Information & Records Management Policy

Version:	6
Dated:	20 November 2023
Document Owner:	Information Governance Manager & Data Protection Officer

Revision History

Version	Date	Revision Author	Summary of Changes
V6	02/11/2023	Rick Cockram	Minor corrections to the published versions. Addition of technical controls for classification. Update to the Classification Examples.
V5	16/08/2021	Rick Cockram	Merged the Records Management, Classification and Retention policies
V4.2	14/05/2018	R Platt	Minor changes to published version
V 4.1	26/04/2018	Rick Cockram	Initial 2018 revision.
V 4	01/08/2009	Caroline Dominey	Previous Published Version

Table of Contents

Introduction

Effective management of information is vital to enable the professionalism that is expected from a Russell Group university. The efficient management of the University's information is necessary to support its core functions, to comply with legal and regulatory obligations, and to facilitate to the effective management of the University. These all contribute to building a reputation as a leading University.

Data and Information Management underpin an organisation's running and decision making by ensuring access to accurate, up-to-date information when required by those that require them while maintaining a strong security stance. Efficient Information Management processes will ensure ease of access to data, efficient use of physical and virtual storage space, legal compliance and reduced duplication of information and effort.

Aims of the policy

This policy acts as a framework to support the management of information with the aim to:

- Clarify the responsibilities of individuals who own and process information and data.
- Improve and maintain the quality of Information Management procedures, through a coordinated and consistent approach to the maintenance of information throughout the University.
- Promote best practice in Information Management throughout the University, thus reducing duplication of records and effort.
- Enable more streamlined processes and efficient services to staff and students.
- Promote a human centred support framework which aims to make compliance a baseline.
- Work towards adoption of Records Management standards such as BS/ISO15489.

Definitions and scope

This policy applies to all information and data created, received, or maintained by staff of the University while carrying out their corporate functions in any form.

Information Management should be viewed in the context of Information Governance more generally, particularly as it relates to the management of personal data, commercially sensitive information, and business records.

Data: a collection of facts or values which when combined or contextualised provide information.

Information: contextualised data or statements which may be interpreted to deduce insights.

Information asset: a collection or type of information managed together for a common purpose.

Information system: a database which is used to store data and present it to a user as information.

Record: information created, received, and maintained as evidence and as an asset in pursuit of legal obligations or in the transaction of business.

Responsibilities

IT Services

- Exeter IT are responsible for ensuring the technical solutions to enable compliance with this policy and other security requirements are available and configured to the specification of Information Governance.
- Exeter IT are responsible for producing training materials for those technical solutions.

Information Asset Owners

- Information asset owners are responsible for ensuring that all records of their information assets are managed in compliance with this policy.
- Information asset owners are responsible for identifying expectations for information classified in relation to their assets.
- Information asset owners are responsible for identifying where information is shared and ensuring that classification requirements are communicated to recipients.
- Information asset owners must ensure that Information Asset Administrators working with their assets are aware of the expected classifications.
- Information asset owners are responsible for keeping track of exception to their expected classifications.
- Information Asset Owners are responsible for ensuring retention periods for their information assets are identified as part of their responsibilities more broadly.
- Information asset owners are responsible for ensuring that the record collections and retention periods for their assets are included on the University Retention Schedule, along with any relevant citation or business requirements.
- Information asset owners are responsible for ensuring that information is either securely disposed of in line with the University Retention Schedule or appropriately archived.

Information Governance Manager & DPO

- Records Management is the responsibility of the Information Governance Manager. High quality records management across the University underpins compliance with Data Protection legislation, the Freedom of Information Act, and other legal obligations on the Information Governance Manager.
- The Information Governance Manager is responsible for the creation and maintenance of a retention schedule, further information can be found in the Information Retention Policy.
- The Information Governance Manager is responsible for the effective management of the Modern Records Centre.
- The Information Governance Manager is responsible for the maintenance and publishing of the approved retention schedule.
- The Information Governance Manager is responsible for providing advice and guidance to Information Asset Owners in setting their retention periods should new assets be created, or existing assets need to be updated.

- As the University's Data Protection Officer, the Information Governance Manager is responsible for meeting the legislative requirements of that role. As relating to this policy this includes ensuring appropriate access and integrity of information is maintained while it is active or retains evidential value as well as ensuring the university fulfils its data minimisation obligations.

Information Users

- All users are responsible for ensuring that records for which they are responsible are accurate and are maintained and disposed of in accordance with the University's records management guidelines.
- All users are required to complete the Information Governance online training which includes a section on Records management to support them in complying with this policy.
- All users are responsible for ensuring that information they create and receive is classified appropriately.
- All users are responsible for ensuring that they handle information in a matter appropriate to its classification.
- All members of the University are responsible for complying with all relevant data protection legislation and this policy.
- All members of the University must also ensure that they are aware of the retention periods set for the information they work with and informing the relevant parties should those periods be unclear.

