MTU

Ollscoil Teicneolaíochta na Mumhan
Munster Technological University

Data Protection - Breach Response Policy

21st May 2021

Version: 1.0

www.mtu.ie/policies

Table of Contents

1. Overview 3
2. Purpose 3
3. Scope 4
4. Definitions 5
5. Roles and Responsibilities 6
6. Policy 7
7. Breach Management Plan 7
   - 7.1 Reporting, Identification and Classification 7
   - 7.2 Containment and Recovery 8
   - 7.3 Risk Assessment and Investigation 8
   - 7.4 Notification 8
     - 7.4.1 Data Protection Commissioner 8
     - 7.4.2 Individuals 9
   - 7.5 Evaluation and Response 9
8. Policy Compliance 9
   - 8.1 Compliance 9
   - 8.2 Compliance Exceptions 9
   - 8.3 Non-Compliance 9

Appendix A - Data Incident Reporting Form 10

Document Control 13

1. Overview

The University is responsible for the processing of a significant volume of information. These records are evidence of functions and activities performed across the University.

Good quality records are of value to any organisation, and their effective management is necessary to ensure that the records retained. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

a) comply with information management policies, legal and regulatory requirements (including the Freedom of Information Act 2014, the General Data Protection Regulation 2018), international standards, and best practices;
b) are authentic, reliable and complete;
c) are protected and preserved as evidence to support future actions;
d) ensure current and future accountability;
e) The University has an appointed Data Protection Officer ('DPO') who is available to provide guidance and advice pertaining to this requirement;
f) All Staff must appropriately protect and handle information in accordance with University policies.

This document aims to inform the efficient management of records to a standard which meets accepted best practice. This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. Purpose

The University is obliged under General Data Protection Regulation (GDPR) to ensure that personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Information/data is one of our most important assets and each one of us has a responsibility to ensure the security of this information.

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.

The purpose of this policy is to ensure that a standardised management approach is implemented throughout the organisation in the event of a personal information/data breach.

This policy is designed to:

a) Provide a consistent approach to the management of a personal data breach;
b) Set out the procedure to be followed in the event the University experiences a personal data breach;
c) Reflect the University's responsibilities to comply with the European General Data Protection Regulation;
d) Set out the roles and responsibilities in relation to the management of a personal data breach;
e) Contain any breaches, minimise the associated risk and consider actions necessary to secure personal data and prevent further breaches.

3. Scope

This policy relates to all personal data held by the University in any format.

This policy applies to:

- Any person who is employed by the University who receives, handles or processes personal data in the course of their employment;
- Any student of the University who receives, handles, or processes personal data in the course of their studies for administrative, research or any other purpose;
- Third party companies (data processors) that receive, handle, or process personal data on behalf of the University.

This applies whether you are working in the University, travelling or working remotely. This policy applies to all employees, service providers, contractors and third parties that access, use, store or process personal data on behalf of the University.

4. Definitions

Damage	This is where personal data has been altered, corrupted, or is no longer complete.
Destruction	This is where the data no longer exists, or no longer exists in a form that is of any use to the controller.
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.
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 the University. Examples of personal data include, but are not limited to: a) Name, email, address, home phone number; b) The contents of an individual student file or HR file; c) A staff appraisal assessment; d) Details about lecture attendance or course work marks; e) Notes of personal supervision, including matters of behaviour 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."
Types of Breach	A breach incident includes but is not restricted to the following: a) Loss or theft of confidential or sensitive personal data or the equipment used to store the data (electronic or paper data); b) Failure of equipment; c) Unauthorised use of access to, or modification of, personal data in IT systems; d) Successful attempts to gain unauthorised access to information or IT systems; e) Unauthorised disclosure of personal data; f) Human error leading to loss of personal information.(e.g. forwarding of emails to incorrect recipients, leaving documents on printer)
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 and/or local requirements.

5. Roles and Responsibilities

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

Responsible Office/Person(s)	Role
Governing Body	• To review and approve the policy on a periodic basis.
Audit & Risk Committee	• To oversee all aspects of data protection and privacy obligations.
President	• Ensure processes and procedures are in place within the University to facilitate adherence to the Data Protection Breach Response Policy.
University Executive Team (UET)	• Implement the Data Protection Breach Response Policy and advocate a GDPR compliant culture**.**
Data Protection Officer (DPO)	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR. • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of compliance with data protection and privacy obligations. • To act as a representative of data subjects in relation to the processing of their personal data. • To report directly on data protection risk and compliance to the University Executive Team and the Audit and Risk Committee. • To report directly on data protection risk and compliance to executive management.
Heads of Schools, Departments & Support Functions, Directors of Research Centres	• Implementing the Data Protection Breach Response Policy in their areas of responsibility. • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.
Data Users	• Read and understand this policy document. • Adhere to the policy statements in this document. • Report suspected breaches of policy to their Head of Schools & Support Functions/Directors of Research Centre.

