Data Protection Procedures

Version 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Procedure Details	
Procedure Title:	**Data Protection Procedures**
Version:	1
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	1.0

Table of Contents

1. Overview

South East Technological University (SETU) has developed these Data Protection Procedures, which creates a common core set of values, principles and procedures intended to achieve a standard of compliance with GDPR rules and regulations.

These procedures should not be viewed in isolation. Rather, they should be considered in support of those mentioned in Appendix A by staff, students or third party companies (data processors) that receive, handle, or process personal data on behalf of SETU regardless of whether located in SETU, travelling or working remotely.

These procedures have been agreed through a collaborative process at sectoral level and are designed to provide guidelines to best practice in Data Protection. SETU encourages staff to raise questions about data protection matters.

2. Roles and Responsibilities

The following outlines some of the roles and responsibilities:

Governing Body	Responsible for reviewing and approving policies on a periodic basis.
Executive Management Team	The Executive Management Team is responsible for the internal controls of the 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 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.
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/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/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 EMT where appropriate.
Staff/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 Department/Function and/or the Data Protection Officer.

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

3. Scope

This procedure 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. Data Protection Privacy Notice Procedures

Faculties and Functions must provide the following to Data Subjects when collecting personal data at the point of collection or alternatively as soon as is practical:

- Data Controller's name and business address.
- Information processing legal basis.
- What information is being collected?
- Why it is being collected?
- Who is collecting it? (specific group/department)
- How is it collected? (via online questionnaire, application form etc.)
- How will it be used? (used to inform a project, used to offer a place, used to check viability of a programme etc.)
- Who will it be shared with? (consider internal & external 3rd parties)
- Whether SETUwill or could transfer Personal Data outside of the European Economic Area and if the EU Commission has not determined if the recipient jurisdiction/country has adequate Data Protection laws in place (see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en for information on this).
- The information transfer terms i.e. pursuant to a contract including EU Commission's Model Standard Contractual Clauses, or other legally approved mechanism.
- How will it be stored? (secure, password protected database, on cloud based platform etc. if this is the case include a link to the platforms privacy notice)
- How long will it be stored for? (retention policy guidelines)
- How will it be destroyed? (securely deleted, shredded etc.)
- Notice of the Data Subject's various GDPR rights including access rights, rectification, erasure, correction, restriction on processing, objection and portability of Personal Data held about them, and the means of exercising those rights (for example, who to contact).
- Notice of the Data Subject's right to lodge a complaint with the supervisory authority and SETU's lead supervisory authority details.

- Details of SETU's legal/contractual obligation to collect the data where required.
- Notice of whether the data subject is obliged to provide the Personal Data and the consequences of not providing the Personal Data.
- If Processing involves automatic decision making or profiling than the notice should provide meaningful information about the automatic decision making logic and consequences of the Processing for the Data Subject.
- Any other information to guarantee "fair processing", as deemed necessary by the Faculty or Function. For example, SETU should disclose where it may use the Personal Data in a manner not apparent to the Data Subject.

If the Faculty or Function intends to process Personal Data for an additional process outside of original consent then the Function must get the Data Subject's additional consent.

Wherever possible, these disclosures should be given at the first point of contact with the Data Subject or, if it is not possible on collection or as soon as reasonably practicable thereafter. In the case of employees, the disclosures should be made in the employment contract. Appropriate disclosures should also be made in any job application form, employee handbook or other internal employment document. The disclosures should be made in a manner calculated to draw attention to them.

Please refer to Appendix B for the Privacy Notice Requirements Checklist.

5. Data Access Management Procedures

5.1 Overview

The purpose of this specific procedure is to ensure there is a process in place to actively manage the life cycle of system and application accounts – their creation, use, dormancy, and deletion -- in order to minimize opportunities for attackers to control them. Additionally, it is to ensure there is a process and tools in place to track/control/prevent/correct secure access to critical assets (e.g., information, resources, and systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

5.2 Requirements for the Management of Access

- Establish and enforce a process to ensure that access to SETU systems and staff accounts (including Administrator end-users) is restricted to ensure that only specific access rights are assigned commensurate with their role and justification.

• Ensure appropriate configuration of access for all user accounts to SETU systems through a centralised point of authentication.

• Ensure appropriate configuration of network and security devices for centralised authentication.

• Ensure that access rights given to users has a documented and valid business justification approved by Head of Function / Head of Department.

