Information and Data Security Policy v1.7

Policy Owner:	CIIO
Creation Date:	5th January 2021
Version:	1.7
Scope:	This policy applies to all information and data users of Maynooth University
Related Policies:	Patch Management Policy Password Policy Data Incident Policy
Consultation:	HEAnet ICT Security Services, IT Services, HR, Data Protection Office, Registry, Library, Dean's office, Procurement Office, Research & Innovation
Approved by:	University Executive
Approval Date:	9th March 2020

Revision History

Version	Date	Comment
1.0	11.7.19	Original Release
1.1	31.10.19	Updated following review
1.2	27.11.19	Updated following additional consultation
1.3	10.12.19	Updated following additional consultation
1.4	08.01.20	Added Physical media elements and revised principles
1.5	27.01.20	Updated Roles and Responsibilities
1.6	02.03.20	Updated to reflect input from University Executive
1.7	05.01.21	Added ‘Approved by’ and ‘Approval Date’ following internal audit

Next Review Date: 2022

Table of Contents

1 Relevant Information

Maynooth University is a knowledge driven institute of higher education. Maynooth University's information and data relates to learning, teaching, research, administration and management are high value assets that must be properly managed and protected. Information and data security is critically important.

Effective information and data security requires the participation and support of all employees, students and all others who have access to the University's information, data and related systems.

Maynooth University is committed to the continual development of its Information and Data Security Policy in order to meet its professional, ethical, legal and contractual requirements.

Compliance with this Information and Data Security Policy is essential in order to ensure the safeguarding of University information from theft, unauthorised disclosure, unauthorised modification or destruction.

2 Definitions

Information
For the purpose of this policy, information includes data stored on computers, cloud services, transmitted across computer networks, printed, written, sent by post or fax or stored on removable devices. It includes records containing personal and non-personal data. Much of this policy relates specifically to electronic information but the same principles and level of care should apply to paper based information.

Information asset
Information assets include information, computer software and hardware.

Confidentiality
Requires the protection of information from unauthorised access and disclosure.

Integrity
Involves safeguarding the accuracy, completeness and consistency of both information and computer software.

Availability
Involves ensuring information and the associated services needed to process information are accessible to staff and students as required.

Security
Refers to the mechanisms and procedures designed to ensure that appropriate and effective controls to safeguard information are in place.

Access
Refers to any mechanism by which individuals gain access to information.

3 Scope of the policy

This policy applies to all information and data users in the Maynooth University.

This policy is intended to support the protection, confidentiality, integrity and availability of Maynooth University's information and data assets. This includes, but is not limited to, information and data:

- Stored on electronic media such as IT systems, cloud services, CD-ROMs, USB keys, hard disks, etc.
- Stored on physical media such as printed or handwritten on paper, filing cabinet, white boards, etc.
- Transmitted across internal and public networks.
- Presented using audio visual media.

4 Information & Data Security Policy

Staff and other authorized users of information systems at Maynooth University must comply will the following principles which provide an overview of how Maynooth University aims to ensure the integrity, confidentiality and availability of its information and data, information systems and connectivity.

- Information and data must be protected and managed in line with relevant legislations.

- Information and data will be made available to those who have a legitimate need for access. No access will be given without specific authorization.

- Recipients of information and data should take due care to maintain the integrity, confidentiality and availability of information and data.

- Processes and procedures should be in place to maintain the integrity of information and data; information and data should be accurate, complete, timely and consistent.

- Processes and procedures should be in place to protect IT facilities, services and systems against loss, unauthorised use or abuse.

- Adequate physical security measures should be in place to protect areas that contain and process information and data on paper and other physical media.

- University information and data should be stored, accessed, transferred or communicated only through systems and services, which are provided and recommended by the University.

- Core services such as Email, OneDrive and Teams provided by the University must be used for the University business. Personal email (e.g. Gmail, Hotmail etc.) and non-university approved cloud services (e.g. Google Apps, Dropbox, etc.) must not be used for University business. If there is a requirement to use non-core services outside the approved list, the onus is on the user to ensure the security of the University information and data.

