Records Management Policy

Policy Name – Records Management Policy	
Version number: 1.0	
Policy Owner	**Policy Author/Reviewer**
The Deputy Chief Digital and Information Officer	Digital Records Manager ICT Governance
Approving body	**Date of approval**
Information Services Directorate (approved on 27.05.20) and Digital Strategy Steering Committee (approved 22.09.2020)	22 September 2020
	Equality Screened
	Yes
	Next Review date
	January 2025
Queries relating to this document should be directed to the Policy Owner – Digital Records Manager – recordsmanagement@ulster.ac.uk This document can be made available on request, in alternative formats and in minority languages to meet the needs of those who are not fluent in English.	

Introduction

Records management is the process of managing records, in any medium, from creation to disposal. These records, whether in paper or electronic format, are a vital University asset. They provide evidence of its actions and decisions and must be managed actively and systematically at all times, to ensure transparency, accountability and legal and regulatory compliance.

Scope

This policy applies to Ulster University staff, students, agency staff, visitors, contractors and third-party users. This policy applies to all records created, captured, maintained, used or destroyed by Ulster University across its core activities of research, learning and teaching; and all supporting activities which it undertakes.

Records are defined as documents, information or data created, received and maintained as evidence and as an asset by the University in pursuit of its legal obligations or in the transaction of its activities.

Records are subject to the University retention schedule requirements. All records, regardless of their form or the system in which they are captured, created or maintained are covered by this policy.

Aims

The aims of this record management policy are to ensure that:

- Accountability – records are maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy
- Quality - records are complete, accurate, the information they contain is reliable and their authenticity can be guaranteed.
- Accessibility - records and the information in them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the University. In line with Paper-Lite Objective, staff will be encouraged to digitize records. This will improve access for users with a disability.
- Security - records are secure from unauthorised or inadvertent alteration or erasure. Access and disclosure will be properly controlled, and audit trails will track all use and changes. Records will be held in a robust format, which remains readable for as long as records are required.
- Retention & Disposal – records are retained and disposed of appropriately using documented retention and disposal procedures (in line with Paper-Lite Objective to reduce volume of existing and new paper held by at least 85%).
- Performance Measurement - the application of records management procedures is regularly monitored against agreed indicators and action taken to improve the overall function

- Training – all users are trained and made aware of their responsibilities for recordkeeping and record management.

Relationship with Existing University Policies

The Records Management Policy should be read in conjunction with the following policies and guidance:

GDPR Policy
Records Retention and Disposal Schedule
Protective Marking Standard
Business Classification Scheme
Business Continuity Management
Using The University Archive

Responsibilities

The University has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment.

All persons engaged in University business - including all staff, casual staff, postgraduate researchers, secondees, agency workers, contractors, suppliers, partners, external researchers, visitors, honorary staff, and individuals undertaking volunteering or work experience - are required to adhere to this policy when creating, maintaining, using or disposing of records.

Individual schools, departments and offices must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with the University's records management guidelines. All records within a department or section should have an identified 'owner' responsible for their management whilst in regular use.

Standards

The following standards must be maintained at all times:

Records Capture/Creation

- Records must provide evidence of the actions and transactions that generated them, and they must serve as a trusted source for future decision making and information needs.
- Records must have certain attributes: they must be authentic, complete and usable.
- Unique identifiers should be assigned to the records so that will remain unchanged as long as the records exist (content management, naming convention, version control).
- Security and access controls should be applied during the process of capturing records to ensure that the records are protected from unauthorised

access, alteration and destruction/deletion (for example, SharePoint role permissions).

Records Maintenance

- Once records are created and captured, they must be maintained in such a way that their attributes of authenticity, reliability, completeness and usability are preserved for as long as the records are needed to serve the University's needs, and to meet legal and regulatory requirements.
- They must be organised, classified and described in a manner that facilitates their access and retrieval, and they must be protected to ensure that they are secure from unwarranted alteration and destruction (tracking systems to control movement/audit use of records)
- Systems in place to enable data subjects to make requests
- Arrangements for business continuity.
- The University's policy on retention and disposal should be applied to records during record creation.

Records Retention & Disposal

- Retention of records to comply with relevant legislative and policy requirements concerning the length of time records must remain in existence.
- Retention rules must be consistent for all forms of records.
- Retention rules must be applied to records and trigger the appropriate disposal event when the retention period expires.
- When records are due for disposal steps must be taken to ensure that they are deleted or destroyed properly.
- Storage systems for records requiring long-term retention to include electronic archiving.
- Mechanisms for regular transfer of records designated for permanent preservation to archive.

Performance Measurement

- Development of effective indicators and review systems to improve records management standards.

Training and Guidance

- Generic and specific guidance and training on records management standards and procedures.

Management of Records

Records Creation/Capture

A record is information created, received, maintained and disposed as evidence and information by the University or person, in pursuance of legal obligations or in the transaction of business. These records can be in paper or digital format.

