RECORDS MANAGEMENT POLICY

1. INTRODUCTION

This Policy sets out the principles for ensuring that Keele University knows what information it holds, where it is, and can retrieve and distribute it efficiently.

1.1 Purpose

The University's records are a vital corporate asset: they provide evidence of its actions and decisions and must be managed actively and systematically to ensure transparency, accountability and legal compliance.

The principal aims of records management at the University are to:

i. protect the interests of the University, its staff, students and other stakeholders by maintaining high quality information for as long as it is required, and to ensure its timely and secure destruction;
ii. comply with statutory and regulatory requirements affecting the use and retention of records;
iii. support decision making, teaching and research by maintaining accurate and reliable documentation;
iv. support business efficiency and continuity by ensuring information can be quickly located and retrieved and protecting information that is vital to the continued functioning of the University;
v. provide evidence in litigation, where required;
vi. prevent unauthorised or unlawful disclosure of information by ensuring records are held securely and access is controlled and managed;
vii. preserve historical records of the University for future administrative and research purposes.

1.2 Scope

This policy:

- Is binding on all those who create or use University records such as staff, students, contractors, consultants, visitors and guests of the University, whether accessing records on or off-campus;
- Applies to all records in electronic or hard copy format that are created, received and maintained by University staff in the course of carrying out their role;

- Includes records created, received and maintained in the course of research, whether internally or externally-funded, in addition to any contractual and academic record-keeping requirements;
- Applies in all parts of the organisation including any records held by institutions partnered with the University;
- Applies when information is held by others on behalf of the University; for example where a Data Processor processes information on the instruction of the University, such as a contracted parking management company.

When information is held by the University solely on behalf of another person or organisation, for example where the University is acting as a Data Processor for research data under the instruction of another Institution, it is excluded from the scope of this policy.

2. POLICY

2.1 Definitions

a) Record	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
b) Records Management	Controlling records within a comprehensive regime made up of policies, procedures, systems, processes and behaviours; these ensure that reliable evidence of actions and decisions is kept and remains available for reference and use when needed, and that the organisation benefits from effective management of one of its key assets, its records.
c) Retention Schedule	A list of types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of or transfer records to historical archives.
d) Records System	An information system which captures, manages and provides access to records through time.

2.2 Records Creation

Where records are created or held, they must contain relevant content, sufficient contextual information, integrity and authenticity to ensure the University complies with any legal or regulatory requirements including those set out in Section 4.

Records must be created or held in a durable form that will enable the University to access them for the full length of their retention period.

Where records created or held contain personal information this information must be relevant to the original purpose for which it was collected and must not be excessive.

Information should be compiled at the time of the event or matter to which it relates, or as soon as possible afterwards.

Where the University's processes are changed, or new processes established, due consideration must be given to the University's compliance with any legal and regulatory requirements to ensure an auditable record of such changes.

Records management considerations should be appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data there is a legislative requirement to do this to ensure that a data protection by design and default approach is followed.

2.3 Records Maintenance

Records must be categorised, handled and stored in accordance with the University Data Classification and Handling Policy.

Suitable controls or systems should be in place to protect the authenticity, reliability, integrity and usability of records. Such controls and / or systems should protect records from unauthorised access, change, loss or destruction.

To enable knowledge sharing, business continuity and collaboration, records should be accessible to those who require access (whilst complying with the University's Data Classification and Handling Policy).

Records must be maintained to ensure accessibility and usability for as long as required, this may require the migration of records to newer formats or systems. Where migration is carried out, sufficient safeguards must be taken and documented to ensure authenticity, reliability and integrity of the records are maintained.

2.4 Records Retention

Records must be retained in line with the University's Records Retention Schedule, to ensure that records are retained for no longer than is necessary for the University's business needs.

Unless they have historical value and / or relevant exemptions apply, personal information must not be kept for longer than necessary.

2.5 Records Disposition

Records should be reviewed at regular intervals, usually annually. Records must be destroyed in line with the University's Records Retention Schedule.

