Information and Records Management Policy Guidance

Introduction

This policy guidance 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 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 usable 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.

Contents

Further guidance

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

Appraisal and selection

Assessing your RM maturity

Boxes and supplies

Committee records

Creating records

Data mapping

DBS certificates

Disposal form

Dispose of IT equipment

Disposing of information

Email management

External records store: inventorying

External records store: transfer to

External records store: recall from

External records store: destruction

File plan

Glossary

Managing workspaces

Metadata

Naming files and folders

Non records

Office moves

Record 'holds'

References

Remote working

Research data

Retention schedules

Security classification & handling scheme

Temporary records

Transferring archival records

Version control

Video conferencing

Vital records

What are records?

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.

Capture and control of records

Records must be created and captured that are full, accurate and have sufficient context so that it is possible (now and in the future) to establish what has been done/decided and why.

Records must be up to date and accessible. They should be of a suitable quality to allow those who use or rely on them to work efficiently, to be able to find and interpret them, and to demonstrate compliance with any relevant legislation, policies or regulatory codes. They should help staff and the organisation to meet public and stakeholder expectations around accountability and good governance.

Where University departments and offices purchase or develop IT and business systems, record-keeping requirements must be considered, documented and addressed from the initial requirements or procurement stage. The Records Manager should be consulted for advice.

All digital records created or received in the course of university business must be adequately maintained within a managed and endorsed University IT system. A list of endorsed University systems and software is maintained by IT Services. A system endorsed by IT Services should have a completed Computing Risk Assessment *and* (where it holds records) a completed lifecycle management assessment.

Where University departments procure or develop IT and business systems, records management requirements should be considered, documented and addressed from the initial requirements' stage. The completion of a Business System Lifecycle Management Assessment is recommended for new digital systems and services to help assess their ability to function as a recordkeeping system. The Records Manager should be consulted for advice and to help agree retention decisions and document processing activities. Where a new system or technology will process personal information, the screening questions for a Data Protection Impact Assessment should also be completed.

Records should be created at, or as close as possible to, the time of the event or transaction they relate to. Supporting data about the record (metadata) should be captured to ensure records can be identified, understood in context and time, trusted and managed.

Decide what format (file format, digital/hardcopy) is most appropriate for the management, accessibility, storage and preservation of the record and its information. This should be informed by how long it's needed (i.e. retention period), operational needs and how it will be used, any security risks, dependencies and vulnerabilities, and any specific legal requirements for particular records.

All records should carry at least the core metadata elements required to enable effective operations and lifecycle management. For drafts and revised versions, version numbers or procedures for version control should be in place to allow Information Users to distinguish between different versions and understand the status of the document (e.g. draft, final, approved etc.).

Staff who create and use information must be aware of any restrictions on access and apply/maintain access controls and security markings as relevant. Records should be protected from unauthorised alteration or untimely or accidental deletion.

Guidance on the storage of physical records is set out on the University's Information and Records Management website.

Information created when outsourcing or working jointly with another organisation

Some University work may involve working jointly and collaborating with other universities, and organisations, or outsourcing a function or service to an external contractor.

When collaborating or outsourcing, set out each party's responsibilities in an information sharing agreement. Ensure the sharing agreement details:

- how information should be handled
- what, if any, controls and requirements for security are required
- the obligation and methods to record any decisions that are taken about the information shared. For example, records management controls and when and how information/records will be destroyed or transferred when the project/relationship/service ends or the information is no longer of use.
- obligations under copyright, data protection and freedom of information legislation
- The ownership of any copyright

If you work with an external contractor, information they hold on your behalf is also within the scope of your responsibility for information management purposes. This means you should ensure the contractor applies appropriate information management standards and procedures.

University systems

Departments and individuals who procure, develop or implement digital or physical systems to process records must ensure that the system adheres to the six Records Management Principles and the provisions of the Information Management Framework for the entire lifecycle of the record.

The Business System Lifecycle Management Assessment Tool is designed to help assess a system's ability to function as a recordkeeping system and support the lifecycle management of the records and data in it.

The Statutory Code on Records Management expects that corporate tools and systems are in place will allow the university:

- To manage and organise information throughout its life;
- To locate and use information;
- To have back-ups and contingencies to recover from system failures and major disasters;
- To ensure that the timely destruction of information is carried out in line with its sensitivity and is permanent.

Digital systems, services, databases and applications that capture records should be declared in the Systems' Register and the record/data types they contain should be declared on departmental Information Asset Registers.