• Establish a process to ensure that all access rights held by users are reviewed on a regular basis and any unauthorised access or access rights granted without a valid business justification is corrected immediately. Access must be reviewed immediately in response to new and evolving threats, capabilities, vulnerabilities, customer requirements or experience of security incidents.

• Establish a process to ensure that all user accounts and/or two-factor authentication tokens held by terminated staff are suspended, deleted and removed immediately. Any re-joining staff must reapply for access rights to the necessary SETU systems.

• Establish a process to ensure that access for users whose role has changed is modified in line with the appropriate access rights of their new role/duties.

• Ensure that all users use their specific login details when accessing any SETU system.

5.3 Technical Measures for the Management of Access

- Ensure that all information stored on SETU systems is protected with file system, network share, application, or database specific access control lists and no sensitive personal data is available to unauthorised users.

- Ensure that archived data (which is not backup data) that is no longer required is removed from SETU systems when there is no longer a valid business justification to retain it. This includes, copies of business data, logs data, configurations, software, system and host device images.

6. Data Handling & Clean Desk Procedures

Protecting the integrity of confidential data that resides within SETU is critical. This procedure is needed to establish the minimum requirements for handling data and maintaining a "Clean desk". To comply with GDPR regulations, Faculties and Functions should follow this procedure when processing personal data to ensure it is handled correctly.

The following should be adhered to:

a) Personal, Sensitive & Confidential Data, when stored in an electronic format, must be protected with strong passwords.

b) You should never leave confidential documents unattended and unsecured at your desk or when working remotely.
c) You should never leave documents containing personal data at printers, in meeting rooms or other such public/semi-public places unattended.
d) You should check your mail slot regularly to ensure that documents are collected in case such documents contain personal and/or sensitive confidential data.
e) You should not leave 'Post-it' notes on your desk. These notes often contain personal data such as telephone numbers which should be secured.
f) Information stored in filing cabinets should be reviewed regularly and disposed of in line with the Data Retention Policy and Data Inventory and Retention Schedule.
g) If you notice a colleague has left confidential documents unattended, you should put these documents in safekeeping and return to the person concerned as soon as possible.
h) Do not bring confidential documentation which contains personal data out of the office unless there is a definite need/reason to do so. In addition do not leave them unattended.
i) Always lock your computer screen if away from your desk.
j) Always lock away all data carriers, such as files, documents, USB keys, etc. when not required.
k) Always secure your paper based files appropriately in a secure location e.g. locked press, drawer or appropriate alternative.
l) Always shred/dispose of confidential documents in confidential bins or by shredding.
m) Always store your IT equipment when leaving it unattended e.g. locked press, drawer or appropriate alternative.
n) Where there are shared facilities e.g. shared office space, the personal information should be stored appropriately either in a drawer or simply a note pad closed on a desk for example. In the case of a shared computer, ensure that the computer is locked when away from the desk and/or logged off if someone else is using the same computer also.
o) Users shall not leave laptops and other portable computing devices, unattended and in plain sight when logged into SETU systems. (for example, in public areas or conference rooms). Users are responsible for all activities carried out under their specific user ID
p) Users must log off or otherwise lock systems or initiate a password protected screensaver (e.g. Ctrl+Alt+Del or Windows logo key+L on Microsoft Windows systems).
q) While travelling, portable devices and paper based files containing confidential information should not be left in plain sight. The appropriate security measures should be utilised for example storage in car boots and hotel safes where appropriate.

7. Data Handling

SETU documents should be managed in a systematic, structured manner, and information security requirements should be maintained throughout the document lifecycle (i.e., creation, transmission, storage, modification, retention and destruction).

The table below publishes the data management requirements for the four data classification levels with the treatment of Confidential and Strictly Confidential data largely the same. Please refer to Data Governance Policy for information on data classification.

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

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

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

8. Data Storage Limitation Procedures

Faculties and Functions must only keep Personal Data for the period necessary and for permitted uses as per the Data Retention Policy and Data Inventory & Retention Schedule.

Faculties and Functions should delete/purge or otherwise erase any Personal Data that violates:

- Data Protection Legislation
- Contractual Obligations
- Requirements of Data Protection policies and procedures
- If the SETU no longer requires the Data
- If the Personal Data no longer benefits the Data Subject in the relevant process

Faculty and Functions should Anonymise and / or Pseudonymise Personal Data rather than erase if:

• The law prohibits erasure;
• Erasure would impair the legitimate interests of the Data Subject;
• Erasure is not possible without disproportionate effort due to the specific type of storage; or
• Where the Data Subject has disputed the accuracy of the Personal Data, the SETU disagrees with that assertion and resolution has not been reached.

