University of Liverpool

Information Management Policy

Reference Number	CSD-020
Title	University of Liverpool Information Management Policy
Version Number	9.0
Document Status	Active
Document Classification	Public
Effective Date	01 July 2024
Effective Date	30 June 2025
Author	Michelle Alexander, University Information & Records Manager
Signatories:	Information Governance Committee
Implemented by	See Section 2 Responsibilities
Comments	Based on Records Management and Records Retention policies that were approved by Senate on 27 June 2012. Known as Records Management Policy until June 2019.

1. Scope

1.1 The University of Liverpool recognises that **appropriate creation of and efficient management of its information is essential** for effective administration and to meet strategic aims and objectives, to provide evidence of the transactions and activities of the University and to enable it to comply with legal and regulatory requirements. This is particularly important during times of significant organisational change or if part or the whole of the University ever ceased to operate.

1.2 This policy applies to all University information; that is **information created, received or maintained by the University as a result of its activities**, including the carrying out of research and the fulfilment of compliance with any regulatory requirements.

1.3 The information may be **structured or unstructured and held in any format or medium**, including hard copy, electronic documents, emails, chat messages, texts, audio and video, maps or plans and social media channels. It may also be **stored, managed or hosted elsewhere**, on various systems, apps and software, including cloud-based services, personal devices and removable media, and any such arrangements must comply with this policy.

1.4 A small proportion of the University's information may be selected for **permanent preservation** in the University archives to be available for historical research and to give a lasting record of the University's business.

2. Responsibilities

2.1 The **Information Governance Committee (IGC)** is responsible for approving each version of the policy, encouraging its implementation and communicating about good information management to all University staff.

2.2 **Heads of Operations/ Deans and Heads of Professional Services Departments** (or their nominated representatives) are responsible to the Senior Leadership Team for the implementation of this policy within the University of Liverpool.

2.3 The **University Information & Records Manager** is responsible for maintaining the policy and for promoting and supporting best practice across the University.

2.4 **Records Liaison Officers** in each area of the University are responsible for following best practice in using the Information & Records Management services and may also be well placed to assist with promoting best practice and facilitating good communication between their area and Information & Records Management in support of this policy.

2.5 **All members of staff** are responsible for following this policy and specifically for:

- being aware that the policy covers all information created, received or maintained by them in the course of their duties, including carrying out research for internally or externally funded projects
- completing the **mandatory training** module on Data Protection and Information Security and being aware of the key policies listed in Section 4
- ensuring the **creation of accurate records** that document the actions and decisions for which they are responsible
- **storing information appropriately and securely**, in particular using IT Services centrally managed IT facilities and services as per the IT Acceptable Use Policy (see Section 4 below)
- ensuring that **new systems or software comply** with this policy and the Information Security Policy (see section 4), particularly if it is managed locally; also being compliant during the decommissioning of systems or when migrating data between systems
- taking particular care with **vital records** (i.e. those required for the continued functioning of the University in the event of a disaster)
- taking particular care with records containing **personal and sensitive information**
- **identifying obsolete information** and disposing of it in an appropriate, secure and, if necessary, auditable manner

2.6 Where relevant, **other parties**, including students, contractors, consultants and visitors should be made aware of their responsibilities under this policy. Service level agreements and contracts with third party providers must ensure compliance with the policy and this should be regularly reviewed.

3. Aims and objectives

3.1 The UK implementation of the international standard on records management, which this policy is aligned with (but not certified to), states,

'Managing records encompasses the following:

a) creating and capturing records to meet requirements for evidence of business activity;
b) taking appropriate action to protect their authenticity, reliability, integrity and useability as their business context and requirements for their management change over time.'[1]

3.2 By managing information and records well, the University will be able to:

- **fully exploit its information** as a corporate resource and use it to support business decisions, policy formation and evidence-based research and development

- provide **transparent and accountable evidence** and information about policies and compliance, transactions, interaction with stakeholders and rights and obligations of individuals and organisations

- work in the **most efficient way**, for example by staff being able to retrieve up-to-date and accurate information in a timely manner

- retain information **required by law**, in particular records relating to financial and environmental concerns, health and safety and contractual agreements

- comply with **regulations and legislation**, including Data Protection and Freedom of Information

- protect and defend its **rights**, including intellectual property rights and in litigation

- be better prepared in terms of **business continuity and risk management**

- demonstrate **previous compliance** with correct procedures

- **free up physical and electronic storage space and staff time**, thus contributing towards the University's strategic objectives, including around sustainability

- record the **business and cultural identity** of the University, ensuring that information with **historical value or interest** to the University and wider world is retained and preserved.