Systems should be managed effectively over their own lifespan, from acquisition to decommissioning, to ensure their integrity, reliability and performance

Where a records system is being replaced or superseded by another system the Records Management Principles and Information Management Framework must be adhered to. Where a records system is to be decommissioned, the Information and System Owners must provide for the maintenance or transfer of the records, so that they remain accessible, trusted and complete for the required retention period. Further information on digital continuity, and the migration/conversion of records, is given below. IT Services maintain protocols for decommissioning business systems.

Storage

Records should be held in a managed system (whether digital or analogue) and maintained in such a way that they remain secure and usable for their lifetime. They should be stored in conditions that take account of the records' specific properties and sensitivities and protect the records and their information from unauthorised access or use, damage, loss or obsolescence. Security for both physical and digital environments should reflect the sensitivity, volume, value and needs of the information. When choosing a storage location, due consideration should also be taken of the need to preserve important information in a usable format for its lifetime, and how the choice of storage will enable access commensurate with the frequency of use.

The University operates a digital first policy and information is typically 'digital by default'.

Records should be stored according to the University's file plan where possible, with consistent file naming, to ensure information is well organised and findable.

The University will produce and maintain guidance on the storage of records on its Information and Records Management and IT web pages.

Google Drives: personal drives (Google My Drive) and the documents you create in them are intrinsically linked to the individual. They remain linked to the individual and their account even when shared with others, unless ownership of the individual document is transferred. This means that when someone leaves and their account is deactivated, the documents in it, and all access to the contents of the drive, is lost.

Google My Drive is accordingly most useful for drafting and collaborating on the creation and sharing of documents. Once the document is completed and finalised, where possible it should be stored in the appropriate record keeping system or Shared Google Drive. The Policy for Google Shared Drives should be consulted.

Records (digital and analogue) that have enduring legal, evidential or historic value should be transferred (by arrangement) to the University Archive.

Physical records storage

Hard-copy records and other analogue formats should be stored in secure areas with access provided only to authorised staff.

Current (active) records should be stored with the department or unit responsible for the records. Non-current (inactive) hard copy records whose retention period has not expired can be stored in the University's off-site store. Inactive records stored off-site should be stored with a disposal date and the Information Asset Register should reflect the new location of the records and (date) range covered.

Non-current hardcopy/analogue records identified that are inactive and not referred to regularly can be transferred to the offsite records store.

Non-current records (physical and digital) identified and selected as archives must be stored with the University Archive.

Records stored with an individual employee should be made available to authorised users and be accessible in the event of a legal or authorised request.

Original hard-copy corporate records should typically not be stored outside University premises or systems without approval from the Information Owner. In the case of research notes and records when data is being gathered in the field, adequate protection and safeguards should be in place commensurate to the sensitivity and value of the records in question.

Organisation of records

Business classifications

University has a business classification scheme or 'file plan' to aid the arrangement and assessment of the value of records that derive from its functions and activities. The scheme operates independently of corporate departmental structures. It allows a 'business process map' or 'file plan' to be created.

The file plan is a scheme that identifies overlapping processes and the activities that derive from key functions. It underpins the corporate retention schedule, which identifies principal record creators and holders. Record-keeping systems and filing structures (folders structures on drives, or the use of labels/tags) should reflect the file plan where possible.

Version control should be used to distinguish draft versions from those that are 'declared' as the final version, and to distinguish between previous final/published versions, so that users can understand and have confidence in the quality and status of the record.

Information should be stored in such a way that once a final version is agreed or published, the information cannot be altered, re-edited or tampered with.

Further guidance is available on managing workspaces, naming files and folders, version control, and metadata for record-keeping.

Security classifications

University information must be classified, stored and handled in accordance with the University's Information Classification and Handling Scheme. The scheme provides guidance on the classification of information and the appropriate methods for handling the different levels of security required. It encompasses all information held by the University, in all formats (physical and electronic). Security classifications for particular record series are given in the Records Retention Schedule.

Metadata

Metadata, which is defined as "deliberate, structured data about data," is essential for ensuring that corporate records and data are fit for purpose, trustworthy, and can be appropriately organised, retrieved, and managed. To support effective records management and enable well-informed business decisions, all records and information must include a core set of metadata elements. These mandatory elements — Creator/Author, Date(s) (usually the date of creation), Title, and Subject/Keywords — should be present in all documents and records to provide the basic contextual information required for good data management. Other recommended elements, such as Version information, Security classification, and Retention period should be considered and applied as applicable to the record's context.