9. Security of Personal Data

When implementing Personal Data security measures each Faculty / Function must consider:

- Technological developments
- Implementation costs
- Nature of relevant personal data
- Inherent risks posed by human action/physical/natural environment

10. Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is designed to assist SETU 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 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. Refer to Appendix D for a copy of the DPIA template which is also available to download www.setu.ie. Faculties / Functions may consult with the Data Protection Officer where appropriate.

11. Data Processing Activity Procedures

SETU is committed to ensuring that all SETU data and processing activities are clearly identified, as required under Article (30) of GDPR. Each function is responsible for the creation and maintenance of an inventory of important data in the form of a Data Processing Register. The register should include details of manual data and data held on SETU systems and databases.

11.1 When Operating as a Data Controller

When operating as a Data Controller, each Faculty and Function must maintain a written record of processing activities in the form of a Data Processing Register (Appendix C provides a template for the GDPR Data Processing Register), to include:

- Data Controller name and contact details (and joint controller if applicable), the Data Controller's representative
  - The Processing purposes
  - Data Subjects category descriptionPersonal Data category description
  - Personal Data disclosure recipient categories
  - If outside the European Economic Area, the recipient identification, country and Personal Data protection relevant transfer mechanisms and safeguards

- Personal Data erasure time limits by category
- Personal Data safeguarding technical and organisational security measures

11.2 When Operating as a Data Processor

When operating as a Data Processor, each Faculty and Function must maintain a Processing activity written record when carried out on a Data Controllers behalf for the Processing relationship lifetime. That record must mirror the above but include details of the Data Controller(s) which the Function is processing personal data for. Appendix C provides a template for the GDPR Data Processing Register.

11.3 Data Processing Activity Maintenance

Faculties and Functions must maintain all completed processing activity records on a secure system and provide a copy of the master document to the Data Protection Coordinator. The Data Protection Officer will review records of processing periodically and will implement an appropriate monitor and review process in line with GDPR requirements. The Data Protection Officer is responsible for providing Data Protection Registers to the Data Protection Commission on request.

12. Third Party Transfer Procedures

Faculties and Functions must not transfer Personal Data to a Third Party outside of the EEA regardless of whether SETU is acting as a Data Controller or Data Processor unless certain precautions are taken or the original Personal Data consent explicitly allows Third Party transfer or transfer is authorised by law. All reasonable, appropriate and necessary steps should be taken to maintain the required level of Personal Data Protection. 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. Adequacy decisions may be updated from time to time and should be checked in all cases.
The most recent Commission 'adequacy decisions' are as follows:
Approved transfer of data to Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.
Additionally, the Commission made decisions about other countries with some restrictions as follows:

1. The transfer of personal data to Japan only covers private sector organisations.
2. The transfer of personal data to only cover data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA. For further details for sharing data with Canada visit https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents

3. For details on transferring data to the UK & US please go to https://edpb.europa.eu/edpb_en

The EU recognises the transfer country/territory as having an adequate level of Data Subject legal protection relating to Personal Data Processing or

• The EU recognises the transfer mechanism as providing adequate protection when made to countries/territories lacking adequate legal protection.

• The original Personal Data consent explicitly allows Third Party transfer or transfer is authorised by law.

• All reasonable, appropriate and necessary steps have been taken to maintain the required level of Personal Data Protection; and

Subject to the provisions above, including any necessary SETU approvals, Faculties and Functions may transfer Personal Data to a Third Party outside of the EEA where any of the following apply:

• The Data Subject has given explicit Consent to the proposed transfer; or

• The transfer is necessary for the performance of a contract between the Data Subject and the SETU or the implementation of pre-contractual measures taken in response to a request by a Data Subject; or

• The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between SETU and a Third Party; or

• The transfer is necessary or legally required for the establishment, exercise, or defence of legal claims; or

• The transfer is required by law; or

• The transfer is necessary to protect the Data Subject's vital interests; or
• The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

13.Third Party Relationships Procedures

Where a Faculty or Function engages a Third Party for processing activities including the use of cloud services, this Data Processor must protect personal data through sufficient technical and organisational security measures and take all reasonable compliance steps.

When engaging a Third Party for personal data processing, Functions must enter into a written contract, or equivalent. This contract or equivalent:

- Shall clearly set out respective parties responsibilities
- Must ensure compliance with the GDPR and Data Protection Act 2018 requirements.

