Information Retention Policy

Version:	**1.0**
Dated:	**14 May 2018**
Document Owner:	**Information Governance Manager**

Revision History

Version	Date	Revision Author	Summary of Changes
V 0.1	May 2018	R. Cockram	Initial Draft.
V 0.2	May 2018	R. Platt	Amendments to initial draft
V 1	May 2018	R Platt	Approved Version

Approval

Version	Approval Board	Date of Approval
V 1.0	Information Governance & Security Steering Group	May 2018

Table of Contents

1. Introduction:

1.1 The University of Exeter acknowledges that appropriate retention periods must be set for all information processed by the University to ensure effective administration and to meet its strategic aims and objectives. The proper management of this process will enable the University to provide evidence of its transactions and activities and enable it to comply with its legal and regulatory obligations.

1.2 This policy applies to all Information processed by the University including information created, received or maintained by the University while carrying out its business.

1.3 A small proportion of the University's records may be selected for permanent preservation in the University archives to be available for historical research and/or to give a lasting record of the University's business.

2. Responsibilities

The University of Exeter is the 'data controller' and the Council of the University is ultimately responsible for compliance with current data protection legislation.

2.1 **Information Users**

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 data they work with and informing the relevant parties should those periods be unclear.

2.2 **Senior Information Officers (SIO)**

Director of College Operations and Directors of Professional Services have the responsibility of overseeing compliance and developing good data protection practice within their designated areas.

2.3 **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.

2.4 **Information Asset Owners (IAO)**

Information Asset Owners are responsible for ensuring retention periods for their information assets are identified as part of their responsibilities more broadly. They need to ensure these are included on the University Retention Schedule, along with any relevant citation or business requirements. The IAO must also ensure that information is either securely disposed of in line with the University Retention Schedule or appropriately archived.

2.5 **System Owners**

System owners/administrators are responsible for ensuring systems that hold information have the capability to securely delete information and not just to archive it. Where appropriate the system owner should ensure a scheduled process is in place (automated or manual) for identifying and deleting information once it is outside the relevant retention period identified by the IAO.

2.6 **Information Governance Manager**

The Information Governance Manager is responsible for the maintenance and publishing of the approved retention schedule. They will also provide advice and guidance to Information Asset Owners in setting their retention periods should new assets be created or existing assets need to be updated.

3. Retention periods

3.1 Information should be kept for as long as it is needed to meet the operational needs of the University, together with legal and regulatory requirements. Through the Information Audit process, we have:

- determined the value and processing conditions for each of our information assets,
- assessed their importance as relating to their support for business activities and decisions,
- established whether there are any legal or regulatory retention requirements. Examples of these include but are not limited to: The Limitation Act (1980), The Higher Education and Research Act (2017), The Employment Act (2008), terms and conditions of funding bodies of research grants.

4. Retention Schedule

4.1 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.

4.2 Retention periods are set by Information Asset Owners to ensure that they meet the business and legal requirements for the data being processed. The Information Governance Manager is responsible for advising on setting retention periods as well as collating approved retention periods and publishing them in the University Retention Schedule. The document will be closely related to the Information Asset Register but will be published as a separate resource.

5. Information disposal

5.1 Paper Documents

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

5.1.2 Physical documents containing sensitive information including but not limited to commercially sensitive data, IP data and Personally Identifiable Information must be disposed of in confidential waste bins.

5.2 Digital Documents

5.2.1 Digitally created documents stored on the University shared drives and personal U drive can be deleted using your computer's recycle bin function as normal. They will be retained in the University's rolling backup which provides resilience and recovery options; this is purged regularly.

5.2.2 Where data is held in a system rather than a drive, 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.

5.3 Archival Transfer

5.3.1 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 possible options on an ad hoc basis.

6. Using copies of data owned by other departments

6.1 Sharing information internally is vital to the efficient management of the University. In cases where you are called upon to use a copy of data where a master copy is held by another department, your own retention requirements should be considered separate to theirs.

6.2 For example, during the recruitment process a hiring manager will require access to HR data. Once the recruitment exercise is over that data is updated and returned to HR, the hiring manager would no longer have a reason to process it. In this case a shorter retention period is permitted as the University's legal obligations are being met by the master copy.

7. Relationship to existing policies

7.1 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 (Appendix 1)
- Information Security Controls policy
- University Data Classification Policy

7.2 SIOs and IAOs should also ensure their records comply with any external guidelines, policies or legislation, including but not limited to:

- Data Protection legislation, Freedom of Information and Environmental Information Acts
- Requirements of the research councils, ERDF, other funders of research
- Requirements of any audits.

8. Implementation and resources

8.1 Director of College Operations and Directors of Professional Services will implement practices to ensure compliance with this policy and review them regularly. It is the responsibility of the information asset owner to ensure that good housekeeping practices are undertaken to ensure the accuracy and relevance of information assets that reside on the University servers.

8.2 It is strongly advised that any personal or residual information or data that has no value or is no longer required for University purposes should be removed from the relevant drives and servers on a regular basis, at least annually.

8.3 Retention and disposal of records will be governed by the University Records Retention Schedule. The schedule provides a list of the types of records produced by the University, and details of the length of time that they should be retained to meet operational and regulatory requirements.

9. Contacts

9.1 Any queries or proposed amendments should be referred to the Information Governance Office at dataprotection@exeter.ac.uk.