University of Central Lancashire

Information management policy

Approved: 07/05/2019

Document control information

Classification	Internal and external
Responsibility for drafting	Corporate Records Manager
Consulted with	Information Security and Data Quality Group
Approved by	Pro Vice-Chancellor & Registrar (Corporate Development)
Effective from	May 2019
Enquiries to	Corporate Records Manager

This document is issued by Legal and Governance. Any copied or printed versions will be an uncontrolled copy. The definitive version is available from the Corporate Records Manager: DPFOIA@uclan.ac.uk

Contents

A Introduction 4
B Scope of the policy 4
C Effective information management....5
C.1 Actively manage information....5
C.2 Identify and preserve appropriate records....5
C.3 Store information appropriately....5
C.4 Set standards to govern access to information 6
C.5 Identify information assets 6
D Responsibilities 6
D.1 University Secretary & General Counsel 6
D.2 Directors and Heads of Schools....7
D.3 Information Asset Owners 7
D.4 All staff, contractors, volunteers, etc. to whom this policy applies 7
E Relationships with existing policies and obligations 7
F Further Resources 8
G Breach of the policy 8
H Glossary of terms....9

University of Central Lancashire
Information management policy

A Introduction

Information is a valuable asset and forms the basis on which decisions are made and services provided. Effective information management results in the creation of accurate, reliable information, which is appropriately stored, processed, and protected in line with legislative and regulatory requirements, and operational needs.

The University's information assets are made up of data and records. 'Data' can be defined as numbers, words or images that have the potential to be organised or analysed to present a specific view or answer a question. Unlike data, 'records' contain content, context and structure and can be defined as information created, received and maintained as evidence to document activities and decisions. The availability of good quality data and records enables the University to carry out its fundamental role as a higher education and research institution.

Good information management also supports compliance with the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 and data protection legislation – the Data Protection Act 2018 and the General Data Protection Regulation – by ensuring that information is available to the right people at the right time and ensuring that information, particularly personal data as defined by data protection legislation, is not kept for longer than is necessary. Disposing of records that are no longer required also decreases the cost of storage and reduces the risk of using out of date data.

This policy sets out how the University will ensure its information is managed effectively. It documents the actions required for effective information management, the roles and responsibilities of key parties and lists the further resources available to support the implementation of this policy.

This policy is reviewed regularly by the Corporate Records Manager, on behalf of the University Secretary and General Counsel. Recommendations for any amendments should be reported to the Corporate Records Manager for consideration as part of the review process. The University will continue to review the effectiveness of this policy to ensure it is achieving its stated objectives.

A glossary of terms used in this Policy can be found in section H.

B Scope of the policy

This Policy applies to all employees including temporary, casual, contract and agency staff, contractors or service providers acting on behalf of the University and to volunteers. Responsibilities are outlined in section D.

This policy applies to all information created, received or maintained by the University in the course of carrying out its business, including organisational, research and teaching information. This includes information held, managed or produced by third parties on behalf of the University, including contractors and partners. All such information remains under the ownership of the University. Information and records created through partnerships are also subject to contractual record keeping requirements.

It covers information stored in all formats and media including but not limited to electronic, digital and physical forms, and covers all classifications including public, internal and confidential/sensitive information (including personal data).

C Effective information management

The University is committed to creating and maintaining information that supports and documents its activities, to good information governance, and to complying with legal and statutory requirements, in particular the FOIA and data protection legislation. Information forms our corporate memory and is an important organisational asset.

To uphold this commitment, the University will do the following:

C.1 Actively manage information

Information will be actively managed from creation to disposal, in line with the University Retention Schedule. The Retention Schedule lists the types of information produced and received through University activities and identifies the period of time for which this information must be retained. The retention period is based on legal, contractual or regulatory requirements where applicable, and on operational needs and sector guidance where there are no such requirements. The rationale behind the retention period is included in the schedule. The University recognises that legal requirements concerning retention take primacy. All data, records and information will be created, stored and maintained with the understanding that there are statutory and organisational requirements specifying how long it should be retained, and all responsible staff will undertake activities to ensure these requirements are met. Information will not be retained indefinitely but regular action will be taken to audit records and identify those that should be disposed of.