14.Subject Access Request (SAR) Procedures

Employees and students of SETU are entitled to a copy of personal data SETU holds about them. If the data subject requires this information they should make a Subject Access Request (SAR) through the Data Protection Office of SETU. External requests for personal data should also be directed to the Data Protection Office for response.
All subject access requests must be made via the Subject Access Request (SAR) form (see Appendix E.) that is available on SETU website.

The Data Protection Officer upon receipt of the request shall in the following order:

1. Contact the data subject or their representatives confirming receipt of the request along with the date the request was received. In addition, if there is any doubt regarding the identity of the requestor, the Data Protection Officer may request a valid photo ID as additional proof of identity.
2. Determine if the request should be refused under GDPR. If the request is to be refused then the Data Protection Officer shall contact the data subject to inform them of this and shall set the status of the request as closed providing details of the case closure.
3. Determine the effort involved in satisfying the request. If the Data Protection Officer determines that the effort involved means:
    a) The request cannot be satisfied within the 1 month GDPR timeline but can be satisfied with an extension then the Data Protection Officer shall contact the requester and inform them of the need for an extension as well as the reason why an extension is required, and also an approximation of when the request requirements will be met. This contact shall be documented.
    b) There is a requirement for the charging of a fee then the Data Protection Officer shall contact the requester and inform them of this need. The requester must then decide whether they are proceeding with the request or whether they wish to terminate the request. This contact shall be documented and depending on the decision of the requester shall either close the request or continue to fulfil the request.
4. The Data Protection Officer shall proceed to fulfilling the request. Once the request is completed then the Data Protection Officer shall contact the requester providing the relevant documents pertaining to the request.
5. The Data Protection Officer shall verify the identity of the requester by their employee ID card/student ID card (if internal requestor) or official ID documentation (e.g. passport, driver's license) (if external requestor) before the transfer of data is complete.
6. The Data Protection Officer shall close the open request.

15.Procedure Compliance

Breaches of these procedures 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. Any exception to the procedures outlined above shall be reported to the Data Protection Officer.

Failure of a third party contractor (or subcontractors) to comply with these procedures 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 document.

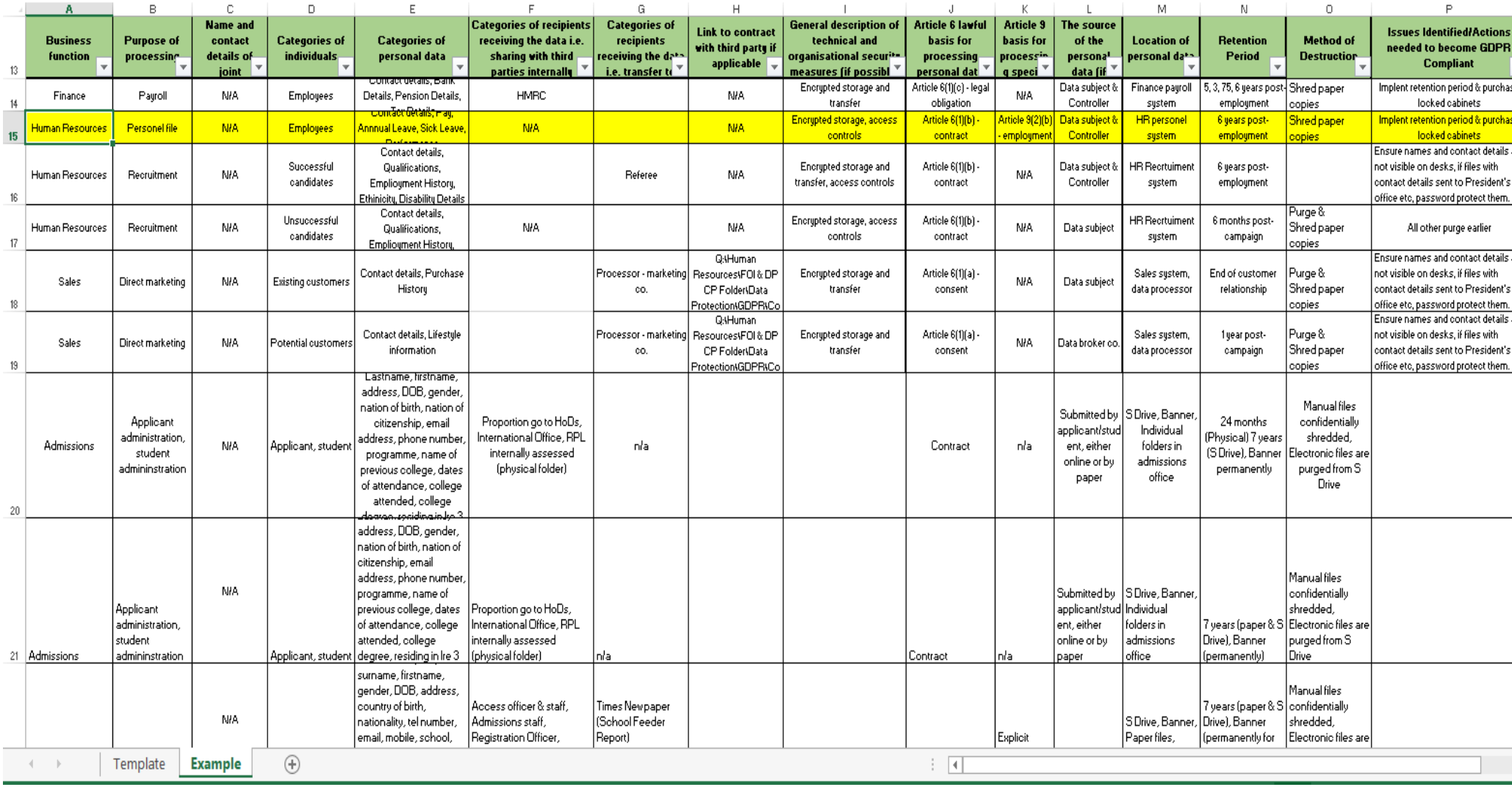
- Data Protection Policy
- Data Inventory and Retention Schedule
- Data Retention Policy
- Data Governance Policy