The means of disposal of records will be identified via the University's Data Classification and Handling Policy.

As good practice, destruction of records should be authorised by the appropriate manager and documented. Duplicates made for working purposes should be kept only for as long as required and then destroyed. Duplicates should be avoided wherever possible with the duplicate never being kept for longer than the original record.

Where records are scheduled for destruction, but are subject to a Freedom of Information, Environmental Information or Information Rights Request, destruction must be delayed until the request has been concluded, in line with legislative requirements.

Records must not be destroyed if they are required in connection with an on-going or pending investigation, grievance, complaint or legal dispute.

2.6 Vital Records

Records that would be vital to the continued functioning of the University in the event of a disaster (e.g. fire, flood, 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 continues to fulfil its obligations to its stakeholders (e.g. current financial information, legal documents, research data and core student data).

Vital records must be stored on central servers, so that they are protected by appropriate back-up and disaster recovery procedures. Vital records that are only available in paper format should be duplicated, and the originals and copies stored in separate locations. If however, duplication is impracticable or legally unacceptable, such as the destruction of a deed, necessary protective measures should be implemented.

3. ROLES AND RESPONSIBILITIES

3.1 All information users are responsible for creating, maintaining, and preserving records to which they have access in accordance with this Policy.

3.2 All staff are responsible for ensuring the security and where applicable the confidentiality of University property and all University information, files, documents, data etc. within their possession or to which they have access, including both paper and electronic material.

3.3 Information Asset Owners are responsible for ensuring that all records in their area are managed and disposed of in conformance with this Policy.

3.4 Information Asset Managers are responsible for day-to-day management of records, created received and maintained by the University in their respective areas.

3.5 Information Governance Champions support and implement best practice in records management across their areas.

4. RELEVANT LEGISLATION

When considering Records Management. the University is subject to the provisions of the:

GDPR / UK GDPR
Data Protection Act 2018
Freedom of Information Act 2000
Environmental Information Regulations 2004
Reuse of Public Sector Information Regulations 2015

This is not an exhaustive list of legislation affecting Records Management within the University as different business functions and activities are also subject to specific legislation or regulations, or

to professional best practice or relevant ethical guidelines, for example, employment law, health and safety legislation and financial legislation.

The University will, so far as is practicable, seek to comply with relevant external documentation, such as guidance material from The National Archives, codes of practice, and other guidance material from the Information Commissioner. It will co-operate with other higher education institutions and other relevant public authorities with the aim of benefiting from best practice experience.

5. RELATED POLICIES AND PROCEDURES

This Policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including without limitation our:

- Data Protection Policy.
- Information Security Policy.
- Freedom of Information Policy
- Records Retention Schedule
- Data Classification and Handling Policy
- Appropriate Policy Document
- Information Governance Framework

6. REVIEW, APPROVAL & PUBLICATION

6.1 Review This Policy will be reviewed and agreed by the University Executive Committee before final approval.

6.2 Final Approval This Policy will require final approval from Council.

6.3 Publication This Policy will be published on the website within the Policy Zone. The University's Information Governance web pages will maintain prominent links to this Policy as appropriate on both external and internal facing pages.

7. DOCUMENT CONTROL INFORMATION

Document Name	Records Management Policy
Owner	Director of Legal, Governance & Compliance
Version Number	V1.5
Equality Analysis Form Submission Date	NA
Approval Date	16/9/2021
Approved By	Council
Date of Commencement	16/9/2021
Date of Last Review	May 2021
Date for Next Review	16/9/2024
Related University Policy Documents	Data Protection Policy Appropriate Policy Records Retention Schedule Data Classification & Handling Policy Information Security Policy

	Freedom of Information Policy Information Governance Framework
Administrative update	10/03/2022; Head of Legal, Governance & Compliance updated to Director of Legal, Governance & Compliance
For Office Use – Keywords for search function	