MANCHESTER 1824
The University of Manchester

Information Security Policy

1 Introduction

This Policy forms part of a suite of policies and procedures that support an Information Governance Framework.

2 Purpose

Information is an important asset to the University and it is the policy of the University that information used for the University's teaching, learning, research, commercial and administrative activities must be protected from threats which may result in financial loss, reputational damage or exposure to liability. The purpose of this Policy is to inform staff as to how this is achieved and to summarise their responsibilities in relation to information security.

3 Scope

For the purpose of this Policy, information includes the raw data from which information is derived and audio-visual materials.

This Policy applies to:

- all information created, received or used in the course of University business which must be protected according to its sensitivity, criticality, and value, regardless of the media on which it is stored, the location of the data, the manual or automated systems that process it, the methods by which it is distributed or the locations from which it is accessed; and/or
- all members of staff, as well as individuals conducting work at or for the University and/or its subsidiaries, who have access to University information (**"staff"**). This includes temporary, honorary, visiting, casual, voluntary and agency workers, students employed by the University and suppliers (this list is not intended to be exhaustive).

Information entrusted to the University by third parties, or accessed as part of delivering University business, will also be safeguarded in accordance with this Policy and associated procedures and technical security standards which set out the minimum standards, unless the University has agreed to adhere to third party policies that are more restrictive.

4 Responsibilities and compliance framework

Information security involves the implementation of proportionate controls and responsibilities which are recognisable by external regulators, funding bodies, business partners and collaborative partners as being in line with recognised information security standards (such as ISO/IEC 27001 Information Security Management System) and which support compliance with relevant legislation and regulations.

The Registrar, Secretary and Chief Operating Officer and the Deans of Faculties are accountable for compliance with the Information Governance policy framework.

Heads of School and Directors are responsible for ensuring that all information and processing is in line with the Information Security, Data Protection and Records Management policies.

Information Asset Owners are responsible for the information being processed. Where information is created and accessed by many users (such as the University's administrative applications) the Information Asset Owner is the business owner for the service. Information Asset Owners also include, for example, the authors of research papers, dissertations, databases or spreadsheets (this

list is not intended to be exhaustive). A key responsibility of the Information Asset Owner is to ensure that a risk assessment is carried out to identify and mitigate the likelihood and impact of security failures and/or breaches and to determine the information's security classification in order for the appropriate security measures (people, process, technology) to be applied. This includes measures to ensure:

- Confidentiality - information is protected from unauthorised access and disclosure throughout its lifecycle, from creation to final disposal;
- Integrity - the accuracy and completeness of information is safeguarded and unauthorised amendment or destruction prevented, including the integrity of externally provided data;
- Availability - information and associated services is available to authorised users in line with business and funding body requirements;
- Authentication – the identity of persons accessing highly restricted and critical systems which permit the creation, amendment or deletion of University records must be recorded and verifiable; and
- Legislative and regulatory compliance.

Access must only be provided on a "need to know" basis.

The "Information Security Classification, Ownership and Secure Information Handling Standard Operating Procedure" provides further details regarding mandatory information handling requirements and specific technical security measures are prescribed in the "Minimum Controls Technical Security Standard".

Any high risk processes must be escalated through local risk registers and notified to the Information Governance Office. Where appropriate, these risks will be further escalated to the University's Information Governance Committee.

All staff:

- must act in accordance with this Policy and associated procedures and guidelines (see Document Control Box) established to protect information, and must seek advice and guidance from the Information Asset Owner or the Information Governance Office if clarification is required;
- must embed information risk assessment within normal working practices and throughout information handling processes;
- must report any actual or suspected failure or breach in information security (ie any compromise of information confidentiality, integrity, availability or authentication), "near misses" or working practices which jeopardise the security of the University's information; and
- must undertake information security related training as appropriate for their role.

Other specific responsibilities within the wider Information Governance Framework are detailed in the "Information Governance Accountability and Assurance Framework Standard Operating Procedure".

Staff must note that any breach of this Policy may be treated as misconduct under the University's relevant disciplinary procedures and could lead to disciplinary action. Serious breaches of this Policy may constitute gross misconduct and lead to summary dismissal or termination of contract.

5 Monitoring compliance

The information security management framework (controls and responsibilities), as described in the University's policies, procedures and technical security standards, is subject to internal monitoring,

alerting and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of the commitment to continual improvement. The University will also undertake appropriate benchmarking and may be audited by external bodies.

Reports on the matters related to this Policy will be provided to the Information Governance Committee.

6 Review of Policy

This Policy will be reviewed at least annually or when significant changes are required.

Version amendment history

Version	Date	Reason for change
1.0	June 2010	Creation
1.1	October 2011	Updated links to related policies and procedures
1.2	Nov 2014	Updated links to related policies and procedures
2.0	May 2016	Inclusion of the requirement for staff to undertake information security related training
2.1	Sept 2017	Minor amendments: change of name from Information Security Governance Group to Information Governance Committee; change of job title of lead contact from Head of Information Security to Head of Information Governance; added link to Information security classification, ownership and secure information handling SOP - published
2.2	Dec 2017	Minor amendments: GDPR related; minor changes for consistency with other policies; added authentication; approved by IGC 23 Jan 18
2.3	24 Jan 2018	Minor amendment requested by OGC- sent to PRC for endorsement on 6 Feb 2018
2.4	4 Dec 2018	Minor amendments: analytics related; minor changes for use of external data – IGC approved
3.0	March 2019	Inclusion of Information Asset Owner role and risk escalation responsibilities; inclusion of Deans as accountable, HoS as responsible; reference to av materials
3.1	Sept 2019	Change of name of responsibilities SOP

Document control box	
Policy / Procedure title:	Information Security Policy
Date approved:	March 2019
Approving body:	Information Governance Committee
Version:	3.1
Supersedes:	3.0
Previous review dates:	Dec 2018
Next review date:	Sept 2020
Related Statutes, Ordinances, General Regulations:	Statute XIII Part III re disciplinary procedures for staff; Ordinance XIV Intellectual Property Rights (IPR), Data Protection and the Use of Information Systems; University General Regulation XV Use of Information Systems; University General Regulation XVII Conduct and Discipline of Students – (I) re misuse of property and information systems (H&S)
Related policies:	Data Protection Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914 Freedom of Information Policy:

Document control box	
	http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14915 Records Management Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14916 Acceptable Use Policy – IT facilities and services: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277
Related procedures:	Information Governance Accountability and Assurance Framework SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=8039 Acceptable Use of IT Facilities and Services - Standard Operating Procedure for Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 Information security classification, ownership and secure information handling: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 Data Protection by Design and Default SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=37445 Disciplinary and dismissal procedure for support staff: http://documents.manchester.ac.uk/display.aspx?DocID=480
Related guidance and or codes of practice:	Information Governance Guidance: http://www.staffnet.manchester.ac.uk/igo/ Records Retention Schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514 IT Security guidance: http://www.itservices.manchester.ac.uk/secure-it/
Related information:	
Equality relevance outcome:	Low
Policy owner:	Director of Compliance and Risk
Lead contact:	Head of Information Governance