Managers and Supervisory Roles

- Managers and all employees in supervisory roles should ensure that regular reviews are in place in their areas to ensure that the set retention periods are met, and retention reviews are carried out in a timely manner.

System Owners

- System owners are responsible for ensuring systems that hold information have the capability to securely delete information and not just to archive it.
- System owners are responsible for ensuring that a scheduled process is in place (automated or manual) for identifying and deleting information once it is outside the relevant retention.

Policy statements

The University will:

- Go further than just the letter of the law when it comes to handling personal information and adopt good Information Management practice standards.
- Provide a dedicated Records Management Service, in the Information Governance Team, to provide advice and guidance on current procedures, tooling to support best practice and also support in changing and implementing new systems.

- Develop and maintain a robust records retention schedule, providing guidance on the retention and destruction of records held.
- Identify and retain vital records for operational use.
- Provide advice and guidance to University staff on their use of records and document management systems using an approach based on BS/ISO 15489:2016.
- Provide training and develop a range of guidance notes to support Records Management across the University.
- Protect and keep secure all records in a manner appropriate to their value, content, and retention period.

Information Classification

Overview

Distinct types of information require differing levels of scrutiny and protection. Information must therefore be classified to ensure that those requirements are communicated and can be met. The information's container must be labelled with that classification to avoid any ambiguity. In the case of particularly valuable information the reasoning for the application of a particular label should also be kept for audit purposes.

As part of the process to protect and ensure best practice information governance and security, monitoring and security systems are in place to add an extra level of security for the University's information. Access to these systems is restricted.

Requirements

- Users must consider all relevant factors and assign a classification as defined in the classification scheme set out in Appendix 1 at the point at which information is first stored.
- Once information is classified it must be marked to ensure its classification is available to any user handling it.
- Users must consider the classification assigned to a piece of information when storing or transferring the information.
- If information a user receives is not classified or is incorrectly classified, they must consult with the author or originator of the information and either reclassify the received copy or update the source as appropriate.
- The university will provide tooling where necessary to enforce handing appropriate to the classification and reduce the risk of inappropriate use.

Technical controls and marking

It is the responsibility of information asset owners to ensure that appropriate processes for marking information with appropriate classifications is in place wherever that information is stored.

Some information by its nature may be classified by type and automatically protected in certain environments. Where information is processed through Microsoft 365 for example, Data Loss Prevention tools will scan the information and apply pre-determined restrictions based on its type.

Some tools including Microsoft 365 have the facility to mark documents with Sensitivity Labels relating to the classifications set out in Appendix 1. Sensitivity Labels will apply appropriate technological controls to enforce appropriate handling and reduce data loss.

Document management

Electronic Document and Records Management Systems

- Microsoft SharePoint has been identified as the University's EDRMS along with the full Office365 suite.
- SharePoint is an increasingly important system for the University. Collaboration is a core requirement of document storage as are other elements of the tool to support the sharing and long-term preservation of documents and other information/data containers.
- OneDrive storage is made available to all users with Microsoft 365 accounts at an appropriate level. This storage is only considered suitable for materials related to the account owner as an individual, for example employment matters, health, or childcare related materials and similar. OneDrive storage must not be used for information and documents relating to the user's role.
- Appropriate SharePoint sites and structures must be used in place of a user's individual OneDrive storage allocation for all materials related to the carrying out of their role. This is to prevent business continuity issues related to the starters, movers, and leavers policy and ensure information assets can be managed together. Such materials include all documents created as part of the individual's work for the University in approved and draft form as well as all research data which is not otherwise stored in a more secure environment.
- IT Services are responsible for the management of SharePoint, the implementation of the necessary security controls, and the required communications and training for staff and students.
- Information Governance are responsible for providing the business driver for changes to SharePoint as a platform. This includes SharePoint and its derivative products such as OneDrive and Teams.

Records Management

Records provide evidence of the University's business activities and may be important for operational, legal, or historical purposes. Records play a vital role in ensuring that the University can operate effectively and, if managed correctly, can be a significant asset to the University. Records Management involves the systematic management of information, to ensure that it is available when and where necessary and that it is kept securely, for as long as necessary, but no longer. This document provides the policy framework through which this effective management will be supported and monitored.

Identification of records

The identification of records, as compared to documents, is the responsibility of Information Asset Owners who should record their record collections on the University's Information Asset Register.

Vital Records are defined as records which are vital to the continuing operation of the University. These records may be identified in business continuity plans by plan owners where appropriate.

Modern Records Centre

It is the responsibility of the Information Governance service to provide up to date advice, guidance, and documentation to support the MRC (Medical Research Council).

The physical management of the files in the MRC as well as the retention reviews will also be carried out by the Information Governance Service

Digital archives

Information Governance are additionally responsible for provision of tooling to support the retention of non-physical documents to make sure they are registered maintained and reviewed as paper records.

