Data Breach Procedure

Version 1.0

Revision History:

Date of this revision: October 2024	**Date of next review**: October 2026

Version Number/ Revision Number	Revision Date	Summary of Changes	Changes marked
1.0		New Procedure	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	n/a		

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	Data Protection Officer	Oct 2024

Quality Assurance:

Date Approved: Oct 2024	Date Procedure to take effect: Oct 2024	Date Procedure be Reviewed: Oct 2026
Written by:	Data Protection Officer	
Approved by:	VP for Governance/University Secretary	
Approving Authority:	n/a	
Head of Function responsible:	Corporate Compliance & Risk Manager	

Document Location:

Website – Policies and Procedures & Data Protection	X
Other - GDPR Hub	X

1.0 INTRODUCTION

SETU is required by data protection laws to safeguard personal data and to respond swiftly and appropriately in the event of a security breach involving personal information. If a breach occurs that poses a risk to individuals, the University is legally obligated to notify the Data Protection Commission within 72 hours of becoming aware of the incident. Additionally, when there is a high risk to individuals' rights and freedoms, those affected must be informed without undue delay. Prompt action is crucial in responding to any actual or suspected data security breach to prevent harm to individuals and to minimise operational, financial, legal, and reputational damage to the University.

2.0 PURPOSE

The purpose of this procedure is to provide a framework for reporting and managing data security breaches affecting personal or sensitive personal data held by the University. This procedure supplements the University's Data Protection Policy which affirms SETU's commitment to protect the privacy rights of individuals in accordance with data protection legislation.

3.0 SCOPE AND RESPONSIBILITY

This procedure applies to:

- All SETU Stakeholders to include Staff, Students, Governing Body Members, etc.
- All data processors who process data on behalf of the University.

4.0 WHAT IS A PERSONAL DATA BREACH?

A data breach is defined 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."*[1]

Personal data security breaches can happen in a number of ways, including via:

- disclosure of confidential data to unauthorised individuals
- inappropriate access controls allowing unauthorised use of information
- alteration or deletion of records without authorisation by the data owner
- transmission of emails containing personal or sensitive information in error to the wrong recipient
- unauthorised access to computer systems (e.g., hacking, etc)
- viruses or other security attacks on IT equipment systems or networks
- equipment failure
- loss or theft of data or equipment on which data is stored (e.g., memory stick, laptop, etc)
- loss or theft of paper records
- access to confidential information left unlocked in accessible areas (e.g., leaving PC unattended when logged into user account, documents left at shared photocopiers)
- breaches of physical security (e.g., forcing of doors/windows/filing cabinets).

The General Data Protection Regulation (GDPR) identifies three categories of breaches:

- **Confidentiality Breach** – unauthorised or accidental disclosure of or access to personal data
- **Availability Breach** – unauthorised or accidental loss of access to or destruction of personal data
- **Integrity Breach** – unauthorised or accidental alteration of personal data.

[1] Article 4(12) GDPR

If there is any doubt as to whether a data breach has occurred, the Data Protection Officer (DPO) must be consulted immediately by emailing dpo@setu.ie.

5.0 PROCEDURE FOR REPORTING A PERSONAL DATA SECURITY BREACH

All actual or suspected breaches must be reported to the DPO dpo@setu.ie and department manager **immediately.**

The person reporting the breach will be required to complete a 'Breach Notification Form' for assessment as **soon as possible and no later than 24 hours** after discovering the breach/ suspected breach. The urgency of reporting a breach/ suspected breach to the DPO is to enable the University to comply with statutory reporting obligations which require the University to notify the Data Protection Commission within 72 hours of becoming aware of the breach where the breach is likely to result in a 'high risk' to the rights and freedoms of the data subjects, and to inform the data subjects, where appropriate, without undue delay. Failure to report a breach within the prescribed timelines may result in the University being fined by the DPC.

6.0 DPO MANAGEMENT OF A PERSONAL DATA BREACH

Upon receiving the Data Breach Notification Form, the DPO will take the following steps:

6.1 IDENTIFICATION & ASSESSMENT OF THE INCIDENT

Information provided in the SETU Breach Notification Form will assist the DPO in assessing:

- Whether a personal data security breach has occurred
- The nature of the personal data involved
- The cause of the breach
- The extent of the breach (i.e. number of individuals affected)
- The severity of the consequences for the affected individuals.

Following this assessment, the DPO will determine the level of risk involved (None/Unlikely, Low, Medium, High, Severe) using the ENISA Personal Data Breach Severity Assessment Methodology[2].

In line with the accountability principle, an internal record of this assessment will be retained as well as a log of all data breaches.

6.2 CONTAINMENT & RECOVERY

Immediate and appropriate action will be undertaken by the individual responsible for the data breach, in collaboration with their manager, to mitigate the impact of the breach., including:

- Relevant functions (e.g., IT Services, Buildings & Estates, Communications Office) will be informed to enable action to be taken to contain the breach (e.g. isolating/closing a compromised section of the network, finding a lost piece of equipment, changing access codes on doors, etc.).
- Where possible, data losses will be recovered (e.g., physical recovery of equipment/records, the use of back-up tapes to restore lost/damaged data).
- Where appropriate, Gardaí will be informed (e.g., in cases involving theft or other criminal activity).

6.3 NOTIFICATION

[2] https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

Based on the evaluation of risks and consequences, and where a high risk to the rights and freedoms of individuals is identified, the DPO will notify the Data Protection Commission of breaches within 72 hours of the University becoming aware of the incident.

The manager of the area will also notify affected individuals in appropriate circumstances and certainly where the data breach is likely to result in a 'high risk' to their rights and freedoms. Affected individuals will be informed of:

- the nature of the breach
- the circumstances leading to the breach
- the steps taken to rectify the breach, and
- where applicable, the fact that the breach has been notified to the Data Protection Commission.

6.4 EVALUATION & RESPONSE

Following a personal data security breach, the Data Protection Officer (DPO) will conduct a review of the incident and provide the manager with an evaluation. This assessment will ensure that the actions taken during the breach were appropriate and effective, while also identifying opportunities for improvement, such as updating policies and procedures, GDPR training or addressing systemic issues.

7.0 FURTHER INFORMATION

Further information may be obtained from the SETU Data Protection Policy available or on the Data Protection Commission website at www.dataprotection.ie