The University has introduced a Protective Marking Scheme to provide guidance on the handling of Personal and Sensitive information, and also materials shared with third parties and subject to contractual or other controls.

Marking	**Rationale for Selection**
OPEN	These are considered documents that do not require classification for the purpose of information security. Unmarked material is considered open or unclassified. The protective marking 'Open' may also be used to explicitly indicate that this is the case.
PROJECT	These are considered documents that if compromised could: Cause distress to individuals • Breach proper undertakings to maintain the confidence of information provided by third parties • Breach statutory restrictions on the disclosure of information • Cause financial loss, loss of earning potential or could facilitate improper gain or advantage for individuals or companies • Prejudice the investigation or facilitate the commission of crime • Disadvantage the University in commercial or policy negotiations with others
CONTROL	Additional to those points included in the 'Protect' classification, these documents, if compromised could: • Cause "substantial" distress to individuals • Make it more difficult to maintain operational effectiveness • Impede the effective development or operation of University policies • Undermine the proper management of the public sector and its operations

Protectively marked material shall be marked in UPPERCASE LETTERS and shall be marked clearly in the document header and footer or where inappropriate to use header & footer, by means of a watermark.

Information gathered by the University on business systems will retain the Protective Marking of the system from which it is extracted when transferred to another format or document. Portability of information creates particular issues which need to be addressed with the information custodian - particular attention must be paid to safeguard against the risks presented by "secondary processing;" the use of information for purposes other than those for which it was volunteered.

Document Management System

All records created or received during University business are to be captured into an appropriate document management system. Naming the records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so, will facilitate the storage and retrieval of records, which will enable end users to browse file names more effectively and efficiently.

Naming records according to agreed conventions should also make file naming easier for colleagues, because they will not have to ‘re-think’ the process each time.

Records Maintenance

Audit Trails

Audit trails are the manual or electronic records that chronologically catalogue events or procedures to provide support documentation and history that is used to authenticate security and operational actions or mitigate challenges. These records provide proof of compliance and operational integrity. Audit trails can also identify areas of non-compliance by providing information for audit investigations.

Business Continuity

The University faces a variety of risks whether they are from external forces or internally. Internal risks arise both at the strategic (organisation-wide) level and at the operational (business process) level.

The objective of business continuity management is to ensure the uninterrupted availability of all key business resources to support essential (or critical) business activities. University records are covered by the Business Continuity Plan.

Records Retention & Disposal

Records must only be kept for as long as required to meet operational, business and legal needs. The University’s Records Retention Schedule is intended to provide guidance regarding appropriate retention periods for different categories record regardless of the record medium. The full Records Retentions and Disposal Schedule can be found here.

When a record reaches the end of its retention period a decision must be taken on its disposal.

- Permanent Preservation – send to University Archive
- Destruction

Paper Storage

The University will use an approved off-site document storage provider in cases where onsite storage is not appropriate.

Documents will be stored in a storage facility which meets all appropriate security and environmental standards.

Off-site storage will be used for documents that need to be retained for a length of time, but do not need to be accessed regularly.

University Archive

Originating departments should retain all records which they need for their own operational purposes for as long as they need them. Records should only be transferred to the University Archive when they cease to be operationally relevant.

Where it has been noted that records should be retained permanently by the University Archive, such records may eventually be deposited in the Public Record Office of Northern Ireland (PRONI) in accordance with any future strategy agreed between the University and PRONI.

A guide to the types of records that can be held in the University Archives can be found here.

Disposal

The record owner is responsible for ensuring records are destroyed in a timely and secure manner. All copies, including drafts, versions etc, held in any format must be destroyed at the same time.

Onsite Disposal

- White bags for general wastepaper, can be ordered for delivery and collection, using the Estates Services Helpdesk.
- Red bags for confidential waste to be shredded, can be ordered for delivery and collection, using the Estates Services Helpdesk.
- Hardware and backup media is disposed of twice yearly, and can be requested via Estates Services Helpdesk.

Off-site Disposal

The University will use an approved off-site document destruction provider in cases where onsite destruction is not appropriate.

Documents will be shredded in a manner which meets all appropriate security and environmental standards.

A certificate of destruction will be provided after every shred service.

Digital Records

When deleting digital records, ensure that all copies held in email folders, file shares, SharePoint, system recycle bin are also deleted. Deletion of an electronic file removes the link to the file, but it is possible that the file contents could still be retrieved using technical measures. Therefore, adequate security must continue to be applied to file locations and devices used to hold them until they have been fully expunged or wiped.

System backups will continue to hold copies of deleted digital records until such time that the backup is deleted.

Legislation, regulations and standards

This Records Management Policy should be read in conjunction with the following legislation, regulations and standards.

- The Public Records Act 1958
- General Data Protection Regulation 2018
- The Data Protection Act 1998
- The Freedom of Information Act 2000
- Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018

Contacts and Further Information

Advice and further information relating to this policy can be obtained from:

Name: Digital Records Manager

Email: recordsmanagement@ulster.ac.uk