6. Policy

This policy should not be viewed in isolation. Rather, it should be considered as part of the University suite of Data Protection policies (see Document Control).

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:

a) Reporting, Identification and Classification;
b) Containment and Recovery;
c) Risk Assessment;
d) Notification;
e) Evaluation.

7. Breach Management Plan

7.1 Reporting, Identification and Classification

Any individual who accesses, uses or manages personal data is responsible for reporting data breach incidents to the Data Protection Officer and their Head of Function as soon as it is detected. If the incident occurs outside of normal working hours it should be reported as soon as is practicable.

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

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. A "Data Incident Report" form (see Appendix A) should be completed and forwarded to the appropriate Head of Function and the Data Protection Officer.

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.

7.2 Containment and Recovery

This involves limiting the scope and impact of the breach of personal data through:

- Appropriate steps to be taken immediately 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;
- Determine a suitable course of action to resolve the incident.

7.3 Risk Assessment and Investigation

An assessment of the risks associated with the breach should be carried out immediately and should take the following into consideration:

a) The potential adverse consequences for an individual(s);
   - How likely it is that adverse consequences will arise
   - How serious or substantial the consequences would be should they materialise

b) The nature, sensitivity and volume of personal data;
c) The type of the breach (loss/theft) – what has happened to the data;
d) The ease of identification of an individual(s);
e) Could the data be used inappropriately;
f) The number of individuals involved;
g) Security measures in place (encryption/permissions and/or anonymisation/pseudonymisation of files);
h) Wider consequences.

7.4 Notification

The Data Protection Officer in conjunction with the Head of Function will determine who needs to be notified of the breach. This may include the individuals affected by the breach, the Data Protection Commissioner and the University Executive Team.

7.4.1 Data Protection Commissioner

a) 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.
b) The Data Protection Commissioner must be notified without undue delay and not later than 72 hours after becoming aware of the breach.
c) 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.
d) If not included in the initial report, a follow up report should be submitted including actions taken or to be taken by the University 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.

7.4.2 Individuals (Subject of Breach)

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

7.5 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.

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, procedures will be reviewed and updated as necessary.

The review will take the following into consideration:

a) How personal data is stored;
b) Where personal data is held;
c) Where the greatest risks are;
d) Security of data transmission; and,
e) Security of data access.

8. Policy Compliance

8.1 Compliance

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

8.2 Compliance Exceptions

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

8.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, being taken in accordance with the University's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action. Non-compliance shall be reported to the Data Protection Officer.

Appendix A - Data Incident Reporting Form

Section A: Initial Incident Report *(To be completed by individual reporting the incident and/or Line Manager)*	
Name:	Function:
Date of Notification:	Staff/Student 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? How did this occur?)	
Comments	
Section B: Investigation, Assessment and Response *(To be completed by the Data Protection Officer ('DPO') and reviewed by Staff Manager)*	
Is this a Data Breach Y / N	
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 report to Supervisory Authority*
Risk high? (Y/N and justification). Note: If yes report to Data Subject
Comments

Signed By DPO	**Date:**

Section C: Post Incident Review *(To be completed by the DPO and reviewed by the Staff Manager)*
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 Supervisory Authority and Data Subject where necessary? If so please provide their details and an outline of their response.
Comments

Signed By DPO:	**Date:**
Signed By **Staff Manager:**	**Date:**

Document Control

A. Document Details

Title:	Data Protection – Breach Response
Owner(s):	Vice Presidents for Finance & Administration and Corporate Affairs
Author(s):	Data Protection Officers
This Version Number:	1.0
Status:	Approved
Effective Date:	21/05/5021
Review Date:	2022

Important Note: If the 'Status' of this document reads 'Draft', it has not been finalised and should not be relied upon. An existing approved document is deemed relevant until such time as an updated document has been approved by the relevant approval authority and becomes the new binding document.

B. Revision History

Version Number	Revision Date	Summary of Changes	Changes tracked?	Proposed Review Date
0.1	30/10/2020	Initial MTU Draft	Yes	
0.2	09/02/2021	Updated based on feedback from DPOs – Overview section, Roles & Responsibilities of DPOs	Yes	
0.3	18/02/2021	Review by IT Managers	Yes	
0.4	30/04/2021	Updated based on feedback by IT Managers and DPOs	Yes	

C. Relevant/Related Existing Internal/External Documents

D. Consultation History (where required)

This document has been prepared in consultation with the following bodies:

IT Managers

E. Approvals

This document requires following approvals (in order where applicable):

Name	Date	Details of Approval Required
Governing Body	21/05/2021	

F. Responsible for Communication and Implementation

The Manager/Functional Area responsible for communication and implementation:

Title	Functional Area	Date Implemented
Data Protection Officer	Corporate Affairs	21/05/2021