

Records Management Policy

If you are reading a printed version of this document, you should check <https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14916> to ensure you have the most up to date version.

1. Introduction and purpose

- 1.1. This Policy forms part of a suite of policies and procedures that support an information governance framework.
- 1.2. University records 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.
- 1.3. 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. It aims to ensure that records are available as assets to the University and are capable of reuse in appropriate contexts, including artificial intelligence (AI).
- 1.4. 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helps staff in the performance of their duties by improving access to and organisation of relevant records, removing out of date or superseded records from University systems, and reducing duplication of documents and data. This supports the effective use of AI, including reducing the risk of over-sharing, by applying metadata that enables identification and protection of information and deleting information that should no longer be held.
- 1.5. 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. Scope and definitions

- 2.1. This Policy applies to:

- 2.1.1. all University records and information processing including research, whether internally or externally funded
 - 2.1.2. records sent, received or used via email, Teams chats or any other method of communication
 - 2.1.3. 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)
 - 2.1.4. all locations from which University-related information is accessed including off-campus locations.

- 2.2. 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.
- 2.3. Reference to "business activity" or "business activities" is interpreted broadly to mean those activities that support the purposes of the organisation's existence. Functions, activities, transactions and work processes are representations of particular forms of "business activity".

3. Roles and responsibilities

- 3.1. 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.
- 3.2. Deans, Heads of School, Heads of School Operations and 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.
- 3.3. The Information Governance Office is responsible for providing policies, procedures, guidance and advice in support of this Policy and for training staff where necessary.

4. General principles

- 4.1. Records are both evidence of business activity and information assets. They can be distinguished from other information assets by their role as evidence in the transaction of business and by their reliance on metadata. Metadata for records is used to indicate and preserve context and apply appropriate rules for managing records.
- 4.2. Managing records encompasses the following:
 - 4.2.1. creating and capturing records to meet requirements for evidence of business activity.
 - 4.2.2. taking appropriate action to protect their authenticity, reliability, integrity and useability as their business context and requirements for their management change over time.
- 4.3. This will be achieved through the implementation of controls and responsibilities including measures to ensure, support and enable:
 - 4.3.1. the delivery of University business including assurance that external data sources are safeguarded through appropriate controls and audit.
 - 4.3.2. legislative compliance - compliance with recordkeeping provisions in current legislation such as the Freedom of Information Act, data protection legislation and the Environmental Information Regulations.
 - 4.3.3. lifecycle management – records must be kept for an appropriate length of time and in an appropriate manner. They must be securely 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.

- 4.3.4. confidentiality – University records must be protected from unauthorised access.
- 4.3.5. integrity – the accuracy and completeness of University records must be safeguarded and unauthorised amendment or destruction prevented.
- 4.3.6. availability – University records must be available to authorised users in line with business and funding body requirements.
- 4.3.7. efficiency – University records must be available to authorised users in a form that ensures efficiency and ease of use.
- 4.3.8. 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.
- 4.3.9. semi-current physical records (records which are not in regular use, but which have not yet reached their disposal date) will be managed, where appropriate, through the University's record storage facilities

4.4. The IGO recommend sharing links to documents within emails where and when possible rather than using attachments. Personal accounts (including personal University OneDrive and email accounts and non-University email accounts) must not be used for storing primary University records. Any emails and documents 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 or SharePoint Online.

5. Monitoring compliance

- 5.1. 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.
- 5.2. Reports on the matters related to this Policy will be provided to the Information Governance Committee.

Version amendment history		
Version	Date	Reason for change
1.0	Oct 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	Dec 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
1.6	26 Aug 2020	Updated links
1.7	13 Oct 2022	Review of the policy and high level review of ISO 15489 and have included more modern language to articulate the benefits of good records management. Also added a recommendation to use links to documents within email ie reduce the number of attachments. Minor formatting changes.
1.8	4 Dec 2023	Minor changes – Removed as the UoM does not have this capability: “The University will also undertake appropriate benchmarking and may be audited by external bodies.”; referenced personal OneDrive and Email not being the place for records but suggesting SharePoint 365, added leavers’ access removal
1.9	Dec 2025	Restructured the policy to fit the University’s policy template, with removal of some irrelevant or duplicated points. Removed reference to the University Records Centre. Changed owner to Director of Information Governance and contact to Records Manager.

Document control box	
Policy title:	Records Management Policy
Lead contact email:	sian.astill@manchester.ac.uk
Date approved:	15 January 2026
Approving body:	Information Governance Committee
Version:	1.9
Supersedes:	1.8
Previous review dates:	December 2023
Next review date:	01 December 2026
Equality impact outcome:	Medium
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
Related policies, procedures, guidance, etc:	Records Retention Schedule: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514 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 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 Other related policies and procedures: http://www.staffnet.manchester.ac.uk/igo/policy-procedures/ Information Governance guidance: http://www.staffnet.manchester.ac.uk/igo/ IT Security guidance: http://www.itservices.manchester.ac.uk/secure-it/
Policy owner:	Director of Information Governance
Lead contact:	Records Manager