropriate steps to minimise the effect of the breach;
- Assess the severity of the breach and identify who will lead the breach investigation;

- Establish who needs to be made aware of the breach e.g. Head of Function/Head of Faculty/Head of Department and/or Data Protection Officer;
- Determine a suitable course of action to resolve the incident.

6.3 Risk Assessment and Investigation

The appropriate Head of Function/Head of Faculty/Head of Department in conjunction with the Data Protection Officer should undertake an assessment of the risks associated with the breach which should be carried out immediately. Consideration should be given in the context of the Data Breach Notification Guidelines document and should focus on the following:

- the potential adverse consequences for individuals;
- how likely it is that adverse consequences will arise;
- how serious or substantial the consequences would be should they materialise;
- the nature, sensitivity and volume of personal data;
- the type of the breach (loss/theft) – what has happened to the data;
- the ease of identification of individuals;
- could the data be used inappropriately;
- the number of individuals involved;
- security measures in place (encryption/anonymisation);
- any other factors to be considered.

6.4 Notification

The appropriate Head of Function/Head of Faculty/Head of Department in conjunction with the Data Protection Officer will determine who needs to be notified of the breach. This may include the individuals affected by the breach, the Data Protection Commissioner's Office or other appropriate individuals/groups.

6.4.1 Notifying the Data Protection Commissioner

- The Data Protection Commissioner must be notified of a breach unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons;
- The Data Protection Commissioner must be notified without undue delay and not later than 72 hours after becoming aware of the breach;

- The initial report will include the circumstances surrounding the breach, the nature of the personal data involved, the number of individuals involved and whether the breach has been contained or is still active;
- If not included in the initial report, a follow up report should be submitted including actions taken or to be taken by SETU to contain the breach, whether it was necessary to notify individuals, and steps to be taken to prevent further breaches of this nature in the future. This report will be made by the Data Protection Officer using details contained in the GDPR Data Breach Report submitted by the relevant individual.

6.4.2 Notifying Affected Individuals

In the event of a breach, SETU has a responsibility to contact the data subjects involved where appropriate. If contacting the data subject is necessary, the Head of Function/Head of Faculty/Head of Department should make the necessary arrangements where:

- Notification will include a description of the breach, how and when it occurred and the personal data involved;
- Notification will include actions taken by SETU to mitigate the associated risks;
- Details of who to contact should they have questions or concerns;
- Include advice where appropriate that the individuals can take (e.g. password change);
- Include note that the Data Protection Commissioner has been informed.

6.5 Evaluation and Response

Subsequent to any personal data breach, a full review of the causes of the breach and the effectiveness of the response will be carried out by the appropriate Head of Function/Head of Faculty/Head of Department in conjunction with the Data Protection Officer where necessary.

Existing controls will be reviewed to determine their adequacy, and identify if further actions and/or controls are necessary to minimise the risk of similar breaches occurring.

Existing policies and procedures will be reviewed and updated as necessary.

The review will take the following into consideration:

- How personal data is stored;

- Where personal data is held;
- Where the greatest risks are;
- Security of data transmission;
- Security of data access.

7. Privileged Users

A privileged user, is a user who, by virtue of function, and/or seniority, has been allocated powers within SETU systems, which are significantly greater than those available to standard users. E.g. the IT manager, academic staff using Moodle/Blackboard who can view student activity, administrators who have full access to the Core HR system/other SETU systems and technicians who have access to activity logs.

SETU's obligations under GDPR includes proper safeguarding of personal data, to include, ensuring appropriate processes and tools are in place and are used to prevent inappropriate use of SETU computer accounts, networks, and applications.

All those mentioned in section 4 of this policy and any other persons or entities that use SETU IT resources, networks and applications during and outside of working hours must adhere to specific requirements.

In order to ensure that the access of all privileged users is managed correctly, Faculties and Functions and/or the IT Manager should:

- Ensure that SETU computer accounts with administrative privileges are only used when required to perform a specific work related task;
- Ensure that administrators only have access to end-user accounts with administrative privileges or administrative accounts with a documented and legitimate business justification;
- Ensure that an inventory of all administrative accounts and all accounts with administrative privileges is maintained and validated at regular intervals to ensure that each person with access to administrative privileges is authorised with a current and legitimate business justification. Evidence of each user validation review and justification for access must be maintained;
- Ensure that administrators are required to access all system and hosts using a fully logged and non-administrative end-user account and transition

to an administrative privilege account when required to carry out administrative tasks or duties requiring elevated access;

- Ensure that third party administrators are required to use a dedicated and hardened connection gateway server and/or dedicated machine for all administrative connections to the in-scope systems, hosts and network devices in order to perform administrative tasks or tasks requiring elevated access;

- Ensure sensitive privileged user activity is subject to audit logging and monitoring.

8. Policy 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 additional documents that may be used in conjunction with this policy.

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

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

Appendix B Glossary of Terms

Administrative privileges	Having administrator privileges (sometimes called admin rights) means a user has privileges to perform most, if not all, functions within a system, computer, operating system, or database. For example, these privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords. Note: A single computer can have more than one administrative account.
Anonymised	Means the process of making personal data anonymous data.
Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to SETU including intellectual property.
Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them. It must be demonstrated that the data subject has provided appropriate consent for data processing. SETU must obtain a consent for any new processing activity outside of initial consent.
Damage	This is where personal data has been altered, corrupted, or is no longer complete.
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 SETU.
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 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 Ownership	A process whereby information/data is assigned an appropriate owner by SETU 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 SETU which is processing personal data for 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 SETU or one 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).
Data Protection Commissioner	Means the office of the Data Protection Commissioner (DPC) in Ireland.
Data Retention	The maximum period of time information/data should be retained by SETU for legal and business purposes. It is the responsibility of the specific faculty/function/area to adhere to SETU's retention period and the eventual destruction 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, suppliers.
Destruction	This is where the data no longer exists, or no longer exists in a form that is of any use to the controller.
EEA	European Economic Area Means the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, as well as the freedom to choose residence in any country within this area. The countries included are Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom, Iceland, Liechtenstein & Norway
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.
Function	Where function is mentioned it is intended to include Departments, Schools and all other functional units in SETU including Research Centres
GDPR	Means EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the processing of personal data and on the free movement of such data which was adopted into Irish law in May 2018

Loss	This should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.
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 behavior and discipline.
Personal Data Breach	GDPR defines a "personal data breach" in Article 4(12) as: "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."
Privacy by Design & Default	Integrating data protection and privacy principles into processes from the very beginning of a project where personal data is being processed right through to the end.
Privileged User	A privileged user, is a user who, by virtue of function, and/or seniority, has been allocated powers within SETU systems, which are significantly greater than those available to standard users. E.g. the IT manager, academic staff using Moodle who can view student activity, administrators who have full access to the Core HR system and technicians who have access to activity logs.

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.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Records	ISO 15489 defines records as "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 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.
Systems	Means all systems and equipment (including server, desktop, laptop, network switch, network router/gateway, printer, backup device, etc.)
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.
Unauthorised or unlawful processing	This may include disclosure of personal data to (or access by) recipients who are not authorised or do not have a lawful basis to have access to the 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.