Staff creating records and managing or procuring systems should ensure that metadata, whether captured automatically or applied manually, is structured and applied consistently across all corporate records and systems. Effective metadata enables the identification, governance, and correct interpretation of data, helping to optimise data storage, manage records retention, and ensure compliance with retention periods. It is critical to ensure that the metadata the system or users supply is accurate, complete, and consistent, particularly considering the need for records to be easily migrated and understood by other systems (interoperability) or when stored/used outside the original filing context (e.g. downloaded files, saved attachments). By adhering to established metadata requirements, the University can maintain the integrity and accessibility of its records, ensuring proper organisation and management for current and future use.

Email and messaging

Emails are corporate records when they contain business-related information and evidence, such as formal communications, policy decisions, advice, transactions, or authorisation of actions, and must be managed in accordance with the corporate Information and Records Management Policy. Identify and retain emails that serve as records of official University business and dispose promptly of those that are not work-related, are redundant, or have expired value. There is no single retention period for emails: their retention is determined by the specific business activity or transaction they relate to, not by the email format itself. Email retention should therefore be based on the email's subject matter and with reference to the University Record Retention Schedule for the relevant retention period for that content.

Emails whose content needs to be seen by or accessible to others should (where possible) be stored in a shared University system (or for certain roles and offices, a non-personal University account) with the appropriate access controls in place to ensure that only those who are authorised to see them have access and that the emails can be understood in context. This helps ensure that the information in the emails can be located and retrieved and regularly reviewed and deleted when that is the appropriate action.

When creating emails, use clear and concise subject lines and keep communications focused on a single subject to facilitate proper classification and filing. To reduce risk and proliferation, wherever possible do not send confidential information as email attachments and instead point/link to documents in shared drives (like Google Drive) instead of attaching files, which allows for better version control and access management.

We are all responsible for the effective management of our emails. This includes using your work account only for work purposes and applying retention actions routinely by reviewing and "weeding" emails continuously. Use email tools, such as labels/folders, to classify emails based on record categories and their assigned retention periods. For non-personal/delegate accounts, the primary contact must establish and communicate specific rules for management, retention, and determining which emails should be treated as records.

As a general rule, always use corporate channels of communication (e.g. University email accounts, Slack) when conducting official University business. As Slack messages may record actions and decisions of or affecting the University, Slack channels/messages, like emails, must be managed as effectively as other digital and paper information.

Video messaging should not be used to convey or discuss corporate information classified as SECRET. For guidance on transmitting CONFIDENTIAL and personal data see the Information Classification and Handling Scheme and IT guidance on encryption. Guidance on video conferencing records is also available.

Non-corporate communication channels

The use of private email accounts, private message accounts (e.g. WhatsApp) and other similar channels (e.g. SMS text messages) should be avoided wherever possible.

Using non-University channels can put information at risk and create compliance challenges when it comes to Data Protection and Freedom of Information legislation. It can mean information is not accessible if needed for legal requests, be stored and managed to different standards, and be at risk of being lost to the official record when an individual leaves an organisation without transferring it.

Some use of non-corporate communication channels to conduct University business may be necessary in certain circumstances, for example while travelling or during an emergency when it's important to communicate quickly.

If you have used non-corporate channels for university purposes, you should transfer and store any relevant official information or record on the relevant University system(s) as soon as possible.

Vital records

Vital records are those records which are essential to the operation of the University and which it would rely on for business-critical functions and business continuity in the event of a disaster.

Information Owners and Information Asset Administrators should work with Records Management to identify the vital records for their area(s) of operation, record the records' status in the department's Information Asset Register, and take appropriate action to secure and protect the availability and integrity of the record.

The identification and safeguarding of vital records necessary for business continuity should be included in relevant University and departmental business continuity / disaster recovery plans.

Information on the identification, storage and protection of vital records is available from the Records Management website

Information Asset Registers

Accurate recording and knowing where all records are located is essential if their information is to be located quickly and efficiently and the records are to be managed and kept secure.

All departments should ensure that an accurate and up-to-date https://www.york.ac.uk/records-management/records/guidance/survey/iar/ is maintained which identifies the information assets the department holds and the personal data it processes in accordance with Data Protection laws.

Where necessary, appropriate tracking systems and audit trails should also be in place to monitor the use and movement of records (e.g. when physical files are stored offsite, loaned to another department, or archived).

Information asset registers can be used to document retention times and actions as applied/enacted, helping to document local operational practice and needs.

Security and access

Information Owners and Information Asset Administrators must ensure that appropriate levels of security are in place to prevent the unauthorised or unlawful use and disclosure, or loss, of information. All records, irrespective of format, must be held in accordance with the University's Information Security Policy. Records with personal data must also be processed in conformance with Data Protection policy and guidance.

