UNIVERSITY OF PORTSMOUTH

RECORDS MANAGEMENT POLICY

May 2023

Contents

Document title		
Records Management Policy		
Document author and department		
Sarah Arnold, University Records Manager, Corporate Governance		
Approving body		
Claire Dunning, Executive Director of Corporate Governance		
Date of approval		
15/05/2023		
Review date		
May 2026		
Edition no.		
6		
ID Code		
041		
Date of effect		
01/06/2023		
EITHER For public access online (internet)? *Tick as appropriate*		**YES**
OR For staff access only (intranet)? *Tick as appropriate*		
For public access on request copy to be mailed. *Tick as appropriate*		**YES**
Password protected. *Tick as appropriate*	**NO**	
External queries relating to the document to be referred in the first instance to the Corporate Governance team: email corporate-governance@port.ac.uk		
If you need this document in an alternative format, please email corporate.communications@port.ac.uk		

The latest version of this document is always to be found at:

http://policies.docstore.port.ac.uk/policy-041.pdf

Summary

What is this document about?

The Records Management policy sets out principles for managing the University's information effectively. It applies to all records – whether paper or electronic – that are created or used by staff.

The key elements of the policy are:

- The University's records are a vital, corporate asset: they provide evidence of its actions and decisions, and must be managed in a consistent, controlled way to ensure transparency, accountability and legal compliance.
- Staff must know what information they hold and where it is held.
- All records – whether paper or electronic – should be organised in a systematic way to ensure they can be quickly and easily retrieved.
- Information must be held securely to prevent unlawful disclosure and to protect expectations of privacy.
- Where appropriate, data should be shared across the University in order to avoid recreating information that already exists and storing duplicate data unnecessarily.
- Departments should control the disposal of their core administrative records in accordance with agreed retention schedules, so that they are managed efficiently and only destroyed legitimately.
- Vital records must be protected to ensure business continuity.
- Emails record the University's actions and decisions, and must be managed as effectively as paper and other electronic records.
- Records documenting the history and heritage of the University must not be destroyed.
- There must be a clear allocation of responsibility within each department for all aspects of record-keeping, including classifying records, applying retention schedules and safely discarding documents.

Who is this for?

This Policy is aimed at all staff.

How does the University check this is followed?

It is not currently possible to enforce this policy pro-actively, although it is anticipated that use of the eRecords system and the introduction of new corporate systems will enable greater control of important electronic records over time.

The University Records Manager provides support and advice to staff with regard to managing their records.

Who can you contact if you have any queries about this document?

Any questions about this policy should be directed to the University Records Manager.

Policy

1. Introduction

The University of Portsmouth recognises that the management of its records is necessary to support its core functions, to comply with its legal, audit and regulatory obligations, and to contribute to the overall management of the institution. This policy sets out principles for ensuring that the University has effective records management.

This policy relates to all types of records – whether paper or electronic – created or used by University staff, and fulfills the requirements of the Lord Chancellor's Code of Practice on the Management of Records (issued under Section 46 of the Freedom of Information Act 2000). Records may or may not contain personal data.

By default, UoP holds the Intellectual Property (IP) for the records created by staff during the time they are employed by the University of Portsmouth. Where the IP remains with a named individual (e.g. some academic research), this should be specified in contracts and, in such cases, the University's record keeping requirements are minimums, beyond which the IP holder may retain the information as they see fit. The University's Intellectual Property Policy can be found on the website.

1.1. Aims

The University's records are a vital, corporate asset: they provide evidence of its actions and decisions, and must be managed in a consistent, controlled way to ensure transparency, accountability and legal compliance. The principal aims of records management are:

- to ensure that, regardless of format or structure, the University's records "possess the characteristics of authenticity, reliability, integrity and useability … to be considered authoritative evidence of business events or transactions and to fully meet the requirements of the business." (ISO 15489: 2016 Records Management);
- to ensure efficiency and consistency in the creation, maintenance, retention and disposal of records;
- to support decision making by maintaining accurate and reliable documentation;
- to provide robust audit trails to evidence decisions and the reasons for decisions;
- to support business efficiency by ensuring information can be quickly located and retrieved;
- to comply with statutory and regulatory requirements affecting the use and retention of records;
- to protect the interests of the institution, its staff, students and other stakeholders by maintaining high quality documentation for appropriate lengths of time;
- to prevent unauthorised or unlawful disclosure by ensuring information is held securely;
- to support business continuity by protecting information that is vital to the continued functioning of the organisation;
- to ensure the timely, secure destruction of information in accordance with retention schedules;
- to preserve the corporate memory by preserving records of historical significance.

