Maynooth University
Data Protection Office

Personal Data Security Incident Management Procedure

Author / Policy Owner:	Data Protection Office
Creation Date:	7th March 2018
Review Date:	3rd September 2019
Version:	3rd September 2019
Scope:	This policy applies to all staff and students of Maynooth University
Related Policies:	Student Data Privacy Notice Staff Data Privacy Notice Data Protection Policy

Revision History

Date of this revision: 3rd September 2019	Date of next review: 3rd September 2020

Table of Contents

1. Introduction

Maynooth University is obliged under the Data Protection Acts 1988 to 2018 (Data Protection Law) and the General Data Protection Regulation (GDPR) to keep personal data safe and secure and to respond promptly and appropriately to data security incidents and/or breaches which includes reporting such incidents or breaches to the Data Protection Commissioner. It is vital to take prompt action in the event of any actual, potential or suspected incidents or breaches of data security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the University.

2. Purpose

The purpose of these procedures is to provide a framework for reporting and managing data security incidents or breaches affecting personal or sensitive personal data held by the University. These procedures are a supplement to the University's Data Protection Policy which affirms its commitment to protect the privacy rights of individuals in accordance with Data Protection Law and the GDPR.

3. What is a Personal Data Security Incident or Breach?

A personal data security incident or breach is any event that has the potential to affect the confidentiality, integrity or availability of personal data held by the University in any format. Personal data security breaches can happen for a number of reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the data "owner";
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing personal data;
- personal data viewable in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive data sent in error to the wrong recipient.

Personal data is defined as:

Personal data means information relating to a living individual who is or can be identified either directly or indirectly, including by reference to an identifier (such as a name, an identification number, location data or an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual). This can be a very wide definition depending on the circumstances.

Special Categories of Personal Data means personal data relating to an individual's: racial or ethnic origin; political opinions or religious or philosophical beliefs; trade union membership; genetic or biometric data processed for the purpose of uniquely identifying a natural person; physical or mental health, including in relation to the provision of healthcare services; sex life or sexual orientation. Individuals have additional rights in relation to the processing of any such data.

4. Who do these procedures apply to?

These procedures apply to all users of University personal data, including:

- any person who is employed by the University or is engaged by University who has access to University data in the course of their employment or engagement for administrative, research and/or any other purpose;
- any student of the University who has access to University data in the course of their studies for administrative, research and/or any other purpose;
- individuals who are not directly employed by Maynooth University, but who are employed by contractors (or subcontractors) and who have access to University personal data in the course of their duties for the University.

5. What types of data do these procedures apply to?

These procedures apply to:

- all personal data created or received by the University in any format (including paper records), whether used in the workplace, stored on devices and media, transported from the workplace physically or electronically or accessed remotely;
- personal data held on all University manual systems, IT systems managed centrally by IT Services, and locally by individual Departments/Offices/Institutes/Centres or Units.
- any other manual IT systems on which University personal data is held or processed.

6. Who is responsible for managing personal data security breaches

Personal data security incidents or breaches are managed by the Data Protection Officer in conjunction with the Bursar/Secretary and the Director of IT Services (where appropriate).

7. Procedure for reporting personal data security incidents or breaches

There is a statutory requirement on the University that all incidents in which personal data has been put at risk must be reported to the Data Protection Commissioners Officer "without undue delay" and where feasible within 72 hours of becoming aware of the breach.

In the event of an incident or breach of personal data security or a suspected incident or breach occurring, every effort must be made to ensure that it is dealt with immediately and appropriately.

If a person becomes aware of an actual, potential or suspected incident or breach of personal data security, he/she must report the incident ***immediately*** to the Data Protection Officer.

Incidents/breaches must be reported immediately by phone, email or on the personal data security breach report form (appendix A).

Data Protection Officer
Ann McKeon
dataprotection@mu.ie
Tel +353 1 7086184

- Line managers should also be notified as appropriate
- IT Services must also be notified as appropriate at ext 3388 or email helpdesk (servicedesk@mu.ie).

1. The Data Protection Officer will review the incident, as reported and consult with relevant staff.

2. The personal data security breach/incident will be reported to the Data Protection Commissioner as appropriate.

3. All breaches are recorded on the University Data Breach Register (link).

   If a decision is made not to report a breach, a brief summary record of the incident with an explanation of the basis for not informing the Data Protection Commissioner will be recorded on the University Data Breach Register.

4. Containment and Recovery

   Containment involves limiting the scope and impact of a data security breach. If a breach has occurred, appropriate action will be taken by the Data Protection Officer to minimise any associated risks which may include but not limited to:

   - Establishing who within MU needs to be made aware of the breach and ensuring relevant staff are informed what is required to assist in the containment exercise;
   - Establishing whether there are any actions which may recover losses and limit the damage the breach can cause;
   - Where appropriate, informing the Gardaí.

5. Risk Assessment

   In assessing the risk arising from a data security breach, the Data Protection Officer must consider the potential adverse consequences for individuals, i.e. how likely are adverse consequences to materialise and, if so, how serious or substantial are they likely to be.

6. Evaluation and Response

   All personal data security breaches will be investigated to identify the root causes of the breaches.

   Subsequent to a data security breach, a review of the incident by the relevant University staff and the Data Protection Officer will occur to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

8. General

All Data Protection issues should be addressed to the:

Data Protection Officer
Ann McKeon
dataprotection@mu.ie
Tel +353 1 7086184

Data Controller
Maynooth University
Maynooth
County Kildare
Ireland
W: www.maynoothuniversity.ie

APPENDIX A
Personal Data Security Breach Reporting Form

Please act promptly to report any Personal data security incidents or breaches. If you discover a data security incident or breach, or suspect a breach may have occurred you must immediately contact the Data Protection Officer by phone, email or by completing section 1 of this form and notify or email it immediately to:

Data Protection Officer
dataprotection@mu.ie

The Data Protection Law **requires** that all incidents in which personal data has been put at risk must be reported to the ODPC "without undue delay and where feasible within 72 hours of becoming aware of the breach".

SECTION 1: Notification of Personal Data Security Incident or Breach	**To be completed by the person reporting the incident**
Date and time incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name and contact details of person reporting incident:	
Brief description of incident and/or details of data lost:	
Number of data subject affected, if known:	
Description of Personal Data placed at risk:	
Brief description of any action taken at the time of discovery:	
SECTION 2 : Assessment of Incident or Breach	**To be completed by the Data Protection Officer or Bursars Office**
Details of the IT systems, equipment, devices, manual records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	

How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements e.g. to research sponsors?	
What is the nature of the sensitivity of the data?	

SECTION 3: Action taken	**To be completed by the Data Protection Officer or Bursars Office**
Incident number:	PDSB/001
Date report received:	
Action taken to date:	
Incident reported to Gardaí?	Yes/No If YES: Date reported
Follow up action required/recommended:	
Reported to other internal stakeholders - details,	
NOTIFICATION TO DATA PROTECTION COMMISSIONER	Yes/No If YES: Date reported Details
Notification to data subjects	Yes/No If YES: Date reported Details
Notification to other external regulator/ stakeholder	Yes/No If YES: Date reported Details

Maynooth University
Data Protection Office
Maynooth, Co. Kildare, Ireland.

T +353 1 708 6184 **E** dataprotection@mu.ie **W** maynoothuniversity.ie