Liverpool Hope University

Information Management Policy

Document Control

Date	Revision/Amendment Details & Reason	Author
July 2013	Approved by University Council (entitled Records Management Policy)	G Donelan
February 2017	Updated to Information Management Policy	M Beecroft
December 2018	Updated to include references to GDPR	M Beecroft
February 2019	Annual Review	M Beecroft
February 2020	Annual Review	M Beecroft

1. Introduction

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 contribute to the effective overall management of the institution. The policy seeks to balance the need to store information with legal obligations to destroy the data safely when it is no longer required.

2. Scope of the policy

2.1 This policy applies to all information created, received or maintained by staff of the institution in the course of carrying out their teaching, assessment, scholarly, administrative or management functions.

2.2 Records are defined as all those documents, which facilitate the business carried out by the University and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy, electronically or held on film, microfiche or other media...

2.3 A small percentage of the University's records will be selected for permanent preservation as part of the institution's archives, for historical research and as an enduring record of the conduct of business. Some records may be retained to substantiate the detail of employment relationships.

2.4 The policy applies to all staff and students of the University and to other users associated with the University. With regard to electronic systems, it applies to use of University owned facilities and privately / externally owned systems when connected to the University network directly or indirectly.

2.5 The policy applies to all University owned / licensed data and software whether loaded on University or privately / externally owned systems, and to all data and software provided to the University by sponsors or external agencies.

3. Responsibilities

3.1 The University has a corporate responsibility to maintain its records and recordkeeping systems in accordance with the regulatory environment. The Head of Legal Services, Governance and Risk has overall responsibility for this policy and any queries about the operation of this policy should be directed to the Head of Legal Services, Governance and Risk.

3.2 Rectorate Team members, senior managers and individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the University's information management guidelines.

4. Legal and Regulatory requirements

The University will abide by all UK legislation and relevant legislation of the European Community relating to the holding and processing of information. This includes the following:-

- Data Protection Act 2018
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Freedom of Information Act 2000
- Copyright Designs and Patents Act 1988

In addition, the storage, processing and transmission of payment card information must be conducted in accordance with Payment Card Industry Data Security Standards (PCI DSS) mandatory

requirements.

5. Storage

All records should be stored with due regard for appropriateness, efficiency, cost effectiveness and security. It is the intention of the University to digitise information where possible and when resources allow.

Confidential and sensitive records should be stored securely, in locked cabinets if held in hard copy and in line with the Information Security Policy if held electronically.

6. Disposal of Information

Personal, confidential and business critical information must be disposed of in a secure manner.

For paper information, items should ideally be cross-shredded onsite and placed in a confidential waste unit.

For electronic information:-

- DVDs / CDs should be shredded and then put into a recycling unit
- Computer hard drives and external storage media (USB, detachable hard drives etc) should be wiped with a suitable software tool. No unencrypted data should remain on these types of media before re-using / recycling / disposal
- Media that cannot be wiped initially will need to be protected before being overwritten e.g. storage tapes should be kept in a locked safe

7. Policy Awareness and Disciplinary Procedures

This policy will be made available to all staff and students via the governance section of the University website maintained by the Head of Legal Services, Governance and Risk Office. Staff, students, authorized third parties and contractors given access to University information will be advised of the existence of the relevant policies, codes of conduct and guidelines.

Failure to comply with the policy may lead to suspension or withdrawal of an individual's access to information systems.

8. Retention periods

Records should be disposed of in accordance with the following agreed retention schedules. At the expiration of their currency, records should be destroyed securely or, if they have lasting historical value, added to the University archives. There may be specific archives, for example, employment related records held in Personnel.

8.1 Financial Records

The Finance Office will retain records for the following periods

Accounting Records (e.g. purchase orders, invoices)	Current financial year plus six years
Payroll Records	Current financial year plus six years
Insurance Records	Current financial year plus six years

Financial Statements	Retained indefinitely
External Project records	Minimum of current financial year plus six years, although if funder requires longer retention then this will be complied with. For External Projects with European Funding, the retention period is the year of the Official EU Programme Closure letter plus 3 years

8.2 Personnel Records

The Personnel Office will retain records for the following periods

Staff personal files	Up to six years after member of staff leaves employment. N.B, Basic data may be kept on electronic system (CIPHR) indefinitely in order to substantiate the employment relationship
Recruitment files	Twelve months after recruitment exercise for unsuccessful candidates; details for successful candidate will be on personal file

8.3 Building & Estates Records

The Estates Office will retain records relating to buildings (i.e. Property Terriers and Health & Safety files) whilst the University has ownership or occupancy of such buildings. The files will be transferred to the new owner on completion of sale/transfer.

Records relating to construction projects will be retained for six years in line with the Financial Regulations.

8.4 Student and Curriculum Records

Student Records will be retained in line with the already agreed Archiving Policy for Student and Curriculum Data.

8.5 Governance and Management Records

The University Secretary's Office will retain indefinitely the following corporate documents:-

- University Council agendas, minutes and papers
- University Council Committees agendas, minutes and papers Senate and Senate Committee agendas, minutes and papers
- Rectorate Team, Senior Management Team and Heads of Department agendas, minutes and

papers.
- All Audit and Inspection reports

8.6 Electronic information not included above

Type of information	Retention Period
Student Personal Network Drive	12 months after the date of graduating or ceasing studies
Staff Personal Network Drives	12 months after the date of leaving – annual backup copies are kept in the safe for emergency retrieval
SITS	Indefinitely due to the need to link student records together irrespective of the time between study
Moodle	5 years after the creation of the Moodle for a particular academic year
Kinetics	5 years after the academic year for which the data applies
CIPHR	6 years
Academic Profile System	Indefinitely
Agresso	Current financial year plus six years
Building Access – Salto	12 months
Ceridian	Current financial year plus six years
Health Questionnaire	5 years after the academic year when the data was collected
Performance Review	5 years from the end of employment

9. Policy Review

This policy will be reviewed on an annual basis to identify any required revisions.

References

JISC best practice guidance: www.jiscinfonet.ac.uk/infokits/records-management

CIMTECH Managing Information and Records guide [2013 edition]:
http://www.herts.ac.uk/cimtech/publications/the-cimtech-guide

Information Commissioner's Office guidance:

http://www.ico.org.uk/for_organisations/sector_guides/education

http://www.ico.org.uk/for_organisations/freedom_of_information/guide

http://www.ico.org.uk/for_organisations/data_protection/the_guide

http://www.ico.org.uk/for_organisations/environmental_information/guide

http://www.ico.org.uk/for_organisations/privacy_and_electronic_communications/the_guide

Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000. Revised and re-issued July 2009:
http://www.nationalarchives.gov.uk/documents/information-management/foi-section-46-code-of-practice.pdf