1.2. Responsibilities

The University has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. The member of the University Executive Board with overall responsibility for this policy is the Executive Director of Corporate Governance.

The University Records Manager is responsible for developing records management procedures, advising on good practice and promoting compliance with this policy.

Heads of departments are responsible for ensuring that their department has processes in place to meet the requirements set out in section 2 (below).

Line managers are responsible for ensuring that their staff are aware of this policy and comply with its requirements.

All members of staff are responsible for ensuring that their work is documented appropriately and that the records which they create or receive are managed correctly. In addition, they have a responsibility to know what information they hold and where it is held.

Failure to comply with this policy may be subject to HR management policies.

1.3. Legislation and standards

Records held by the University of Portsmouth are regulated by a variety of legislation, including employment, contract and financial law, as well as the Freedom of Information Act 2000 and Data Protection legislation[1]. In addition, the University requires high quality records to be maintained for the purposes of audits and reviews by financial and other regulatory bodies. The University's activities overseas may also be subject to the laws and regulations of other countries.

1.4. Related policies

The Records Management policy should be read in conjunction with the following University policies (all of which are available on the University website):

- Data Protection Policy
- Email Policy (Staff)
- Information Security Policy
- Retention Policy
- Staff Access to University Facilities and Leavers' Procedures
- Information Governance Policy

The Records Management Policy should also be read in conjunction with the Information Security Advisories and the Freedom of Information web pages.

1.5. Further information

Guidelines on the procedures necessary to comply with this Policy will be developed by the University Records Manager, and made available on the Records Management intranet pages.

[1] At the time of writing, the Data Protection legislation comprises the Data Protection Act 2018, the UK General Data Protection Regulation (GDPR) and the retained EU GDPR

2. Management of records

2.1. Creating records

Each department must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records possessing 'the characteristics of authenticity, reliability, integrity and useability' (ISO 15489: 2016 Records Management).

The records must be accurate and complete, so that it is possible to establish what has been done and why. The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met. It is essential that the integrity of the information is beyond doubt: not only should it be compiled at the time of the event/transaction to which it relates (or as soon as possible afterwards), but also it should be protected from unauthorised alteration or deletion. In addition, version control procedures are required for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

Where appropriate, branded templates should be used, so that records are produced consistently and quickly. Wherever possible, records should be created in a way that enables accessibility by those with disabilities.

2.2. Classifying records

All records – whether paper or electronic – should be organised in a uniform, logical way, so that they can be easily and speedily retrieved (allowing enquiries to be answered promptly and in line with statutory timescales). A classification scheme or filing structure should be devised (based on an analysis of each department's business functions and activities) to ensure that documents are grouped appropriately and consistently. It is important that only items of a similar nature are placed together: if the contents of folders and the folders themselves are too diverse, it will be difficult not only to locate material, but also to assign appropriate retention periods.

Standardised referencing and titling are essential, so that information can be readily identified and retrieved. Departments should develop naming conventions and glossaries to ensure consistent terminology is used for (e.g.) activities, committees and organisations. In addition, the titles of electronic documents and folders, as well as the covers of paper files, should describe the content or subject matter accurately and helpfully.

2.3. Access and security

Information that is only accessible to a single person should be kept to a minimum: as far as possible records that other staff may require must be stored in a secure, shared area within a centralised filing system, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, data should also be shared across the University in order to avoid wasting resources recreating information that already exists and storing duplicate data unnecessarily.

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. Paper records containing confidential information must be stored in locked cabinets within locked rooms when not in use, and access only granted to authorised staff.

Access to restricted electronic data should be controlled through the use of log-ins, multi-factor authentication, passwords and, if appropriate, encryption. Computers must not be left unattended when logged on, even for short periods of time and staff should consider the use of privacy screens where any sensitive information on their screens may be visible to students or visitors to their department. In addition, information held in digital systems should be protected from accidental or unauthorised alteration, copying, movement or deletion. If possible, the systems should maintain audit trails allowing all actions to be traced to specific people, dates and times. It is essential that any data held on laptops, as well as portable storage devices (such as USB memory sticks, CDs, DVDs) where still in use, is kept securely (using encryption where necessary) and protected from theft.

2.4. Storage and preservation of records

Records need to be preserved in a usable state (protected from damage and obsolescence) throughout the current and semi-current phases of their life cycle.

This topic is now covered by section 5.3 of the Retention Policy (available on the University website).