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

Appendix B – Privacy Notice Requirements

Data Controller's name and business address.	
What information is being collected?	
Why it is being collected?	
Who is collecting it? (specific group/department)	
How is it collected? (via online questionnaire, application form etc.)	
How will it be used? (used to inform a project, used to offer a place, used to check viability of a programme etc.)	
Who will it be shared with? (consider internal & external 3rd parties)	
Whether SETUwill or could transfer Personal Data outside of the European Economic Area and if the EU Commission has not determined if the recipient jurisdiction/country has adequate Data Protection laws in place (see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en for information on this).	
How will it be stored? (secure, password protected database, on cloud based platform etc. if this is the case include a link to the platforms privacy notice)	
How long will it be stored for? (retention policy guidelines)	
How will it be destroyed? (securely deleted, shredded etc.)	
Notice of the Data Subject's various GDPR rights including access rights, rectification, erasure, correction, restriction on processing, objection and portability of Personal Data held about them, and the means of exercising those rights (for example, who to contact).	
Notice of the Data Subject's right to lodge a complaint with the supervisory authority and SETU's lead supervisory authority details.	
Details of SETU's legal/contractual obligation to collect the data where required.	
Notice of whether the data subject is obliged to provide the Personal Data and the consequences of not providing the Personal Data.	
If Processing involves automatic decision making or profiling, the notice should explain the automatic decision making logic and consequences of the Processing	
Any other information to guarantee "fair processing", as deemed necessary by the Function. For example, SETUshould disclose where it may use the Personal Data in a manner not apparent to the Data Subject.	

