University of York

Information and Records Management Policy

1. Introduction

The University recognises that the efficient management of its records is necessary in order to support and provide evidence of its core functions, to comply with its legal and regulatory obligations, to meet accountability requirements and stakeholder expectations, to enable the effective management of the institution and to advance its strategic priorities.

The policy sets out how to ensure the creation, maintenance and protection of authentic, reliable and useable data and records, with appropriate evidential characteristics, within the University. It establishes a framework and accountabilities for information and records management, through which best practice can be implemented and audited.

2. Scope

This policy applies to all recorded information in digital and hard copy formats that is created, received and maintained by University members as Information Users in the course of carrying out their University functions. Records are those documents, regardless of format, which facilitate University activities (e.g. teaching, learning and research) and operations and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. Records may be created, received or maintained in hard copy or electronically.

This policy applies to records created in the course of research, whether internally or externally-funded, in addition to any contractual and academic record-keeping requirements.

This policy covers all applications and business systems used to create, manage and store University information and records, including content and information management systems, databases, email, voice and instant messaging, websites, and social media applications. The policy covers information created and managed in-house and off-site, including cloud-based platforms.

This policy is binding on all those who create or use University records, i.e. Information Users such as University staff, students, associates, partners, contractors, consultants and visitors, whether accessing records from on or off-campus.

3. Roles and responsibilities

All staff, as Information Users, are responsible for creating, maintaining and preserving accurate records that support and document their activities in accordance with this policy and its associated policies, procedures and guidance. They must know what information they hold, where it is held and complete mandatory records management training.

University Officers, Heads of Departments and Professional Services, as Information Owners, are responsible for ensuring that all records in their area are managed in conformance with this policy and associated policies and procedures. Information Owners are responsible for promoting this policy and ensuring their staff complete mandatory records management training and that their departments and units complete information asset registers.

Principal and Co-investigators affiliated to the University are responsible for ensuring that their research projects and their resulting records and data are created, managed and disposed of in compliance with this policy, the University's Code of Practice on Research Integrity, and any specific legal, ethical and contractual conditions.

Information Champions are responsible for maintaining information asset registers, and for providing a local point of contact for queries, liaising with the Records Manager and University Archivist as required.

The University's Information and Records Manager is responsible for promoting and supporting compliance with this policy across the University and its wholly-owned subsidiaries, including the development of retention schedules and procedures, drawing up guidance and providing training and support on good information and records management practice.

The University's Information and Records Manager, as **University Archivist**, has responsibility for the University Archive and the authority to determine and requisition those University records with historical or enduring evidential value.

The University of York owns all records created by its employees carrying out University-related functions and activities unless otherwise specified under contract or in its Regulations. Unless the originator asserts ownership, records received by the University are also its property.

Staff, students, associates, partners, contractors, consultants and visitors who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

4. Oversight

The **Chief Operating Officer**, as Senior Information Risk Owner, has overall responsibility for records management within the University. The implementation, oversight and management of information and records management policy on a day-to-day basis is delegated to the Information Security Board.

The **Information Security Board**, chaired by the Director of IT Services, is responsible for the approval of information and records management policy, for overseeing policy implementation and for regular policy reviews. It monitors the effectiveness of the information and records management policy across the University. It also monitors information risks and compliance through reporting and it commissions and responds to independent audits of records management arrangements.

5. Policy

The University will manage records and data efficiently and systematically, in a manner consistent with ISO 15489 and the statutory Code of Practice on Records Management, to support University operations and to meet legislative, regulatory, funding and ethical requirements. All information management practices in the University should align to this policy and its supporting procedures.

Records will be created, maintained and retained in order to provide information about and evidence of the University's decisions, transactions and activities. Appropriate systems will be in place to record these decisions and activities.