The University's Information Classification and Handling Scheme describes the categories of confidentiality which should be used to classify University information and records. It will assist with determining appropriate practice regarding the storage, access, handling and disposal of records.

Access to records

Information Users, whey they create and/or store records, must ensure that appropriate access and permission controls are in place and are respected throughout the life of the information to protect records from any unauthorised access, disclosure, accidental loss, alteration or damage to the information and that the records are managed in line with the Information Management Framework.

Internal access to records: University staff should have ready, appropriate and proportionate access to the relevant corporate information they legitimately need to do their job. Access in each case, however, must be for a valid and authorised business reason, proportionate, in line with Data Protection principles and grounds, and with respect for any duty of confidentiality, the security classification scheme, or external contractual requirements or security marking schemes. Access to records by staff in another department or unit will require approval from the relevant Information Owner. Members of Legal Services and Records Management may be considered authorised users where access to specific records is required for the purpose of their roles.

Confidential, personal or otherwise sensitive information will not be widely available and will have access permissions assigned to it in line with the Information Classification and Handling Scheme and Information Security policy.

Access to information within personal IT accounts and for formal investigations will be managed under the IT Investigations and Data Access policy.

Access to corporate information by agents and contractors working on behalf of the University will be in accordance with the Third Party Access to University Information and IT Services Policy

Access privileges and individual, group and temporary accounts are assigned and managed in accordance with the Managing User Access Policy.

The public's general right of access to recorded information held by the University is managed under the Freedom of Information Act and its associated legislation. The legislation works to promote openness across the public sector. The right to access one's own personal information (as a data subject) is managed through a Subject Access Request.

Migration and conversion

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 (digitisation), Records Management should be consulted. Decommissioning should be carried out in line with IT Services guidelines on Decommissioning Digital Services and any digitisation in line with Records Management guidance.

The disposal of source records, following migration or conversion/digitisation should be authorised (by the Information Owner following consultation with Records Management) and appropriately planned and documented. During the migration or conversion process, all record content and associated metadata in the originating system or format must be retained until the process is finished and appropriate quality controls completed - with confirmation that the integrity and reliability of the destination system or format have been controlled and secured.

Off-site storage and scanning for retrieval

The University has an approved off-site storage service for hard-copy records that are no longer in active or in regular use, and which still need to be retained in line with the retention policy. The service provides for the cost-effective storage and management of such records to conform with security and records management standards.

Records suitable for the off-site store will need to be boxed and inventoried, have agreed retention periods, not be due for destruction for at least 3 years, and not require frequent retrievals. Records Management will discuss your storage, retrieval and retention requirements with you before any transfer.

An associated digitisation service is available which can assist with remote desktop access to information held off-site and make records more accessible. It can bring significant benefits, but careful consideration should be given to whether scan-on-demand is a suitable solution. This is particularly the case where scanning duplicates copies of the record, impacts on the legal position or evidential integrity/legal admissibility of documents, or a record series is still being added to.

Further details of the off-site storage and scanning services can be found on the External Store wiki.

Digitisation

Where the digitisation of a complete record series is being considered it should be done in accordance with a documented procedure, all processes associated with the digitisation must adhere to the Information Security and Classification and Handling policies and to the University's guidance in relation to the digitisation of records.

The digitisation of corporate records should meet the requirements of BS 10008-1 *Evidential weight and legal admissibility of electronically stored information* and include appropriate quality control and assurance measures and documented audit trails.

If the original physical record is to be destroyed post-digitisation then the digitised rendering needs to be able to be managed as the authoritative record throughout its lifecycle and disposed of, or preserved, in line with the provisions of the University's Records Retention Schedule.

Where the physical original has (or may have) enduring legal, evidential or historical value, the Records Manager and University Archivist must be consulted before scanning or destruction to determine whether or not the physical record has archival/preservation value.

Whilst in certain instances digitisation might help reduce physical storage space requirements through the disposal of the hard copy record, on other occasions it may not be appropriate to destroy the original post-digitisation. An example of this might be where the record has intrinsic value (e.g. historical) in its original physical format or the digitised image is not able to be relied on as the authoritative record.

Digital continuity

Digital Continuity is the ability to use digital information in the way that the University needs and in line with the University Record Retention Schedule (RRS). If the University does not work actively to ensure Digital Continuity, information can easily become unusable. Digital Continuity is about making sure that information is complete, available and therefore usable for business needs. It means having a clear understanding of

- who the responsible owner of the information is (the Information Owner)
- what needs to be retained and how the University will need to use it, over time and through change and across the record's lifecycle.

and ensuring that

- risks to the Digital Continuity of records/information assets within the Information Owner's remit are managed appropriately
- the technical environment and the way information is managed in the relevant business area continues to support the University's use and obligations.