Appendix C – Record of Processing Activities (ROPA)Template



Business function	Purpose of processing	Name and contact details of joint	Categories of individuals	Categories of personal data	Categories of recipients receiving the data i.e. sharing with third parties internally	Categories of recipients receiving the data i.e. transfer to	Link to contract with third party if applicable	General description of technical and organisational security measures (if possible)	Article 6 lawful basis for processing personal data	Article 9 basis for processing special	The source of the personal data (if	Location of personal data	Retention Period	Method of Destruction	Issues Identified/Actions needed to become GDPR Compliant
Finance	Payroll	N/A	Employees	Contact details, Bank Details, Pension Details,	HMRC		N/A	Encrypted storage and transfer	Article 6(1)(c) - legal obligation	N/A	Data subject & Controller	Finance payroll system	5, 3, 75, 6 years post-employment	Shred paper copies	Implent retention period & purchas locked cabinets
Human Resources	Personel file	N/A	Employees	Contact details, Pay, Annnual Leave, Sick Leave,	N/A		N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	Article 9(2)(b) - employment	Data subject & Controller	HR personel system	6 years post-employment	Shred paper copies	Implent retention period & purchas locked cabinets
Human Resources	Recruitment	N/A	Successful candidates	Contact details, Qualifications, Employment History, Ethinicity, Disability Details		Referee	N/A	Encrypted storage and transfer, access controls	Article 6(1)(b) - contract	N/A	Data subject & Controller	HR Recrtuiment system	6 years post-employment		Ensure names and contact details not visible on desks, if files with contact details sent to President's office etc, password protect them.
Human Resources	Recruitment	N/A	Unsuccessful candidates	Contact details, Qualifications, Employment History,	N/A		N/A	Encrypted storage, access controls	Article 6(1)(b) - contract	N/A	Data subject	HR Recrtuiment system	6 months post-campaign	Purge & Shred paper copies	All other purge earlier
Sales	Direct marketing	N/A	Existing customers	Contact details, Purchase History		Processor - marketing co.	Q:\Human Resources\FOI & DP CP Folder\Data Protection\GDPR\Co	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	Data subject	Sales system, data processor	End of customer relationship	Purge & Shred paper copies	Ensure names and contact details not visible on desks, if files with contact details sent to President's office etc, password protect them.
Sales	Direct marketing	N/A	Potential customers	Contact details, Lifestyle information		Processor - marketing co.	Q:\Human Resources\FOI & DP CP Folder\Data Protection\GDPR\Co	Encrypted storage and transfer	Article 6(1)(a) - consent	N/A	Data broker co.	Sales system, data processor	1 year post-campaign	Purge & Shred paper copies	Ensure names and contact details not visible on desks, if files with contact details sent to President's office etc, password protect them.
Admissions	Applicant administration, student admininstration	N/A	Applicant, student	Lastname, firstname, address, DOB, gender, nation of birth, nation of citizenship, email address, phone number, programme, name of previous college, dates of attendance, college attended, college degree, residing in Ire 3	Proportion go to HoDs, International Office, RPL internally assessed (physical folder)	n/a			Contract	n/a	Submitted by applicant/student, either online or by paper	S Drive, Banner, Individual folders in admissions office	24 months (Physical) 7 years (S Drive), Banner permanently	Manual files confidentially shredded, Electronic files are purged from S Drive	
Admissions	Applicant administration, student admininstration	N/A	Applicant, student	address, DOB, gender, nation of birth, nation of citizenship, email address, phone number, programme, name of previous college, dates of attendance, college attended, college degree, residing in Ire 3	Proportion go to HoDs, International Office, RPL internally assessed (physical folder)	n/a			Contract	n/a	Submitted by applicant/student, either online or by paper	S Drive, Banner, Individual folders in admissions office	7 years (paper & S Drive), Banner (permanently)	Manual files confidentially shredded, Electronic files are purged from S Drive	
		N/A		surname, firstname, gender, DOB, address, country of birth, nationality, tel number, email, mobile, school,	Access officer & staff, Admissions staff, Registration Officer,	Times Newspaper (School Feeder Report)				Explicit		S Drive, Banner, Paper files,	7 years (paper & S Drive), Banner (permanently for	Manual files confidentially shredded, Electronic files are	

Template | Example

Data Protection Impact Assessment Template

Background:
Data Protection Impact Assessments ('DPIAs') can be used to identify and mitigate against any data protection related risks arising from a new project, which may affect SETU. DPIAs are mandatory for any new high risk processing projects.

When to use a DPIA:
Under the GDPR, a DPIA is mandatory where data processing "is likely to result in a high risk to the rights and freedoms of natural persons/data subjects (the person to which the data relates). However, carrying out 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 and a copy sent to the Data Protection Officer to retain on file.

Who must carry out the DPIA:
It is the responsibility of the project team to ensure that a DPIA is carried out for any new high risk data processing projects.

DPIA Process:

1. **Need for DPIA:**
   Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties. You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a DPIA was identified
2. **Describe the information flows:**
   Describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

3. **Identify data protection and related risks**
   Identify the key privacy risks and the associated compliance and corporate risks.

4. **Identifying data protection solutions to reduce or eliminate the risks**
   Describe the actions you could take to reduce the risks, and any future steps which would be necessary.
5. **Signing off on the outcomes of the DPIA**
   Ensure appropriate sign off of outcomes is formally documented and retained.

6. **Integrating data protection solutions into the project**
   Ensure the controls and actions identified are tracked through to completion to ensure the rights of the data subject are upheld.

Template

1. Need for a DPIA Please answer the below questions	
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Are you using information about individuals for a purpose it is not currently used or in a way it is not currently used?	
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
Will the project require you to contact individuals in ways that they may find intrusive?	