Records must be maintained in line with these six Records Management principles to ensure their viability and quality across their lifecycle:

i. The record is present: the information the University needs to evidence and reconstruct the relevant activity or transactions is recorded and is accurate.

ii. The record can be accessed: when it is needed, it is possible to discover, locate and access the information. It is possible to present it in a way that is true to the original presentation of the information. The authoritative version can be identified in cases where multiple versions exist.

iii. The record can be interpreted: a context for the information can be established, showing when, where and who created it, how it is related to other records, and what process/activity it comes from.

iv. The record can be trusted: the information and its representation is fixed and matches that which was actually created and used, and its integrity, authenticity and provenance can be demonstrated beyond reasonable doubt.

v. The record can be maintained: the record can be accessed, interpreted and trusted for as long as it is needed (in line with the Retention Schedule and in some cases permanently) notwithstanding transfers to other agreed locations, systems, formats and technologies so that it remains present, accurate, trustworthy, interpretable and accessible.

vi. The record's value is understood and protected: it is recognised that our records form part of our corporate memory and are an important institutional resource which must be protected across their lifecycle in accordance with the above principles.

Where University departments procure or develop IT and business systems, records management requirements must be considered, documented and addressed from the initial requirements stage. A Business System Lifecycle Management Assessment should be undertaken for new digital systems and services to help assess their ability to function as a recordkeeping system and the Records Manager consulted for advice.

Departments and services must maintain full and accurate records of their records, IT and record-keeping systems and processing of personal data in Information Asset Registers. This includes ensuring that records which are essential to business continuity ('vital records') are identified and protected.

Appropriate measures will be employed to safeguard the security and integrity of University records and provisions made (i) to maintain their reliability, integrity and preservation during their lifespans and (ii) to prevent the unauthorised or unlawful use, disclosure or loss of information.

Records must be maintained and stored in such a way that they can be easily identified and located to support business activities and that ensures appropriate accountability, using established procedures for secure access and handling.

Records will be retained and disposed of in accordance with agreed retention schedules in a controlled and compliant manner. Retention schedules will set out the minimum period for which a record should be retained and will be reviewed regularly and amended as necessary. Retention schedules will be agreed by the senior Information Owner(s) for the relevant University function. When the currency of the records and their need to be retained expires, the records will either be destroyed or, if they have lasting historical value, transferred to the University Archive.

Where systems and applications are to be decommissioned or records are scheduled for migration or conversion between business/record systems, including conversion to digital formats, the Records Manager should be consulted. The decommissioning of digital services and digitisation should be carried out in line with IT Services' and Records Management guidance and the Records Management Principles.

A small percentage of the University's records will be selected for permanent preservation, in line with the Appraisal Policy for Corporate Records. These records will become part of the University Archive which will maintain the University's corporate memory by preserving records of enduring evidential and historical significance.

Information and records management awareness and training will be provided for staff as part of the University's statutory and compliance training programme.

This document, together with its subsidiary policies and implementation documents, defines the framework within which records are managed across the University.

6. Policy implementation documents

This document, together with related records management guidance is available from the records management website.

A policy context document provides further contextual guidance to support the University Information and Records Management Policy.

The Records Retention Schedule defines how long records should be kept for before being deleted/destroyed, reviewed or transferred to the University Archive.

The appraisal policy for corporate records sets out the process by which the University will distinguish and select those records with the highest value for permanent preservation from those of no enduring value.

The Research data management policy enables the University and its researchers to meet the standards and responsibilities set out in the University's Code of Practice on Research Integrity and to meet funder, ethical, legal and other responsibilities.

7. Policy review

The policy will be reviewed on a three-yearly basis. It is next due for review in January 2026. After this date, policy and procedural documents may become invalid.

Document history

Version	Date	
1	12 December 2012	Approved by Information Strategy Group
2	29 January 2016	Reviewed and approved by Information Security Board
3	31 July 2019	Reviewed and approved by Information Security Board
4	5 April 2023	Reviewed and approved by Information Security Board

Information and Records Management Policy

Guidance: policy context

1. Introduction

This guidance document provides associated context and further information to support the implementation of the University Information and Records Management Policy.

The University recognises that the efficient management of its records is necessary in order to support its core functions, to comply with its legal and regulatory obligations and to enable the effective management and operation of the institution. It is committed, through the Information and Records Management Policy, to creating, keeping and maintaining those records which document its principal activities, including teaching, research, the administration of its resources and the protection of the rights and interests of the organisation and its stakeholders.

The Information and Records Management policy follows from the University's Information and Records Management strategies. Its purpose is to ensure the creation and maintenance of authentic, reliable and useable records, with appropriate evidential characteristics, within the University by establishing a framework and accountabilities for records management. Through this framework best practice can be implemented and audited.