Information retention

Retention periods

Information should be kept for as long as it is needed to meet the operational needs of the University as well as relevant Data Protection act, legal and regulatory requirements.

Specific information can be found in our published retention schedules.

Retention schedules

The University Retention Schedule is a vital document for the management of information at the university. It aligns the University Information Asset Register with its record collections and informs information users of existing agreed retention periods. Maintaining a retention schedule is a requirement to allow the University to meet its data minimisation obligations and reduce the risk of information exfiltration in the event of a cyber-attack.

Information disposal

Paper documents

Physical documents containing no sensitive data may be recycled using standard recycling facilities.

Physical documents containing sensitive information including but not limited to commercially sensitive data, University IP and Personally Identifiable Information must be disposed of in confidential waste bins and stored in a secure location until collected.

Digital documents

Digitally created documents can be deleted using the delete options available locally on your computer or SharePoint site as normal. They will be retained in the University's rolling backup or the SharePoint central recycle bin which provides resilience and recovery options; these are purged regularly.

Where information is held in a database, processes for deletion of files and data will vary. Users should refer to existing guidance specific to the system in question or contact the system owner.

Archival transfer

Physical documents with long retention periods and low access requirements may be considered for transfer to an archival facility. A limited amount of long-term storage is managed internally by the Information Governance Team, who are also able to advise on other viable options on an ad hoc basis.

Digital materials should be archived in appropriate locations such as with in Microsoft 365 or using a repository such as ORE.

Using copies of information owned by other departments.

It is acknowledged that it is often a business necessity to share information which is owned and managed by other departments, to meet contractual, legislation or regulatory requirements. Where possible such information should be accessed in its original location and not duplicated.

For retention purposes the owner of a copy is only required to maintain their copy for as long as is required to carry out the necessary processing, after which it must be securely destroyed. It remains the responsibility of the owner to retain information for the full duration of the retention period if that is longer.

Copies must also be stored and shared in accordance with the classification of the information. If any requirements are unclear or handling instructions are not provided it is the responsibility of the recipient to seek the necessary details from the owner.

For reasons of security and ease of management it is preferred that information be stored in a location which is accessible to anyone with a legitimate need.

Copies of information must not be emailed to any recipient internally or externally unless strictly necessary. Instead, appropriate sharing technologies should be employed to allow the intended recipient to fetch the information themselves. This greatly reduces the risk of data breaches and dramatically reduces the number of copies of information the university holds.

Relation to existing policies

This policy should be used in conjunction with other relevant University policies and documents including but not limited to:

- Data Protection and Freedom of Information Policies
- University Records Retention Schedule
- Information Security Controls policy

Feedback

Any queries or proposed amendments should be referred to the Information Governance Department at informationgovernance@exeter.ac.uk.

Appendices

Appendix 1: Information Classification Examples

Classification	Impact of public disclosure	Definition	Examples
Public	None.	Information which may be made available to the public at large without risk.	• Publications • Press releases & public events • Public facing policy & guidance • FOIA disclosures • Core details of senior staff & structures • Basic contact details of public facing staff
Community	Low Highly unlikely to result in reputational or financial damage to the University. *Government equivalent: Not classified*	Information not intended for the public, but which may be made available to University of Exeter Students, peers, and partner organisations through non-public channels.	• University address book details • Internal communications including Viva Engage posts
Internal	Low Unlikely to result in reputational or financial harm to the University. May result in minor data privacy breach. *Government equivalent: Official*	Information which may be made available to all University of Exeter Employees and Associates.	• University Policy and guidance materials • Internal communications • Support and complaints procedures
Restricted	Medium Likely to result in reputational or financial harm to the University or a third party. May result in a data privacy breach or breach of confidentiality. *Government equivalent: Official*	Information which may be made available to authorised employees in order to carry out their role. It may be stored in shared locations with appropriate protections.	• Personal data of identifiable individuals. • Individual staff member's HR records including contracts, wellbeing information and pay slips. • Contacts and NDAs
Confidential	High Poses an immediate or significant risk to the reputation and or financial position of the University or a third party. Would result in a severe privacy breach or breach of confidentiality. *Government equivalent: Official-Sensitive*	Information to which access is strictly controlled and restricted only to predetermined, approved groups or members of University of Exeter staff by name or role. Information must be stored in locations with security appropriate to the sensitivity of the data.	• Special category personal data of identifiable individuals. • Bank details and financial information • Transcripts and exam papers • University IP including course content and unpublished research data. • Investigations, & disciplinary proceedings • Commercially sensitive information
Secret	Critical May pose risk to national security. *Government equivalent: Secret and above*	The existence of the information is known only to a very small number of named individuals who have been explicitly cleared for access and possess appropriate verifications.	Information subject to the Official Secrets Act or an equivalent.