- All portable devices which stores University information and data must be encrypted and secure.

- All information and data users should undergo information security awareness training as part of the operation and support of information and data security.

- A process of continuous improvement will be established via a combination of control reviews, assessments, self-assessments and both internal and external audits.

5 Roles and Responsibilities

The roles and responsibilities for the Information and Data Security Policy are;

University Executive

- Responsible for approving the Information and Data Security Policy.
- Lead and foster a culture that values, protects and uses information and data for the success of the University and benefit of its members.
- Ensure that a fit for purpose information security framework is in place, including this policy as the top-level reference document.

Data Protection Officer

- Advise the University and its employees of their responsibilities and obligations regarding personal data under applicable data protection legislation.
- Monitor compliance with the data protection legislation and relevant policies.
- Provide guidance on the completion of Data Protection Impact Assessments.
- Co-operate and act as the contact point with the Data Protection Commission in relation to complaints, investigations, audits and consultations and any other matter relevant to the legislation.
- Draw the University's attention to any failure to comply with the applicable data protection rules.

Information Security Manager

- Advise the University on compliance with this policy and its associated supporting policies.
- Review, update and promote the Information and Data Security Policy and other supporting policies.
- Periodically assess security controls as outlined in the Information and Data Security Policy and other supporting policies.
- Co-ordinate the investigation of and maintain records of security incidents as they arise.
- Reporting to the CIIO on the status of security controls within the University.
- Implement and run an effective information security awareness program.

Heads of Department

- Familiarise themselves with this Information and Data Security Policy.
- Where a policy breach is highlighted, heads of academic and administrative areas must co-operate in ensuring that relevant reporting procedures are followed.
- Ensure all information and data under their remit is safeguarded including third party access.
- On an annual basis, all Head of Departments or an assigned delegate are required to engage with information security in relation to compliance with the Information and Data Security Policy and other associated policies.

IT Services

- In concert with information security; design, develop, implement and maintain IT systems and services with regard to the information and data security requirements of confidentiality, integrity and availability.
- Provide advice and assistance to support the implementation and management of the Information and Data Security Policy and procedures.
- Technical delivery of the Information and Data Security Policy objectives.

All Users

- Ensure their understanding and compliance with the Information and Data Security Policy and all other relevant policies in relation to digital and non-digital forms of information and data.
- Ensure that they request, where necessary, and receive adequate and relevant information and data security awareness training.
- Report information and data security incidents via the defined and approved channels.

6 Governance

The University's information and data security governance must ensure compliance with various pieces of legislation relating to the handling and use of information and data, as well as the common law duty of confidentiality. These include, but are not limited to:

- The General Data Protection Regulation (GDPR)
- Irish Data Protection Bill
- Freedom of Information Act 1997
- European Communities Data Protection Regulations, (2001)
- European Communities (Data Protection and Privacy in Telecommunications) Regulations (2002)
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act (1991)
- Child Trafficking and Pornography Act (1998)
- Intellectual Property Miscellaneous Provisions Act (1998)
- Copyright and Related Rights Act (2000)
- Health and Safety Act (1989)
- Non-Fatal Offences Against the Person Act (1997)
- Electronic Commerce Act (2000)
- ECommerce Directive (2000/31/EC)
- Regulations entitled European Communities (Directive 2000/31/EC) Regulations 2003 (S.I. No. 68 of 2003)

Compliance with this policy is the responsibility of all users who may be held personally responsible for any breach of the legislation.

7 Awareness and Distribution

A copy of the Information and Data Security Policy will be published on the University website.

Orientation Training.

All new employees are required to read and acknowledge their acceptance of the Information and Data Security Policy as part of their employee orientation.

Updates

Updates to policies and procedures will be made periodically and will be posted to the University website.

8 Review and Reporting

The Policy will be reviewed and updated on, on-going basis, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practices.

9 Contact

Maynooth University Information Security Manager
Email: informationsecurity@mu.ie
Telephone: +353 1 708 6388