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.

This Policy applies to:

- all information created or received 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 will also be safeguarded in accordance with this Policy which sets out the minimum standards, unless the University has agreed to adhere to third party policies that are more restrictive.

4 Responsibilities and compliance framework

This is achieved through the implementation of 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.

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;
- 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.

A risk assessment must be carried out to identify and mitigate the likelihood and impact of security failures and or breaches and to determine, having considered the cost of doing so, the appropriate security measures (people, process, technology) to be applied.

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 Governance Office if clarification is required;
- must embed 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 are detailed in the Information Security Responsibilities 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) 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.

If you are reading a printed version of this document you should check http://documents.manchester.ac.uk/display.aspx?DocID=6525 to ensure that you have the most up to date version

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

Document control box	
Policy / Procedure title:	Information Security Policy
Date approved:	May 2016
Approving body:	Board of Governors
Version:	2.3
Supersedes:	Information Security Policy 2.1
Previous review dates:	Dec 2017
Next review date:	Jan 2019
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: 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:	SOP Information Security Responsibilities: 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:

Document control box	
	http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 Disciplinary and dismissal procedure for support staff: http://documents.manchester.ac.uk/display.aspx?DocID=480
Related guidance and or codes of practice:	Data Protection Guidance: http://www.dataprotection.manchester.ac.uk/ 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 Govenance