2. Describe the information flows	
Date of Assessment:	
Assessment performed by:	
Function/Department:	

Process Name:	
Description of the envisaged processing operations: (Including collection, deletion and use)	
Purposes of the processing:	
Legal basis for processing:	
Necessity of the processing (Justification)	
Proportionality of the processing (Estimated number of Data Subjects Affected)	
Individuals consulted during the performance of DPIA (Include internal and external consultations held)	

3. Identify data protection and related risks			**4. Identifying data protection solutions to reduce or eliminate the risks**				
No.	Privacy Issue	Risk	Existing Controls Identified	Risk Rating L x I	Additional Controls/ Actions Required	Action Owner	Deadline Date
1							

5. Signing off on the outcomes of the DPIA	
DPIA Assessment result: (Pass- risk eliminated, avoided or accepted; Fail- risk unavoided)	
Approved by:	
6. Integrating data protection solutions into the project	
Next steps/Actions	

Guidance

Example Risks to Individuals:

- Inappropriate disclosure of personal data internally due to a lack of appropriate controls being in place.
- Accidental loss of electronic equipment may lead to risk of disclosure of personal information to third parties.
- Breach of data held electronically by “hackers”.
- Vulnerable individuals or individuals about whom sensitive data is kept might be affected to a very high degree by inappropriate disclosure of personal data.
- Information released in anonymised form might lead to disclosure of personal data if anonymisation techniques chosen turn out not to be effective.
- Personal data being used in a manner not anticipated by data subjects due to an evolution in the nature of the project.
- Personal data being used for purposes not expected by data subjects due to failure to explain effectively how their data would be used.
- Personal data being used for automated decision making may be seen as excessively intrusive.
- Merging of datasets may result in a data controller having far more information about individuals than anticipated by the individuals.
- Merging of datasets may inadvertently allow individuals to be identified from anonymised data.
- Use of technology capable of making visual or audio recordings may be unacceptably intrusive.
- Collection of data containing identifiers may prevent users from using a service anonymously.
- Data may be kept longer than required in the absence of appropriate policies.
- Data unnecessary for the project may be collected if appropriate policies not in place, leading to unnecessary risks.
- Data may be transferred to countries with inadequate data protection regimes.

Corporate Risks:

- Failure to comply with the GDPR may result in investigation, administrative fines, prosecution, or other sanctions. Failure to adequately conduct a DPIA where appropriate can itself be a breach of the GDPR.
- Data breaches or failure to live up to customer expectations regarding privacy and personal data are likely to cause reputational risk.
- Public distrust of organisation’s use of personal information may lead to a reluctance on the part of individuals to deal with the organisation.
- Problems with project design identified late in the design process, or after completion, may be expensive and cumbersome to fix.
- Failure to manage how your company keeps and uses information can lead to inefficient duplication, or the expensive collection and storage of unnecessary information. Unnecessary processing and retention of information can also leave you at risk of non-compliance with the GDPR.

- Any harm caused to individuals by reason of mishandling of personal data may lead to claims for compensation against the organisation. Under the GDPR the organisation may also be liable for non-material damage.

Compliance Risks:

The organisation may face risks of prosecution, significant financial penalties, or reputational damage if it fails to comply with the GDPR. Individuals affected by a breach of the GDPR can seek compensation for both material and non-material damage.

Failure to carry out a DPIA where appropriate is itself a breach of the legislation, as well as a lost opportunity to identify and mitigate against the future compliance risks a new project may bring.

Examples of data protection solutions:

- Deciding not to collect or store particular types of information.
- Putting in place strict retention periods, designed to minimise the length of time that personal data is retained.
- Reviewing physical and/or IT security in your organisation or for a particular project team and making appropriate improvements where necessary.
- Conducting general or project-specific training to ensure that personal data is handled securely.
- Creating protocols for information handling within the project, and ensuring that all relevant staff are trained in operating under the protocol.
- Producing guidance for staff as reference point in the event of any uncertainty relating to the handling of information.
- Assessing the need for new IT systems to safely process and store the data, and providing staff with training in any new system adopted.
- Assessing the portability of using anonymised or pseudonymised data as part of the project to reduce identification risks, and developing an appropriate anonymisation protocol if the use of anonymised data is suitable.
- Ensuring that individuals are fully informed about how their information will be used.
- Providing a contact point for individuals to raise any concerns they may have with the organisation.
- If using external data processors, selecting appropriately experienced data processors and putting in place legal arrangements to ensure compliance with data protection legislation.
- Deciding not to proceed with a particular element of a project if the data privacy risks associated with it are inescapable and the benefits expected from this part of the project cannot justify those risks.