Change risks can include (i) business or organisational changes including restructures, staff turnover etc (ii) technological changes in the IT environment (e.g. losing data, metadata or context during transfers to new formats or systems, or data trapped in ageing legacy systems) (iii) changes to the information assets themselves, and how/where they are stored (e.g. changing the way you structure or store information, format choices and scanning).

Digital Continuity supports the six Records Management Principles in the Records Management Policy, and it is achieved when business requirements, technical environments and information assets support one another.

Transfer of records

When records (digital or physical) are being transported or transmitted, Information Users must take care to ensure the records' safe transition/move to the new location (whether this is temporary or permanent).

Further information on handling is provided in the University's Information Classification and Handling Scheme. Examples of safe transportation include encryption (for digital files) and using double-layered packaging and sending via fully tracked mail delivery, with checks in place for each to ensure that the right recipient and a valid address are used and to confirm delivery.

Digital transfers should be conducted securely using encrypted methods where confidential or large volumes of data are involved (e.g., SFTP or approved secure file-transfer services like DropOff) and should preserve the authenticity, integrity, and usability of the records (e.g. through the use of checksums and digital signatures).

For formal transfers, e.g. under a data sharing agreement, statutory returns, legal responses and access requests etc., a suitable and complete audit trail documenting the transfer, including date, parties involved, method, and (where possible) verification of integrity and receipt should be kept.

Particular guidance is provided for office and record moves on campus.

Records moved from/to campus to/from the offsite records store will be subject to appropriate security, tracking and accreditation.

Retention and disposal of records

The University manages the lifecycle of its records in line with its University's Records Retention Schedule (RRS). The RRS sets out the minimum length of time a record is required for and what should then happen to it. It identifies the master holders of records and gives the reason for the retention and disposition of records.

It is important we keep information only for as long as it has value to the organisation (primary operational/legal/financial value, or secondary evidential, historical or research value). Retention schedules are a clear and defined way of timetabling when information is due for review, transfer to the archive or destruction.

When a record reaches the end of its retention period, a decision must be taken on how it is disposed of. This will involve one of three outcomes:

1. Review: the record is reappraised to determine whether it should be kept for longer or be destroyed
2. Archive: transferred to the University Archive at the Borthwick
3. Destruction

Departments, and specifically the Information Owner, are responsible for ensuring that records in their operational area are destroyed or preserved in a timely and secure manner in accordance with retention policy.

Records due for disposal should be assessed for their research, historic, statistical or archival value prior to arrangements being made for their secure destruction. Contact the University Archivist and consult the Appraisal Policy for further information.

Disposing of a record must be carried out in line with the guidance on Disposing of Information and reference to the University's Information Classification policy. Special consideration must be given to records that contain sensitive information or personal data or are marked as Confidential or Restricted. If records are disposed of insecurely or incompletely, this can risk information being disclosed, can cause a data breach, harm and distress to individuals, and reputational damage and regulatory fines to the University.

The importance of timely records disposal in line with agreed retention periods (managed by the Records Management office) is a core principle of good records management. It is also required by Data Protection and Freedom of Information legislation. Information must be kept about what records have been destroyed or transferred to the Archive or another body, when this happened and why. The records retention schedule, with disposal logs, acts as part of this record.

In the case of destruction, other copies (e.g. backups, scans and downloaded copies, duplicates and print outs etc.) must be destroyed at the same time, unless the copy forms a part of a new or

different record. The Records Management website also provides guidance on the retention of temporary/transitory records (such as draft copies).

Records that relate to anticipated or current litigation, or a current statutory request for access, should be retained notwithstanding the expiry of a retention period or approved disposal process. More information on the procedure for legal holds is available from the website.

Where records are kept for longer than the recommended retention period and are not sent to the University Archive, or records not covered in the Record Retention Schedule are maintained, services/departments should log the agreed retention period in their Information Asset Register.

The RRS is a living document and is subject to ongoing review and development. If the category of record you are interested in does not appear in the schedule, or legislative requirements or operational needs in your area have changed and affect the length of time a record is needed, you should contact your departmental Information Champion or the Records Manager to ensure the RRS remains accurate and up-to-date.

Confidential and personal information must be destroyed securely and a disposal log completed recording the authority for destruction. Confidential and personal information on paper must be destroyed using the University's confidential waste service. Further information is provided on disposing of information.

Ensure you destroy material that has no continuing value on a regular basis. Delete trivial emails and messages as soon as possible after reading. Do not keep multiple or personal copies of documents and dispose of temporary, convenience copies as soon as possible.