C.2 Identify and preserve appropriate records

The University will ensure the identification and preservation of records that form its history. In line with the Retention Schedule a small proportion of the University's information may be selected for permanent preservation in the University archives, to maintain its corporate memory and be made available for historical research. Information of potential Archival value will be identified and should be recorded on the Information Asset Resister (see C.5).

C.3 Store information appropriately

Information will be stored in a facility which is secure, effective and reliable. This means information will be stored in the appropriate University system or repository, and not

elsewhere. University recordkeeping systems and databases will ensure the secure storage of information, records and data to support their integrity and reliability. Recordkeeping systems should be utilised to support compliance with the Retention Schedule (see C.1). Regular backup and auditing actions will be undertaken to ensure the continuing accessibility and preservation of electronic records. The effectiveness of information management within all recordkeeping systems and databases will be reviewed on a regular basis and required changes will be implemented. Consistent rules will be applied to the storage and maintenance of information across services.

C.4 Set standards to govern access to information

Principles and standards which govern access to information will be set. Standards will be based on risk, sensitivity and confidentiality. Access controls will be in place to ensure the right people have access to the right records at the right time. This means information which should be made public will be, information which is internal to the University will be available to those who have a valid interest in it, and sensitive or confidential information will be restricted as required. Where information is shared with third parties, information sharing agreements or data processor contracts will be implemented where necessary, taking advice from Legal and Governance. Concerns regarding access to information should be reported (see G).

C.5 Identify information assets

The University will identify vital information assets which will be described on documents called Information Asset Registers. These will be maintained for each Service and Faculty and reviewed on a regular basis and made available to the relevant business areas. The register is an inventory of the University's information assets and specifies where these assets are stored, who owns and manages them, and other information pertinent to ensuring that the information is being handled appropriately. Additional information is captured in relation to personal data, to ensure that the requirements of data protection legislation are met. Information Asset Owners are recorded on the University Information Asset Register.

D Responsibilities

The University has a responsibility to maintain data and datasets, records, record-keeping systems and information sets in accordance with the law and the regulatory environment. This includes the FOIA, data protection legislation, the Limitation Act 1980 and the wider legislative environment and requirements of relevant regulatory bodies.

Staff and operational areas have responsibilities to ensure the effective management of the University's information, as follows:

D.1 University Secretary & General Counsel

The University Secretary & General Counsel has overall responsibility for ensuring the University manages its information effectively and complies with this policy. The University Secretary & General Counsel is supported in this responsibility by the Corporate Records Manager, who is based in Legal and Governance and can be contacted at

DPFOIA@uclan.ac.uk. Any questions or concerns about the operation of this policy or requests for training or support should be referred in the first instance to the Corporate Records Manager.

D.2 Directors and Heads of Schools

Schools and Services will implement practices to ensure compliance with this policy and review them regularly. Directors and Heads of Schools have a responsibility to ensure the information created and used by their School or Service is being managed in accordance with the requirements laid out in section C.

D.3 Information Asset Owners

Information Asset Owners (IAO) have been appointed in Services and Faculties across the University. It is the responsibility of the named IAO to ensure that good housekeeping practices are undertaken to ensure the accuracy, security and relevance of information assets that reside on the University servers and in University storage areas. The IAO will ensure information assets are managed in line with the requirements laid out in section C. The IAO is responsible for identifying valuable information assets in their Service or School and ensuring their inclusion on the Information Asset Register (see C.5).

