

RECORDS RETENTION AND DISPOSAL POLICY

1. Policy Statement

- 1.1 The University is committed to good practice in records management, and in particular is committed to retaining information for as long as necessary and no longer.
- 1.2 The retention periods for different groups of records shall be determined by consideration of the operational, legal and contractual requirements, and in line with best practice within the Higher Education sector. JISC has conducted extensive research and consultation to provide a Business Classification Scheme and Records Retention Schedule¹ tailored to the needs of the sector, and this shall be followed wherever possible. Any deviation from or extension to this guidance shall be discussed with the Data Protection Officer and the reasoning behind the retention period recorded in the Records Retention Schedule.

2. Scope

2.1 This Records Retention and Disposal Policy:

- Applies to all information for which the University has a legal, contractual or moral responsibility, and which is organised into information sets.
- Applies to all information sets regardless of the format of the information, including collections of documents or emails, databases, collections of images, video or sound etc.
- Applies to all information sets, regardless of the media on which the information is stored, including electronic, paper, film, CD, DVD, microfiche etc.
- Applies to all students, staff, contractors or any other person or organisation having access to University information or University information systems.

3. Introduction

- 3.1 The University collects stores and processes a great deal of information in the course of its activities, and the effective management of its information assets is a critical factor in its operations.
- 3.2 The indefinite retention of all information would present severe logistical problems, and in the case of personal information, would be in breach of Principle 5 of the General Data Protection Regulation. Retaining more information than necessary also increases the amount of work necessary to comply with requests for

¹ <http://bcs.jiscinfonet.ac.uk/he/default.asp>

information under various items of legislation including the General Data Protection Regulation, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

- 3.3 Disposal of some groups of records too early would place the University in breach of certain regulatory and statutory requirements, as well as jeopardising the essential functions of the organisation.
- 3.4 A Records Retention and Disposal policy brings clarity for people within the University who are responsible for records management, minimises the risks associated with keeping information too long or disposing of it too soon, and demonstrates one element of effective records management in line with the section 46 Code of Practice issued by the Lord Chancellor².
- 3.5 This Policy sets out:
 - How the University determines the appropriate retention period for groups of records (one or more information sets serving a particular business purpose), and how staff are informed what these retention periods are; and
 - How the University manages the retention and disposal of information in line with the retention periods.
- 3.6 This policy **does not** list the retention periods for the different groups of records. These are defined in the accompanying Records Retention Schedule.

4. Policy Status

This policy is not part of the formal contract of employment, but it is a condition of all employment contracts that employees will follow the rules and policies created by the University from time to time. Failure to follow the policy can result in disciplinary action being taken.

5. Operation of the Policy

- 5.1 The retention periods for each group of records shall be published in a Records Retention Schedule, maintained by the Data Protection Officer.
- 5.2 The Data Protection Officer shall update the Records Retention Schedule in the light of regulatory, legislative or other developments and take the appropriate steps to ensure that all staff likely to be affected by the changes are informed.
- 5.3 Information Custodians shall ensure that each information set for which they are responsible is matched up with the appropriate record group or groups, and that this and the corresponding retention period is recorded in the Information Asset Register.
- 5.4 Information that is the subject of a subject access request under the General Data Protection Regulation, a Freedom of Information Act 2000 request, a request under the Environmental Information Regulations 2004, or is relevant to a current or

²

<http://webarchive.nationalarchives.gov.uk/20130128112038/http://www.justice.gov.uk/downloads/information-access-rights/foi/foi-section-46-code-of-practice.pdf>

forthcoming legal action, shall not be destroyed until the request or action is complete.

