

Records Management Policy

1 Introduction

This Policy forms part of a suite of policies and procedures that support an information governance framework.

A record is defined in the Records Management British Standard BS ISO 15489 as “Information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business”. All records created and held by the University, both paper and digital, (including email and information held in databases) are subject to this policy.

Records are an important asset to the University and they require appropriate management for effective and efficient administration, for the discharge of University responsibilities and business, and for compliance with legislative requirements. Good management of records also helps staff in the performance of their duties by improving access to and organisation of relevant records, removing out of date or superseded records from University systems and reducing duplication of documents and data.

There are also several pieces of legislation which impact on the way in which the University manages and uses information. Non-compliance with this legislation may result in financial and reputational penalties.

2 Purpose

University records are defined as those documents or data sets which arise from or facilitate the business carried out by the University and which provide evidence of its transactions or activities.

This Policy aims to ensure that the University, creates, maintains, retains, uses and properly disposes of those records which it requires for the conduct of its business and that they are managed in a manner commensurate with legal obligations and information requirements. The University acknowledges the legislative environment within which it operates, particularly in the context of this Policy, those pieces of legislation, related codes of practice and standards listed in the control box below. These all have implications for the way in which public authorities are expected to use and keep records and apply records management standards.

This will be achieved through the implementation of controls and responsibilities including measures to ensure, support and enable:

- the delivery of University business including assurance that external data sources are safeguarded through appropriate controls and audit.
- legislative compliance - compliance with record keeping provisions in current legislation such as the Freedom of Information Act, data protection legislation and the Environmental Information Regulations.
- lifecycle management – records must be kept for an appropriate length of time and in an appropriate manner. They must be disposed of at the end of their lifecycle in accordance with policies, procedures and best practice and in accordance with the University’s Records Retention schedule.
- confidentiality – University records must be protected from unauthorised access.
- integrity – the accuracy and completeness of University records must be safeguarded and unauthorised amendment or destruction prevented.
- availability – University records must be available to authorised users in line with business and funding body requirements.
- efficiency – University records must be available to authorised users in a form that ensures efficiency and ease of use.
- authentication – the identity of the persons accessing highly restricted and critical systems which permit the creation, amendment or deletion of University records must be recorded and verifiable.

- semi-current manual records (records which are not in regular use, but which have not yet reached their disposal date) will be managed, where appropriate, in the University Records Centre

3 Scope

This Policy applies to:

- all University records and information processing including research, whether internally or externally funded, are included, as are records sent, received or used via email or any other method of communication;
- 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);and
- all locations from which University-related information is accessed including off-campus locations.

4 Responsibilities and compliance framework

The University has a corporate responsibility to maintain records of processing and its records management systems in accordance with the regulatory environment. This responsibility therefore extends to all staff who work with University records. Personal email accounts (including personal University email accounts and non-University email accounts) must not be used for storing primary University records. Any emails which are important and need to be kept must be stored elsewhere in an appropriate filing system relevant to their confidentiality or criticality; this could include shared email role accounts. All emails which remain on the email system in a personal University email account will be deleted after a specified period when a person leaves the University.

Deans, Heads of School, Directors or equivalent are responsible for ensuring that records management within their areas is carried out in line with this Policy and established procedures. To assist with this, the University has identified Information Governance Guardians (IGGs) across all organisational units, areas and Schools. IGGs are responsible for helping to ensure that records are managed appropriately within their areas.

The Information Governance Office is responsible for providing policies, procedures, guidance and advice in support of this Policy, for training staff where necessary and for managing the University Records Centre.

5 Monitoring compliance

The information records management system is subject to internal monitoring and auditing throughout the University, and the outcomes from these processes will inform and improve practices as part of a 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	October 2012	Creation and approval by the Board of Governors
1.1	Sept 2017	Data Protection Guardian changed to Information Governance Guardian; Records Management Office changed to Information Governance Office; links updated
1.2	December 2017	Minor changes: for consistency with other policies; defined a record; added authentication; removed explicit legislation reference
1.3	8 Jan 2018	Insertion following Risk and Emergency Management Group recommendation: email deletion; email not appropriate for record storage – Approved by IGC 23 Jan 2018
1.4	24 Jan 2018	Minor changes required by OGC – sent to PRC for endorsement on 6 Feb 2018
1.5	8 Nov 2018	Minor changes: analytics requirements; to reflect email management practice – approved by IGC on 4 December 2018

Document control box	
Policy title:	Records Management Policy
Date approved:	December 2018
Approving body:	Information Governance Committee
Version:	1.5
Supersedes:	1.4
Previous review dates:	December 2017
Next review date:	December 2019
Related Statutes, Ordinances, General Regulations:	Ordinance 14 Intellectual Property Rights, Data Protection and the Use of Information Systems University General Regulation XV Use of Information Systems Statute XIII Part III disciplinary procedures for staff
Equality relevance outcome:	Medium
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 Information Security Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525 Acceptable Use Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16277
Related procedures:	Information Security Classification, Ownership and Secure Information Handling SOP: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=29971 Acceptable Use SOP for Staff: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221 Records Retention Schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514 Other related procedures: http://www.staffnet.manchester.ac.uk/igo/policy-procedures/
Related guidance and / or	Information Governance guidance: http://www.staffnet.manchester.ac.uk/igo/

codes of practice:	IT Security guidance: http://www.itservices.manchester.ac.uk/secure-it/
Related information:	
Policy owner:	Director of Compliance and Risk
Lead contact:	Head of Information Governance