D.4 All staff, contractors, volunteers, etc. to whom this policy applies

All staff have a responsibility to ensure they create and maintain records in accordance with this policy and other relevant University policies. All staff are responsible for ensuring they create accurate records that document the actions and decisions for which they are responsible and maintain those records in accordance with the standards laid down in this policy. This includes storing records appropriately and securely, identifying obsolete records and disposing of them in an appropriate and, if necessary, an auditable manner. All staff have a responsibility to be aware of the information management requirements of the University, and to seek guidance if they are unsure of how information should be processed, stored, shared or disposed of (see F). Furthermore, all staff have a responsibility to raise any concerns relating to information management practice in the University (see G).

E Relationships with existing policies and obligations

This policy should be used in conjunction with other relevant University policies, procedures and guidance including:

- Data Protection Policy
- Freedom of Information Policy
- University Records Retention Schedule
- Information Security Policy
- IT Security Policy
- Email Use Policy
- Research Data Management Policy
- Information Categories Guidance

All parts of the University should also ensure their information management practices comply with:

- Contractual obligations;
- Requirements of statutory audits;
- Requirements of the research councils and any other funders of research activities;
- Obligations under the Freedom of Information Act 2000 (FOIA), Environmental Information Regulations 2004 and data protection legislation – the Data Protection Act 2018 and the General Data Protection Regulation.

F Further Resources

Further resources to support the Information Asset Owner and all staff in managing information and records are available on the Information Governance intranet pages. These resources relate to electronic and physical information management. Guidance and training resources are reviewed on an annual basis to ensure they reflect current best practice and to incorporate any frequently asked questions.

Any requests for further resources and guidance should be referred to the Corporate Records Manager.

G Breach of the policy

If you are concerned that this policy has not been followed you should seek advice from the Corporate Records Manager. If you are aware of a data breach or incident, you should raise this matter through the Data Incident Reporting portal. Examples include but are not limited to:

- Disposal of information before it has reached the end of its retention period;
- Deliberate or accidental use of inaccurate or out of date data;
- Sharing of confidential or personal data with unauthorised third parties.

A member of the Information Governance team and/or the IT Security team as appropriate will review the information given and respond in line with the Information governance incident procedure.

Any staff member found to have knowingly breached this policy may be subject to disciplinary action. Further information on the disciplinary procedure is available on the Human Resources intranet pages.

H Glossary of terms

Data, information and records	Data, information and record are often used interchangeably. In this policy, a "record" is a grouping or collection of information to record a specific activity or decision, e.g. a book of committee minutes or an electronic student file. In comparison, information and data is often less formally structured and would include the contents of an individual's University email account or working documents. These are all covered by this policy. While records and personal data require additional care due to their greater value and risk, all information needs to be managed in order to be most effectively utilised by the University.
Information asset	A collection of data that enables an organisation to carry out its activities and as such is a valuable resource for meeting operational, regulatory and legislative requirements. Information assets can be in any format, including emails, databases, and paper files.
Information asset owner	The individual who has overall responsibility for ensuring that the information asset is being managed appropriately.
Information asset register	The information asset register is an inventory of the University's information assets and records where these assets are stored, who owns and manages them, and other information pertinent to ensuring that the information is being handled appropriately. Additional information is captured in relation to personal data, to ensure that the requirements of the General Data Protection Regulation are met.
Personal data	Data relating to a living individual who can be identified from that data (or from that data and other information in our possession or likely to come into our possession). Personal data can be factual (such as name, address, date of birth) or it can be an opinion (such as aspects of an employment reference). Information can be personal data without including a person's name. Personal data may also be referred to as 'personal information'.
Retention schedule	The retention schedule lists the types of information produced as part of University activities and identifies the period of time for which this information must be retained. The retention period is based on legal, contractual or regulatory requirements where applicable, and on operational needs and sector guidance where there are no such requirements.

Recordkeeping system	A system which captures, manages and provides access to records of business activity over time. This may be: • Electronic • Paper-based The following can be defined as a recordkeeping system: • A cabinet of physical files • A network drive (structured folders) • OneDrive (structured folders) • A SharePoint documents library