2. Definition of 'records' and 'records management'

Records are defined as recorded information, regardless of format, which facilitate and derive from University activities (e.g. teaching, learning and research) and business and which are thereafter retained (for a set period) to provide evidence of its decisions, transactions or activities. Records are fixed in time and contain content (information), context and structure. The use or reuse of the information that changes any of these three factors results in the creation of a new record of a different transaction. Records may be created, received or maintained in hard copy or electronically and include email and instant messaging, social media, websites and blogs. They may also be considered as 'Information Assets'.

A record has the following essential qualities:

- *it is present* (the information needed to evidence and reconstruct the relevant activity or transactions is recorded).

- *it can be accessed* (it is possible to discover, locate and access the information, and present it in a way that is true to the original presentation of the information).
- *it can be interpreted* (a context for the information can be established showing how it is related to other information, when, where and who created it, and how it was used).
- *it can be trusted* (the information and its representation is fixed and matches that which was actually created and used, and its integrity, authenticity and provenance can be demonstrated beyond reasonable doubt).
- *it can be maintained* (the record can be deemed to be present and can be accessed, interpreted and trusted for as long as necessary and on transfer to other agreed locations, systems and technologies).

Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records (ISO 15489). It constitutes a series of integrated systems related to the core processes of the University that ensure that evidence of, and information about, its activities and transactions are captured and maintained as viable records.

3. Objectives

Records contain information that is a unique and invaluable resource and are fundamental to University processes and operations. The objectives of a records management system are as follows:

A systematic approach to the management of the University's records is essential:

- to ensure that the information we rely on has the qualities of a record;
- to protect and preserve records as evidence of our actions.

Records Management enables and supports the University's realisation of the corporate objectives described in its Strategy, namely:

- organisational design that ensures smooth and effective day-to-day operations and empowers us to meet the challenges that arise;
- attention to the use of [information] resources, to ensure we meet our ambitions;
- advancement of curiosity-driven and action oriented research;
- supporting research of the highest academic and ethical standards;
- unlocking data to shape and enhance the learning experience;
- driving knowledge exchange for public good.

Records management is accordingly necessary to:

- ensure that the University conducts itself in an orderly, efficient and accountable manner;
- realise best value through improvements in the quality and flow of information and greater coordination of records and storage systems;
- support core University functions, teaching and research, providing evidence of conduct and the appropriate maintenance of associated tools, resources and outputs;
- meet legislative, regulatory, funding and ethical requirements;

- deliver services to staff and stakeholders in a consistent and equitable manner;
- assist and document policy formation and managerial decision making;
- provide continuity and protect vital information in the event of a disaster;
- protect the interests of the organisation and the rights of employees, clients, students, research participants and present and future stakeholders;
- equip and support researchers to be adaptable and flexible in an increasingly diverse, mobile and global research environment; and
- establish an institutional and cultural identity and maintain a corporate memory.

4. Responsibilities

The University has a corporate responsibility to maintain its information and records and its record-keeping systems in accordance with the regulatory environment. For this reason the member of the University's senior management with overall responsibility for the Information and Records Management policy is the Chief Operating Officer.

The University's Information and Records Manager is responsible for

- defining corporate information policy
- devising standards and guidance for good information and records management practice
- managing the records retention schedule and offsite storage solutions
- information audits and surveys
- oversight of Information Asset Registers
- management of the Record of Processing Activities
- providing advice on data and records management issues, the value, importance and retention of records
- the selection of records as archives and management of the University Archive.

Heads of Departments, Principal and Co-Investigators at the University, and all those who lead a team of staff in an organisational unit, programme or project, have overall responsibility, as Information Owners, for supporting the management of records generated by their department's/team's activities, and should ensure that:

- adequate records are kept of the activities in their functional area of responsibility, for which they are accountable
- the records created, received and controlled within the purview of their department, unit or project, and the systems (electronic or otherwise) and procedures they adopt, are selected and managed in a way which meets the aims of the University's records management policy and any other relevant contractual requirements
- they promote this policy and enable good records management practice within their area
- staff inductions cover local and corporate policies and procedures and staff and students have access to relevant training opportunities
- staff exit interviews/procedures cover the appropriate transfer and return of records, permissions (e.g. transfer of ownership in Google My Drive), equipment and other information assets
- they liaise with the Records Manager where necessary regarding issues or incidents of concern.