- 5.5 Information sets may be retained longer than the retention period for the relevant record group where there is a clear business purpose, for example to comply with the conditions of a research contract. Such exceptions shall be discussed with the Data Protection Officer.
- 5.6 Heads of Department, School or Centre (for cases of automated and manual processing) shall ensure that the retention periods are appropriately reflected in system processing and/or business processes.
- 5.7 Copies of records sets shall be destroyed as soon as their purpose is fulfilled, and in any case no later than the original is destroyed. This does not apply to data backups made for business continuity or disaster recovery purposes, and which would not normally be available for access.
- 5.8 When the retention period expires, the information shall be destroyed in such a way that the information cannot be retrieved. Particular care shall be taken where the information is categorised as restricted or highly restricted. A log shall be kept summarising the information destroyed, and these logs shall be passed to the Information Custodian for permanent retention.
- 5.9 Where the retention period is specified as ‘permanent’, the Information Custodian(s) shall liaise with the Head of Department, School or Centre to agree archiving arrangements, and ensure that the Head of Department, School or Centre make arrangements for these to be incorporated in the relevant computer systems and/or business processes.

6. Responsibilities

6.1 Data Protection Officer:

- Maintain and publish the Records Retention Schedule and inform appropriate staff of any material changes to it;
- Provide advice where there is a perceived need to deviate from the retention periods recommended for record groups in the JISC Records Retention Schedule, or to determine retention periods for information sets that do not correspond with a record group in the JISC Business Classification Scheme;
- Provide advice to Information Custodian in cases where there is a business need to retain an information set for longer than the normal period for the record group; and
- Notify Information Custodian of any requests any legislation or any impending legal actions that might require them to prevent the destruction of data.

6.2 Information Custodians:

- Ensure that each information set for which they are responsible is matched up with the appropriate record group or groups, and that this and the corresponding retention period is recorded in the Information Asset Register;
- Discuss any proposed extension to the retention period of an information set beyond that for the corresponding record group with the Data Protection Officer;

- Discuss archive arrangements with the Head of Department, School or Centre for any record sets to be retained permanently, and ensure that steps are taken to implement these arrangements;
- Ensure that arrangements are made to prevent the destruction of data when informed that they need to be retained because of a request under relevant legislation or because of an impending legal action; and
- Permanently retain data destruction logs.

6.4 Heads of Departments / Schools / Centres / Line Managers / Supervisors:

- Ensure that the retention periods are appropriately reflected in business processes;
- Ensure that logs of data destruction are kept and passed to the Information Custodian; and
- Ensure that their staff are aware of the Records Retention and Disposal Policy.

6.5 Students and staff involved with the maintenance of information sets:

- Comply with the Policy; and
- Report any breaches or suspected breaches of the Policy to their line manager / supervisor.

6.6 The following officers are responsible for the safekeeping of official and legal documents relating to the University:

- Land, property and works – Director of Facilities
- Educational contracts, franchise agreements – Pro Vice Chancellor (Academic)
- Financial documents – Assistant Vice Chancellor (Resources)
- Employment – Director of Human Resources
- Purchasing contracts – Assistant Vice Chancellor (Resources)

7. Equality Impact Assessment

The University of Bolton is committed to the promotion of equality, diversity and a supportive environment for all members of our community. Our commitment to equality and diversity means that this policy has been screened in relation to the use of plain English, the promotion of the positive duty in relation to the protected characteristics of race, sex, disability, age, sexual orientation, religion or belief, gender reassignment, marriage and civil partnership, pregnancy and maternity.

8. Other Related Policies and Procedures

Information Security Policies

Data Protection Policy

Records Retention Schedule

TITLE OF POLICY: Records Retention and Disposal Policy	
Policy Ref	VC/01/2018
Version Number	1.0
Version Date	January 2018
Name of Developer/Reviewer	Registrar (Developer) Contracts and Compliance Officer
Policy Owner (Group/Centre/Unit)	Vice Chancellor's Office
Person responsible for implementation (postholder)	Registrar and Chief Operating Officer
Approving Committee/Board	Executive Board
Date Approved	20/4/2018
Effective from	20/4/2018
Dissemination method (eg website)	Website
Review Frequency	2 years
Reviewing Committee	Executive Board
Consultation history (individuals/group consulted and dates)	GDPR working group; Student Data Management
Document History (e.g. rationale for and dates of previous amendments)	