Information and Records Management Policy

Purpose

1. 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.
2. This policy establishes a framework and accountabilities to ensure the creation, maintenance, and protection of authentic, reliable and usable 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.

Scope

3. 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.
4. The 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.
5. The 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.
6. 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.

Definitions

7. Records: 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.

Policy statement

8. 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.
9. 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. Corporate channels of communication should be used for official business as far as reasonably practicable.
10. Records must be maintained in line with these six Records Management principles to ensure their viability and quality across their lifecycle:
    - The record *is present*: the information the University needs to evidence and reconstruct the relevant activity or transactions is recorded and is accurate.

- The record *is accessible*: 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.
- The record *is interpretable*: 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.
- The record *is 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.
- 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.
- 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.

11. Where University departments procure or develop IT and business systems, records management requirements must be considered, documented and addressed from the initial requirements stage.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. A small percentage of the University's records will be selected for permanent preservation, in line with the method statement on the selection and appraisal of 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.
18. Information and records management awareness and training will be provided for staff as part of the University's statutory and compliance training programme.

Roles and responsibilities

19. **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.
20. **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 maintain accurate information asset registers and provide a local point of contact for queries, liaising with the Records Manager and University Archivist as required.
21. **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.
22. The **Chief Financial and 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.
23. The **Information Security Board**, chaired by the Chief Financial and Operating Officer, is responsible for the approval of information and records management policy, for overseeing policy implementation and for regular policy reviews.
24. The **University Records Manager and Archivist** 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. As University Archivist, the role also has responsibility for the University Archive and the authority to determine and requisition those University records with historical or enduring evidential value.
25. 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.
26. 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.

Monitoring and review

27. The Information Security Board, chaired by the Chief Financial and Operating Officer, is responsible for monitoring the effectiveness and assuring compliance with this Information and Records Management Policy across the University. The Board monitors information and governance risks and compliance status, drawing on a range of inputs including: reporting against the ICO Records management framework toolkit and tracker, key performance indicators for records management, benchmarking against sector standards, monitoring records management maturity, and monitoring security and data incidents. The Board is also responsible for commissioning and responding to independent audits of the University's records management and data governance arrangements to ensure a robust and accountable framework.
28. The policy will be reviewed on a three-yearly basis. It is next due for review in [December 2028]. After this date, policy and procedural documents may become invalid.

Document control

Approval body:	Information Security Board
Policy Owner:	Chief Financial and Operating Officer
Responsible Service:	Records Management
Policy Manager:	Records Manager and University Archivist
External regulatory and/or legal requirement addressed:	Statutory Code of Practice on the management of records issued under 2000 (c. 36), s. 46.
Equality Impact Assessment:	Not relevant for this policy
Approval date:	4 December 2025
Effective from:	4 December 2025
Date of next review:	December 2028

Version control

1.0	12 December 2012	Approved by Information Strategy Group
2.0	29 January 2016	Reviewed and approved by Information Security Board
3.0	31 July 2019	Reviewed and approved by Information Security Board
4.0	5 April 2023	Reviewed and approved by Information Security Board
4.1	7 January 2025	Updated to reflect SIRO and ISB changes
5.0	4 December 2025	Reviewed and approved by Information Security Board