Staff designated as Information Champions, a role held by a member of staff within a University department, provide a key point of contact between departments and the Records Manager in the implementation of records management and compliance policies. Designated by their Head of Department, they will liaise with the Records Manager on behalf of their departments, promote central guidance to colleagues and assist in the local implementation of data management and compliance procedures and best practice.

All staff and contractors are responsible for creating, maintaining and preserving accurate records that support and document their employment/contracted activities in accordance with this policy and its associated policies, procedures and guidance. They must know what information they hold, where it is held and University staff should complete mandatory records management training.

Other staff may have specific responsibilities for records as part of their role e.g. Committee Secretaries and should follow relevant University policy and guidance for the specific types of records that they manage.

5. Legislative, regulatory and best practice framework

University records and its processing of data are governed by a variety of legislation (including employment, contract, charity and financial laws), common law duties (of confidentiality and care), and regulated practice. The Information and Records Management policy framework has been formulated in the context of University policies and guidelines, national legislation and sectoral/professional standards. It is intended to support standards and practice and to promote easier compliance with legislative and regulatory environments. Key policies and legislation related to this policy are cited below.

University policy

- Ordinances and Regulations
- University Data Protection Policy
- Information Security Policy
- University Code of Practice on Research Integrity
- Retention Policy
- Appraisal Policy
- Research Data Management Policy

Legislation

- Charities Act 2011
- Civil Evidence Act 1995
- Consumer Rights Act 2015
- Copyright, Design and Patents Act 1988
- Data Protection Act 2018 and UK General Data Protection Regulation
- Environmental Information Regulations 2004

- Equality Act 2010
- Finance Act 2008
- Freedom of Information Act 2000
- Human Rights Act 1998
- Limitations Act 1980
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- Regulation of Investigatory Powers Act 2000

A fuller survey of legislative and regulatory provisions concerning record-keeping and the processing of University data is maintained by the Records Manager.

Standards

- *Code of Practice on the Management of Records: issued under Section 46 of the Freedom of Information Act 2000 by the Secretary of State for Digital, Culture, Media and Sport providing guidance to public authorities on the keeping, management and destruction of records* (DCMS, 2021)
- ISO 15489:2016 *Information and Documentation – Records Management*
- ISO 27001 *Information Security Management Systems – Requirements*
- *BS 10008-1:2020 Evidential weight and legal admissibility of electronically stored information*
- BSI DSC PD5000:2002 *Legal admissibility: an international code of practice for electronic documents and e-business transactions for evidence, audit, long-term duty of care*
- *BS PD* 5454:2012 Guidance *for the storage and exhibition of archival documents*
- *Records retention management* (Jisc, 2019)
- UKRI Policy and Guidelines on Governance of Good Research Conduct (UKRI, 2013)
- *OfS Regulatory Framework issued under section 75 of the Higher Education and Research Act 2017* (2022)

6. Further information

A suite of Information and Records Management guidance has been produced on the following areas and will continue to be developed.

Appraisal	Metadata
Assessing your RM maturity	Naming files and folders
Boxes and supplies	Non records
Committee records	Office moves
Creating records	Record 'holds'
Data mapping	References

DBS certificates	Remote working
Disposal form	Research data
Dispose of IT equipment	Retention schedules
Disposing of information	Security classification & handling scheme
External records store: inventorying	Temporary records
External records store: transfer to	Transferring archival records
External records store: recall from	Version control
External records store: destruction	Video conferencing
File plan	Vital records
Glossary	What are records?
Managing workspaces	What is Records Management?

Online induction training and awareness material is provided through the University's statutory compliance training programme, the University's general Staff Induction sessions, and Records Management website.

7. Contacts

Records Manager and University Archivist	Dr Charles Fonge, Borthwick Institute records-manager@york.ac.uk
Records Management Assistant	Mr Graham Hughes, Borthwick Institute

Document history and status

Version	Date	
1	12 December 2012	Approved by Information Strategy Group
2	29 January 2016	Reviewed and approved by Information Security Board
3	31 July 2019	Reviewed and approved by Information Security Board
4	5 April 2023	Reviewed and approved by Information Security Board

Review cycle: Three yearly

Date of next review: January 2026