Disposal of records and IT equipment

The disposal of University records and IT equipment must be safe, secure, timely, and documented, with appropriate authorisation. Disposal includes both destroying records that are no longer needed and transferring records with permanent value to the University Archive.

Before destroying a record, you must confirm that it's closed and no longer needed for University business, its retention period has expired (as set out in the Retention Schedules), and it's free of any current legal actions or requests. You must also confirm it has no lasting business, research, or evidential or historic value. Destruction must be authorised by the Information Owner. If a record has lasting historic or research value, it should be transferred to the University Archive in consultation with the University Archivist. A disposal log must be completed for major records to create an audit trail and demonstrate compliance.

Secure destruction methods

The method of destruction depends on the nature and sensitivity of the information (see the Information Classification Policy). Secure destruction is especially important for records containing personal or confidential data.

Paper records with personal or confidential information must be shredded (crosscut recommended) and placed in a confidential waste bag, or securely placed in a confidential waste bag for collection.

Magnetic media, CDs, and USB sticks if possible, should be wiped/reformatted first then placed in a separate confidential waste bag (marked ‘Media’) for collection via a Planon request.

Digital records on shared drives, systems, and databases are the Information, Drive or System Owner’s responsibility to delete. Routinely empty digital 'bins' and recycle folders (including Google Mail and Google Drive 'bins') as items in these locations are still considered held by the University.

IT Services is responsible for the secure disposal or repurposing of old University-managed equipment in line with security requirements. For decommissioning old PCs and devices, refer to IT Services' online guidance for secure erasure and disposal.

Further information is available in the guidance on Disposing of records, the Retention Schedule (which set out how long records should be kept as a minimum) Securely erasing a device, Disposing of old equipment, and the Waste and recycling guide

Archival records and transfer

Records and Information Assets with archival and enduring evidential value should be transferred (by agreement) to the University Archive. Access through the Information Owner and University Archive can still be arranged for staff where it is needed.

The Records Retention Schedule addresses the selection and review of certain categories of record (in any format but with enduring evidential or historical value) for transfer to the University Archive for preservation. These records form the University's corporate memory and are preserved in the archive for historical and research purposes.

The University has policies on the appraisal of records for permanent retention as archives, digital preservation and guidance on the transfer of records to the University Archive.

Decisions pertaining to archival University records should be directed to university-archive@york.ac.uk

Managing access to transferred historical records

Wherever possible, records are transferred as open to the University Archive to ensure their preservation and appropriate public access.

Where a closed record is transferred, this does not affect the statutory rights of access established under FOI Act or the Environmental Information Regulations. As information still held by the University as a public authority, anyone still has the right to make a request to access these records.

If the University Archive receives a freedom of information or legal request to access a closed record that is less than 30 years old, it will consult with the department/office that transferred it prior to disclosure. The transferring department/office is responsible for reviewing the information for remaining sensitivities and for making any further representations about whether it should continue to be withheld from public access. As different rules apply to historical records when it comes to exempting information from disclosure, advice from archivists and Information Governance may also be called on.

Legislative, regulatory and best practice frameworks

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
- 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
- Data (Use and Access) Act 2025
- Environmental Information Regulations 2004
- Equality Act 2010
- Finance Act 2008
- Freedom of Information Act 2000
- Human Rights Act 1998
- Limitations Act 1980
- 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.

Freedom of Information Act 2000. The Freedom of Information Act (FOIA) governs access to and the management of recorded information held by public authorities (including universities). The Act was designed to create transparency in public bodies and to provide greater accountability by providing citizens with the right to submit a request for recorded information held by the public body. This right depends on the ability of the organisation to supply information through good records

management programmes. For this reason, we must adhere to the code of practice on record keeping issued by the Secretary of State for Culture, Media and Sport, under section 46 of the FOIA. The section 46 Code of Practice is used as a statutory statement of good records management practice by the regulator (the ICO) and the courts.

UK GDPR and Data Protection Act 2018. The UK GDPR is the principal legislation governing how personal data is managed. It sets in law how personal and special categories of information may be processed. The Data Protection Act's principles are also relevant to the management of records. Under the UK GDPR, organisations may be required to undertake Data Protection Impact Assessments. The UK GDPR also introduces a principle of accountability and requires the University to document its compliance and how and why it processes personal data (through the Record of Processing Activity and the use of Information Asset Registers). All staff and Information Users must take steps to protect personal data according to the UK GDPR and Data Protection Act 2018.