Inactive records may also require preservation; if they are selected for permanent retention in the University Archives.

2.5. Retention and destruction of records

Departments should ensure the timely, secure destruction of information in accordance with retention schedules. This topic is now covered by section 6 of the Retention Policy (available on the University website).

2.6. Emails

Emails may record the University's actions and decisions, and must be managed as effectively as paper and other electronic records.

This topic is now covered by the Staff Email Policy (available on the University website).

2.7. Vital records

Records that would be vital to the continued functioning of the University in the event of a disaster (e.g. fire, flood, ICT cyber-attack) must be identified and protected. These include records that would recreate the University's legal and financial status, preserve its rights, and ensure that it continued to fulfil its obligations to its stakeholders (e.g. current financial information, current contracts, proof of ownership, current research information).

All critical business data must be stored in the correct corporate system, so that it will be protected by appropriate backup and disaster recovery procedures. Where vital records are only available in paper format it is best practice that they be duplicated, and the originals and copies stored in separate locations. If, however, duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect the documents.

2.8. Records management systems

There must be a clear allocation of responsibility within each department for all aspects of record-keeping, including classifying documents, applying retention schedules and discarding material. The ownership of information should also be clarified, so that there is no ambiguity regarding responsibility for its maintenance and disposal. Line managers should ensure that prior to a member of staff leaving, responsibility for his or her records is transferred to another person; and if any of the information is redundant, it should be deleted by either the departing member of staff or the line manager. For further guidance on the procedures to be followed when staff leave, please see 'Staff Access to University Facilities and Leavers' Procedures' (available on the University website).

Each department's records management systems should be adequately documented, so that their effective operation is not solely reliant upon the memory of individual members of staff. They should also be periodically reviewed and, if necessary, modified to ensure that they continue to support the needs of the department. In particular, electronic systems storing data that may be required for evidential purposes should be regularly monitored and audited: it must be possible to demonstrate the reliability of the system, so that the integrity of the data cannot be questioned.

2.8.1. The eRecords System

The eRecords system is available to all professional services and academic departments across the University for the storage of unstructured and semi-structured records with particular emphasis on those with 'corporate value'. All permanent and fixed-term staff now have an eRecords read-only account by default. Managers are still able to request an eRecords account for temporary staff via the New Starter form, or by contacting IS Service Desk. The system provides built-in version control auditability, ensuring that the most up to date information is available. Additionally the system presents a consistent approach to security permissions and retention schedules. All of which enables the University to be fully compliant with the requirement of Data Protection legislation and integrity.

Back record conversion of semi-current records (electronic or paper) retained by departments is at their discretion. However, if not migrated, departments must be capable of managing their records to the point of disposal in their current format and location.

Further guidance of eRecords can be found on the eRecords intranet page.

2.8.2. Google Drives

Whilst Google Drive provides document storage and the facility to share documents with others, each Google My Drive remains intrinsically linked to the individual. In addition to this, the University has no corporate oversight of, nor ability to manage the content of the Google My Drives or Shared Drives in accordance with legislative requirements. This makes Google Drive an unsuitable repository for University records.

Google Drive may be used for the drafting of records, but once completed these must be declared into the appropriate corporate system and then deleted from Google Drive. Further guidance on how to do this can be found on the Records Management Weeding Starter Pack intranet page under step 7.

2.8.3. Microsoft 365, Sharepoint, Teams etc

Over the coming years, the University will be transitioning gradually to Microsoft. It has not yet been determined how records management will apply to this environment. This section will be expanded in future policy updates. Meanwhile, please refer questions to the University Records Manager.