4. Implementation and resources

4.1 In order to ensure compliance with this policy, departments must ensure that all staff have done the mandatory online training in Data Protection and Information Security and that they are given the time and resources needed to manage information effectively.

4.2 In practice this means every member of staff taking responsibility for the activities in the lefthand column below and departments creating **supplementary local procedures** as described in the righthand column setting out what staff need to do in terms of creating, storing, sharing and disposing of information, using the resources listed below and the support of the Information & Records Management team as required:

Steps needed for good information management:	**Supported by local procedures covering:**
Consistently capture information to give **accurate and relevant evidence** of the University's activities... ...whilst routinely **disposing of short term or ephemeral** items and **avoiding unnecessary duplication**	• what information needs to be captured and what does not need to be created or retained beyond its immediate use • what formats are appropriate • who is responsible for capturing and storing information to avoid duplication
Store and share that information **appropriately**, in a way that facilitates **quick and easy retrieval** of **authentic, accurate and up-to-date** information by those that need to access it... ...and also meets **information security and legislative requirements** and **protects** it from **unauthorised access or loss/ damage**	• where things should be stored so that they are secure from unauthorised access but can be used by those staff that need them • reminding staff to use the Data Protection Policy and the Information Protection Guide
Retain the information in line with the **University retention schedule** (which lists all information types in the University, with how long they should be retained to meet operational and regulatory requirements and the reasons for that retention period) for **as long as it is required**... ...and then **review once the information is no longer needed** for current business purposes to decide whether to **dispose of it appropriately** or transfer it to the **University Archives**	• reminders to follow the **University Records Retention Schedule** (or to document an approved exemption if necessary) • processes for **regular reviews,** at an appropriate point, of information on University systems and servers, records held in the University Records Centre and **local paper and electronic files** to ensure things are kept as long as required but no longer. • processes for **disposing of records appropriately** (see 4.3 below)

4.3 Specifically in terms of **disposing of records**, it is strongly advised any personal or residual information or data that has no value or is no longer required for University purposes should be removed from relevant systems, drives and servers regularly, at least annually. When disposing of information, paper files should be shredded with a cross-cut shredder or disposed of via the confidential waste disposal service through Information & Records Management. Removable media, such as USB sticks, disks etc., can also be disposed of via this service if packaged separately and arranged in advance. Data-bearing assets, such as hard drives, laptops and PCs, should be disposed of via the IT Services Asset Disposal service.

5. Related policies, guidance and contacts

5.1 Further details on information management, including a link to the **retention schedule** and **guidance on specific topics** is available from the Information & Records Management website. This guidance covers topics such as the following:

- Records creation
- Electronic records management
- Email management
- Guidance on specific record types including student files and assessed work, research data and committee records
- Filing schemes and version control
- Office detox, office moves and staff leaving
- Retention periods for records
- Storage options for records
- Destruction options for records
- Archival records selection

5.2 This policy should be used in conjunction with **other relevant University policies** and guidance, including but not limited to:

- Data Protection and Freedom of Information Policies
- University Records Retention Schedule and Information & Records Management Service Level Agreement
- Information security policy, supported by the IT Acceptable Use Policy and the Information Protection Guide
- Research Data Management Policy

5.3 Departments must ensure their records comply with any **external guidelines, policies or legislation**, including but not limited to UK Data Protection, Freedom of Information and Environmental Information legislation, requirements of research councils, ERDF, other funders, auditors, accreditation bodies and regulators, including the Office for Students.

5.4 Any **queries or proposed amendments** should be referred to the University Information & Records Manager: Michelle Alexander m.alexander@liverpool.ac.uk