Other relevant legislation. Other legislation requires information to be held as proof of an activity or compliance against the eventuality of a claim or regulatory audit. The Limitation Act 1980 sets out the length of time someone can bring a legal case after an event and typically sets it at six years. This forms the basis for some of the retention periods in the records retention schedule. A wide range of employment, financial, health and safety, and consumer laws also affect the records, data and evidence we need to keep and for how long.

Codes and 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 and 2025)
- UKRI Policy and Guidelines on Governance of Good Research Practice (UKRI, 2025)
- OfS Regulatory Framework issued under section 75 of the Higher Education and Research Act 2017 (2022)

Office for Students (OfS) as regulator. The legal duties of a university registered with the OfS are primarily contained within the OfS Regulatory Framework. These duties are implemented as Conditions of Registration, which higher education providers must meet on an ongoing basis to remain registered, access public funding, and maintain eligibility to sponsor international students.

Professional and ethical obligations

Researchers should keep accurate, complete and reliable records of the research procedures or survey methods followed, and the results obtained, respect confidentiality and manage sensitivities in line with the University's Code of Practice on Research Integrity and Code of practice and principles for good ethical governance

Staff and students who are registered to a professional body (e.g. the General Medical Council (GMC), Nursing and Midwifery Council (NMC), Social Work England or similar) are required to adhere to record-keeping standards defined by their registrant body. As with the University's research integrity and ethical codes, this is designed to guard against professional misconduct and to provide high quality research and care in line with professional and ethical standards.

Glossary

Access	the right, opportunity or means of finding, using or retrieving information.
Accountability	the principle that individuals, organisations and the community are responsible for their actions and may be required to explain them to others.
Appraisal	the process of assigning value to records and is a means of determining the length of retention for a record and (most commonly) whether it has archival value.
Archive	1. Materials created or received by a person or organisation in the conduct of their affairs and preserved because of the enduring historic, legal or public value contained in the information they contain or as evidence of the functions and responsibilities of their creator; permanent records. 2. The division within an organisation responsible for maintaining the organisation's records of enduring value (i.e. the University Archive). 3. The building that houses archival collections (i.e. the Borthwick Institute for Archives).
Business Classification Scheme	is based on the analysis of functions, processes and activities. It documents the structure of a records management system and the relationships between records and the activities that generate them. It provides an essential basis for the intellectual control of records and facilitates their management and use over time. A business classification scheme can be used to ensure that all records are stored consistently, regardless of their format and underpins an Electronic Document and Records Management System (EDRMS). Also known as a file plan or taxonomy.
Capture	refers to the actions that are taken to secure a record into an effective records management system, where the record can be maintained and made accessible for as long as it is needed.

Classification	the systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a Business Classification Scheme or File Plan
Context	a record must be supported by information about the circumstances in which it was created and used. Records cannot be fully understood without adequate knowledge of the activity that gave rise to them, the wider function of which the activity forms part, and administrative context, including the identities and roles of the various participants in the activity. Contextual information must therefore be captured in the records themselves or in the systems that are used to maintain them.
Creation	refers to the creation of a record in a business activity.
Destruction	a process of eliminating or deleting, beyond a possible reconstruction.
Disposition	a range of processes associated with implementing records retention, destruction or transfer decisions. The final point in a record's lifecycle, usually involving either: 1. destruction; 2. transfer to inactive storage with destruction at a specified later date; or 3. transfer to the University Archive for permanent preservation.
Document	recorded information or object which can be treated as a unit. May include printed or electronic papers such as reports, letters, memos, or e-mail messages. The definition also includes handwritten notes and printed out graphical material. An electronic document is any of these held in machine-readable form or as a scanned image.
EDRMS	electronic document and records management system – a dedicated system for capturing records. It supports the capture, registration, storage and indexing, ownership and access rights, retrieval, checkout and return of documents and records.

Evidential value	the usefulness of records as the primary or legal evidence of an organisation's authority, functions, operations, transactions and basic decisions and procedures.
Information Asset	a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles. An information asset can be in any format.
Information Asset Register	a log or index of Information Assets (e.g. databases, a run of records, types of spreadsheet etc). A register helps you and colleagues understand and manage your information assets and the risks to them. It is important to know and fully understand what information we hold, where and how personal data is processed, and where it is stored and shared in order to protect it and be able to exploit its potential.
File list	a list of files and their titles.
File plan	a classification system used (in particular) for managing electronic records. The National Archives' definition is a structured scheme of categories into which files are grouped. Also known as a taxonomy. See also 'Business Classification Scheme'.
Filing	the process of sorting and arranging, classification or categorising, and storing records so that they may be retrieved when needed.
Folder	a collection of documents or records on a specific topic that are held together for management and disposal as a single entity.
Functions	things an organisation must do to achieve its corporate goals and strategies.
Information Asset Administrators	an Information Asset Administrator (IAA) supports the Information Owner by managing an information asset's day-to-day operations and ensuring policies are followed. This involves tasks like maintaining data quality, controlling user access, recognising security incidents,