Risk Assessment Guidance:

Likelihood/Potential for an Incident to occur	Impact/Outcome of Incident	Risk Level Calculation L X I	Guideline Action Timetable
1 - Rare: No history of event occurring over period of years. This event may occur but in exceptional circumstances.	**1.** Minor compromise of privacy (e.g. un-sensitive personal data such as helpdesk ticket compromised)	1 – 2 Acceptable	No Action
2 - Unlikely: The event would be expected to occur annually	**2.** Minor data breach (e.g. inappropriate contact of data subject via email)	3 – 5 Low	Prioritise after medium risk actions complete
3 - Possible: This could occur monthly, as such it has a reasonable chance of occurring.	**3.** Moderate data breach (Sensitive data e.g. payroll compromised)	6 – 10 Medium	Prioritise after high risk actions complete
4 - Likely: Expected to occur at least weekly, the event will occur in most situations	**4.** Significant data breach (Financial loss, severe stress for a data subject or data subjects	11 – 15 High	Prioritise Action as soon as Practical
5 - Certain: Expected to occur almost daily, it is more likely to occur than not.	**5.** Major data breach (Risk of severe financial loss to a large number of data subjects)	16 – 25 Very High	Action Urgent

Appendix E – Subject Access Request

Subject Access Request (SAR) Form

Subject Access Request Form

Under the General Data Protection Regulation (GDPR) it is your right to request a copy of any personal data that we hold on you. Please note that this form is to aid the Subject Access Request process. Further information on the Subject Access Request process can be found at www.setu.ie

Name (Last, first, middle initial) Date

PPS Number

Address

Phone number Email address

Name Date

Please describe the information you are looking for, including dates and locations

Signature Date

For Employee Use Only

Received By:

Please send this form to gdpr.cw@setu.ie or dataprotection.wd@setu.ie

Appendix F – Data Breach Reporting Form

SETU Data Breach Reporting Form

Please note: A copy should be kept by the individual filling out the form for records purposes

Section A: Initial Incident Report - *To be completed by the individual reporting the incident and/or the appropriate Head of Faculty/Head of Function/Head of Department. Students or external 3rd parties should complete the form and provide it to the appropriate Head of Faculty/ Head of Function/Head of Department*	
Name:	Function:
Date:	Staff Number:
Date of Incident:	Time of Incident:
Who was Notified?	Time of Notification:
Description of Incident: (e.g. impacted systems, witnesses to the incident, websites etc.)	
Type of breach: (confidentiality breach, availability breach, integrity breach).	
Specific details of the breach (What happened? Which systems/files affected? Who was involved? Categories of data affected? How did this occur?)	
Comments	

Section B: Investigation, Assessment and Response *(To be completed by the appropriate Head of Faculty/Head of Function/Head of Department)*
Estimated number of data subjects affected
Estimated number of records affected
Categories of data subject affected (e.g. employees, the public, suppliers etc.)
Categories of personal data affected (e.g. Contact Details, Health Data, Bank Details, etc.)
Potential risks to the data subject/likely consequences of the personal data breach
Mitigating factors in place or proposed to be actioned
Assessment of likelihood of risks to data subject
Assessment of severity of risks to the data subject
Likely to result in a risk to the rights and freedoms of the data subject? (Y/N and justification). Note: If yes it should be reported to the Data Protection Commission. Please contact the Data Protection Officer to report
Risk Level? (None, Low, medium, high and include justification). Note: If some level of risk report to Data Subject

Comments	
Signed By	**Date:**
Section C: Post Incident Review *To be completed by the appropriate Head of Faculty/Head of Function/Head of Department and reviewed by the Data Protection Officer)*	
Potential weaknesses identified which are required to be remediated?	
What action have you taken to prevent similar incidents in the future?	
Has there been any media coverage of the incident?	
Is a Data Protection Impact Assessment ('DPIA') required for the process in light of new information?	

Have we recorded communications to the Data Protection Commission and Data Subject where necessary? If so please provide their details and an outline of their response.	
Comments	
Signed By **Staff Manager:**	**Date:**

Appendix G - Glossary of Terms

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 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.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data	As used in these Procedures 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 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 School 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 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 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 the Data Protection 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 function/area to adhere to the 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.
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.

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.
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.

All other terms used in these Procedures, not referenced in this section shall have the same meaning as the GDPR.