Glossary of records management terminology

Accountability:	The principle that individuals, organisations and the community are required to account to others for their actions. Organisations and their employees must be able to account to appropriate regulatory authorities and to the public to meet statutory obligations, audit requirements, relevant standards and codes of practice, and community expectations. (The National Archives: Model Action Plan for achieving compliance with the Lord Chancellor's Code of Practice for the Management of Records – HE and FE organisations 24 April 2002)
Appraisal:	Process to evaluate business activities to determine the archival worth or evidential value of a record in terms of the quality of its content in relation to stated objectives, standards or criteria. It identifies which records need to be captured and for how long the records need to be kept, to meet business needs, the requirement of organisational accountability. (The National Archives: Model Action Plan for achieving compliance with the Lord Chancellor's Code of Practice for the Management of Records – HE and FE organisations 24 April 2002)
Archives:	The term 'archive' is often used to describe records that are no longer in daily use and are stored separately from an office's current files (see semi-current). The term is also applied to records that are to be kept permanently because they have historical value (see the life cycle of records). Archives provide evidence of the University's most significant functions and activities, document its policy formation, and trace the development of its fabric and infrastructure (e.g. minutes and annual reports of the Board of Governors, strategic plans, financial reviews).
Authentic record:	An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; and created or sent when purported. (ISO 15489:2016 Records Management)
Classification:	The process of devising and applying schemes based on the business activities which generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal. Classification includes determining document or file naming conventions, user permissions and security restrictions on records. In broad terms it is the process by which records are categorised or grouped into retrieval units, whether by function, subject or other criteria. (The National Archives: Model Action Plan for achieving compliance with the Lord Chancellor's Code of Practice for the Management of Records – HE and FE organisations 24 April 2002)
Corporate value:	This is a term used within the Objective eRecords system to denote a record of significant value to the University of Portsmouth. A guide to the application of corporate value can be found within Records Management Factsheet 10 – eRecords.
Destruction:	Process of eliminating or deleting a record, beyond any possible reconstruction. (ISO 15489:2016 Records Management)

Electronic records:	Records processed and retrieved by a digital computer; these include text-based word-processed documents, email messages, spreadsheets, presentations, scanned documents, website and multimedia documents.
Integrity of records:	Records will have integrity if they are complete, unaltered and protected from unauthorised alterations. (ISO 15489:2016 Records Management)
Life cycle of records:	The life cycle of a record consists of three phases: **Current:** initially a record is current or active while it is used to carry out day-to-day work. **Semi-current:** a record becomes semi-current or semi-active when it only needs to be referred to occasionally or has to be retained for a time to comply with legal or regulatory requirements. **Inactive:** finally a record becomes inactive and a decision has to be made whether to discard it or keep it permanently because it has historical value.
Metadata:	Descriptive and technical documentation to enable a system and its records to be understood and operated efficiently, and to provide an administrative context for the effective management of the records. (The National Archives: Model Action Plan for achieving compliance with the Lord Chancellor's Code of Practice for the Management of Records – HE and FE organisations 24 April 2002)
Migration:	Process of moving records from one hardware or software configuration to another without changing the format. (ISO 15489:2016 Records Management)
Paper records:	Records in the form of folders, files, volumes, plans, charts etc. (i.e. not in electronic form).
Preservation:	Processes and operations involved in ensuring the technical and intellectual survival of authentic, useable records through time.
Record:	Information created, received and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations on in the transaction of business. (ISO 15489:2016 Records Management). Records may be in any format (e.g. paper, fax, drawing, plan, video, photo, slide, microfilm, audio recording, CD, email). Records can be sub-divided into three categories: **Structured:** records held as data in structured, relational databases. **Semi-structured**: records wherein the layout, composition and content are constrained by the use of approved templates (e.g. forms), to such a degree that a computer could be scripted to identify specific content blocks and take action based upon them (e.g. OCR/ICR, metadata extraction, process automation). **Unstructured:** records where the lay-out, composition and content are at the discretion of the author.
Records management:	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (ISO 15489:2016 Records Management)
Records system:	Information system which captures, manages and provides access to records over time. (ISO 15489:2016 Records Management)

Reliable record:	A record is considered reliable if its contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities. (ISO 15489:2016 Records Management)
Retention schedule:	Document setting out the length of time for which categories or series of records should be kept according to legal, regulatory, business and operational requirements.
Review:	Process of examining records and assessing whether and for how long they should be retained.
Usable record:	A usable record is one that can be located, retrieved, presented and interpreted within a time period deemed reasonable by stakeholders. It should be connected to the business process or transaction that produced it. (ISO 15489:2016 Records Management)
Version control:	A process that allows for the precise placing of individual versions of documents within a continuum. (The National Archives: Model Action Plan for achieving compliance with the Lord Chancellor's Code of Practice for the Management of Records – HE and FE organisations 24 April 2002)
Vital records:	Records that contain information needed to re-establish an organisation in the event of a disaster. They are likely to be unique/irreplaceable or required immediately following a disaster. They will provide information for continuing/resuming operations, recreating legal and financial status of an organisation or preserving the rights of an organisation or fulfilling its obligations to its stakeholders.

University of Portsmouth
Corporate Governance
University House
Winston Churchill Avenue
Portsmouth PO1 2UP
United Kingdom

T: +44 (0)23 9284 3195

E: corporate-governance@port.ac.uk
W: www.port.ac.uk