	and ensuring information is securely destroyed when no longer needed. While the IAA may be responsible for the proper handling of information, the Information Owner remains accountable and will need to ensure that the IAA understands and has the required competencies to undertake these responsibilities. Responsibilities typically delegated by the Information Owner to the IAA include: ● Managing the joiners, movers and leavers process within the team/system ● Ensuring all team members/system users have appropriate and up-to-date training ● Granting and revoking access to confidential information ● Recognising potential or actual security incidents ● Consulting the Information Owner on incident management ● Ensuring that Information Asset Registers, DPIAs, risk assessments and other documents are accurate and maintained
Information Owners	the senior responsible persons for the management of information within a defined area. (Also known as Information Asset Owners).
Information Users	those working day-to-day with information (i.e., all staff) who are responsible for creating, maintaining and preserving accurate records that support and document their activities in accordance with policies, procedures and guidance.
Managing records	any action relating to the lifecycle of a record, from its creation, and use, through to disposal or archiving, and including storage, file naming, classification and the assignment of metadata, retrieval, transfer and preservation.
Metadata	the information used to describe the context, content and structure of records and their management through time. Commonly defined as 'data about data'. The purpose of metadata (e.g. title, subject, file/document creator, dates) is to help users and systems to identify and retrieve relevant documents without having to read the main text, or to define who has access, what security classification applies, or how long the document needs to be kept for.
Metadata standards	standards or system tools that require users to create records, or to enter information into a system, with consistent and descriptive terms in order to support accurate identification and retrieval.

Migration	the act of moving records from one system to another, with maintaining the records authenticity, integrity, reliability and usability.
Preservation	the processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.
Record	any recorded evidence of an activity. Records are information created, received, and maintained as evidence and information by an organisation or person, in pursuance of their legal obligations or in the transaction of their business. A record may consist of a collection of documents that together provide a complete 'story' about a particular activity or process (e.g. a ‘student record’). Records are kept as audit trail evidence of, and as information about, an organisation’s functions, decisions, processes, procedures, operations, proper conduct, rights and obligations, transactions or its other related 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).

Recordkeeping system	information system which captures, manages and provides access to records (digital or hardcopy) over time.
Records lifecycle	a record's lifecycle begins with its creation or receipt and ends with its disposition (where, as records reach the end of their active lives, they are disposed of in some manner: e.g. destroyed or transferred to the University Archive). Records created and maintained within the University will typically fall into one of the following categories/lifecycle phases: Current records: used regularly and frequently in day-to-day operations. Will generally be referred to at least once a month. Semi-current records: not in use frequently and often inactive, but are still needed for legal/operational reasons (e.g. for audit or evidence, statutory or financial requirements, or in case of complaint/challenge). Archival records: records which are no longer current but have an enduring legal, historical, cultural or educational significance. Other records that are no longer required for the work of the University, whose retention period has expired, should be destroyed if they have not been identified as archival or subject to a legal hold.
Records management	the field of management responsible for, and the practices we follow to ensure, that digital and paper-based information (irrespective of format or media) is creation, received, described and filed, maintained, secured, retained and disposed of in a suitable manner. This includes processes for capturing and maintaining evidence of and information about corporate activities and transactions in the form of records.
Records series	a group of related records or documents that are normally used and filed as a unit because they result from the same activity or function or have some relationship arising from their creation, receipt etc., and that permit evaluation as a unit for retention scheduling purposes.
Retention period	the length of time particular records must be kept. This is usually expressed in terms of years and is often contingent upon an event or specification.

Retention schedule	documents how long records are retained for, how and where they should be stored and what action needs to be taken once the record reaches its retention date.
Retrieval	the process of locating and withdrawing records and delivering them for use.
Review	the process of considering whether a record which has reached a specified point in time has (i) residual value requiring retention for a further period (e.g. because needed for an ongoing case) or (ii) enduring archival value (e.g. because it has historical or research value as an archive).
Security classification	security level assigned to a record, document, file, or information based on the sensitivity of the information.
Tracking	creating, capturing and maintaining information about the movement and use of records.
Transfer	transfer (custody): change of custody, ownership and/or responsibilities for records. Usually moving records from active or semi-active office files to off-site storage or to the University Archive. transfer (movement): moving records from one location to another.
Version control	the management of multiple revisions to the same document.