UNIVERSITY OF CENTRAL LANCASHIRE

Information Management Policy

Approved: 17th January 2018

DOCUMENT CONTROL INFORMATION

CLASSIFICATION	DOCUMENT DESCRIPTION
Classification	Internal and external
Responsibility for drafting	Corporate Records Manager
Consulted with	Learning and Information Services
Document Sponsor	Information Security and Data Quality Group
Approved by	Pro Vice-Chancellor (Corporate Development)
Effective from	January 2018
Next review date	Annual following date approved
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 Policy statement 4
D Responsibilities 5
E Relationships with existing policies 6
F Implementation 6
I Breach of the policy 7
J Glossary of Terms 7

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 operational needs and legislative and regulatory requirements.

The availability of good quality records enables the University to carry out its fundamental roles as a higher education and research institution.

Good information management also supports compliance with the Freedom of Information Act 2000, Environmental Information Regulations 2004 and data protection legislation – the Data Protection Act 1998 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 Disposing of records that are no longer required also decreases the cost of storage and reduces the risk of using out of date data.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 document aims to provide a framework for managing the University's information by explaining the University's underlying approach to information management, documenting the roles and responsibilities of key parties, and listing the tools and resources available to support the implementation of this policy.

B Scope of the Policy

This policy applies to all University 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.

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 (which also covers personal and sensitive personal data).

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 maintain our corporate memory.

C Policy statement

The University of Central Lancashire is committed to creating and maintaining information which supports and documents our activities, to good information governance, and to complying with legal and statutory requirements, in particular the Freedom of Information Act 2000 and the Data Protection Act 1998. We recognise that information forms our corporate memory and is an important organisational asset.

This applies to all data, information and records, in all media, which are created, received or maintained by our staff, irrespective of their contractual status, in the course of University of Central Lancashire business. Information and records created through partnerships are also subject to contractual record keeping requirements.

The University of Central Lancashire is committed to:

- Maintaining records that support its activities as an educational and research institution;
- Ensuring that records are created to provide evidence of its decisions and compliance with legal and statutory requirements;
- Maintaining information systems to support the secure storage of information, records and data and to support their integrity and reliability;
- Developing and maintaining policy and procedures for the review and timely disposal of information in line with organisational requirements, legal obligations and historical value;
- Protecting information from unauthorised alteration, access or loss and providing an audit trail to record the movement and use of information;
- Setting principles and standards which govern access to information based on risk, sensitivity and confidentiality;
- Ensuring that information which is essential to business continuity is identified and protected;
- Ensuring the identification and preservation of records that form our history;
- Monitoring and promoting compliance with this policy.

We will provide adequate and appropriate resources to implement this policy and will ensure it is communicated and understood.

D Responsibilities

This policy applies to all employees, including temporary, casual, contract and agency staff, as well as any contractors or service providers acting on behalf of the University. All employees are responsible for ensuring that 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 document. This includes storing records appropriately and securely, and identifying obsolete records and disposing of them in an appropriate and, if necessary, an auditable manner.

The Chief Operating Officer (COO) has overall responsibility for ensuring the University manages its information effectively and complies with this policy. The COO is supported in this responsibility by the Corporate Records Manager, who is based in Legal and Governance and can be contacted on DPFOIA@uclan.ac.uk or extension 4167. 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.

This policy is reviewed annually by the Corporate Records Manager, on behalf of the COO. 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.

E Relationships with existing policies

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 and related documents, including the Email Use Policy, and Mobile and Home Working Guidance
- Research Data Management Policy
- Information Categories Guidance

All parts of the University including Schools and Services should also ensure their records comply with any external guidelines, policies or legislation, including but not limited to:

- Data Protection, Freedom of Information and Environmental Information Acts;
- Requirements of the research councils and any other funders of research activities;
- Contractual requirements;
- Requirements of any audits.

F Implementation and resources

All parts of the University including Schools and Services will implement practices to ensure compliance with this policy, and review them regularly. It is the responsibility of the named Information Asset Owner 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. It is strongly advised that any information or data that has passed its retention period, has no further value, and is no longer required for University purposes should be deleted or destroyed on a regular basis, at least annually.

Retention and disposal of records is governed by the University Retention Schedule. The 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. The rationale behind the retention period is included in the schedule.

Information Asset Owners are recorded on the University Information Asset Register. The register is an inventory of the University's information assets and documents 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.

In addition, guidance is available on the intranet here to support the Information Asset Owner and all staff in managing information and records. This guidance is reviewed on an annual basis to ensure it reflects current best practice and to incorporate any frequently asked questions.

I Breach of the policy

If you are concerned that the policy has not been followed or 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;
- Excessive retention of information past its retention period.

The Corporate Records Manager, Information Governance Officer and the IT Security team will review the breach and respond in line with the Information governance incident procedure.

J 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.
Sensitive personal data	Information about a person's: • Racial or ethnic origin; • Political opinions; • Religious or similar beliefs; • Trade union membership; • Physical or mental health or condition; • Sexual life; or information about • The commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in any such proceedings.