

Records Management and Retention Policy (IGP-03)

Summary			
This Policy establishes principles for ensuring that the University implements effective records management, accounting for legislative, regulatory and best-practice requirements. It provides guidance on the retention and disposal of records held by the University.			
Scope			
The policy applies to all employees of the University of Bristol, including honorary staff/associates, contractors, temporary staff and any students who are carrying out work on behalf of the University.			
Document Control			
Document type	Information Governance Policy – IGP-03		
Document owner	Information Governance Manager		
Division	University Secretary's Office		
Lead contact	Information Governance Manager		
Document status	Approved		
Version	v1.1		
Approved by	Information Governance and Security Advisory Board	Date	19/04/2018
Date of publication	July 2018	Next review date	
Date of original publication	July 2018	Revision frequency	
Superseded documents	N/A		
Related documents	See Related policies below		

Contents

1. Introduction	2
2. Scope	3
3. Legislation and compliance framework	3
4. Responsibilities	4
5. Related policies	4
6. Standards	5
7. Management of records	5
7.1 Creating records	5
7.2 Organising records	6
7.3 Off-site storage and scanning	7
7.4 Security and access	7
8. Retention	8
9. Disposal	9
9.1 Reappraisal	9
9.2 Permanent preservation	10
9.3 Destruction	10
9.4 Records of disposal	12
9.5 Disposal of IT equipment	12
10. Policy review and ownership	12
Annex 1: Records Disposal Form	13
Annex 2: Document history	15

1. Introduction

Records Management is the process of managing records, in any format or media type, from creation through to disposal in line with legal and business requirements. Effective Records Management allows for fast, reliable and secure access to records ensuring the timely destruction of redundant records as well as the secure identification and archiving of records considered worthy of permanent preservation.

The University of Bristol recognises that the efficient management of records throughout their lifecycle is necessary to support its core functions, to comply with its legal and regulatory obligations, and to contribute to the effective overall management of the institution.

This policy sets out principles for ensuring that the University implements effective records management, and provides guidance on the retention and disposal of records. It covers all

types of records created or used by staff, whatever format they are held in, and addresses the requirements of the Lord Chancellor's Code of Practice on the Management of Records (issued under Section 46 of the Freedom of Information Act 2000).

2. Scope

This policy applies to all records created, received, maintained and held, in all formats, by staff of the University in the course of carrying out their corporate functions. Records are defined as documents, regardless of format, which facilitate the operations and business of the University and which are thereafter retained for a set period to provide evidence of its activities and transactions.

The policy covers records concerning the management, governance and administration of research, but specific guidance in relation to the processing and storage of research data is provided by the [Research Data Service](#), including use of the [Research Data Storage Facility \(RDSF\)](#).

A small percentage of the University's records will be selected for permanent preservation as part of the University's archive for historical and evidential purposes, and as an enduring record of the conduct and management of the University.

This policy applies to all employees of the University of Bristol, including honorary staff/associates, contractors, temporary staff and any students who are carrying out work on behalf of the University. It is a contractual obligation to adhere to the requirements of the policy.

3. Legislation and compliance framework

The management of records held by the University of Bristol is regulated by the following legislation:

- Data Protection Act 2018 & General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- Limitation Act 1980

The Data Protection and Freedom of Information Acts contain provisions relating to the destruction or alteration of information or records after a legal access request has been received. Such destruction or alteration will be considered a disciplinary offence. The Freedom of Information Act 2000 also creates a criminal offence in relation to these actions.

The Section 46 Code of Practice on the Management of Records sets out measures and good practice that should be in place in relation to information management to ensure that requests made under the Freedom of Information Act can be answered in a timely manner, and also that information is not disposed of when it may still be required.

The ISO 15489 series of international standards on information, documentation and records management establishes standards for the management of business records.

Other areas of the University's operations have specific retention requirements set out in separate legislation such as those relating to employment, health and safety, finance and pensions, and environmental information. The University also requires high quality records to be maintained for the purposes of audits and reviews by regulatory bodies.

Research data may also have specific requirements in relation to management, storage, retention and disposal set out under the terms of funding contracts, data sharing agreements, or by ethics committees that must be adhered to.

4. Responsibilities

The University has a corporate responsibility to maintain its records and record-keeping systems in accordance with the regulatory environment. The Senior Information Risk Owner (SIRO) is accountable at an executive level for ensuring that appropriate provisions are in place. This role is held by the University's Registrar and Chief Operating Officer. Heads of Department, School, Faculty, Service, and Division have overall responsibility for the management of records generated and held within their area.

There must be a clear allocation of responsibility within each department to assist with the management of records. All records should have an identified owner responsible for their management whilst in regular use, and for appropriate retention and disposal. This person or role is defined as the Information Asset Owner, and they can receive support from nominated Information Asset Administrators. There must be no ambiguity regarding responsibility for the maintenance and disposal of records.

Line managers are responsible for ensuring that their staff are aware of this Policy and comply with its requirements. All members of staff are responsible for ensuring that their work is documented appropriately, that the records which they create or receive are accurate and managed correctly, and are maintained and disposed of in accordance with the University's guidelines and any legislative, statutory and contractual requirements. Line managers should ensure that when a member of staff leaves, responsibility for their records is transferred to another person; if any of the information is redundant, it should be deleted by either the departing member of staff or their line manager.

It is vital that records management considerations are appropriately incorporated into project and planning processes and system design at the earliest possible stage of development. Where records contain personal data there is a legislative requirement to do this in order to ensure that a ***data protection by design and default*** approach is followed.

5. Related policies

The Policy forms part of the University's Information Governance Framework and needs to be considered in conjunction with the following University policies and guidance:

- IGP-01 - Information Governance Policy
- IGP-02 - Data Protection Policy
- IGP-04 - Records Retention Schedule
- IGP-05 - Document Management Policy

- IGP-06 - Digital Preservation Policy
- IGP-07 – Personal Data Breach Policy
- IGP-08 – Privacy Impact Assessment Policy
- IGP-09 – Information Strategy Principles
- [IGP-10 – Information Classification Scheme](#)
- [Information Security Policy](#)

6. Standards

The following standards need to be maintained at all times:

- Records must be managed in a manner complying fully with legislative and regulatory requirements affecting their use and retention.
- Records must have relevant content, context and format, and must be accurate, authentic, useable, reliable, timely and well managed.
- Records must directly relate to and support a service, function or activity delivered by the University, and be able to support decision-making.
- Records must serve the interests of the institution, its staff, students and other stakeholders by maintaining high quality documentation for appropriate lengths of time.
- Records must be managed via systems and processes ensuring efficiency and consistency throughout their lifecycle of creation, distribution, use, maintenance and disposition.
- Records must be managed and stored in a suitable format to retain quality, relevance, accessibility, durability and reliability. Any transfer to another format must have due regard to retaining these qualities.
- Records must be kept securely as befits the confidentiality and importance of the content, being protected from unauthorised or unlawful disclosure.
- Records must be accessible and retrievable as required to support business efficiency and continuity.
- Records must be retained or disposed of in compliance with the Records Retention Schedule.
- Records must be subject to clearly defined arrangements for appraisal to select those worthy of permanent preservation. Those of historical significance to the corporate memory of the organisation should be preserved.
- Records must undergo appropriate destruction when no longer required, in an organised, efficient, timely and (where necessary) confidential manner.

7. Management of records

7.1 Creating records

Each section of the University must have in place adequate systems for documenting its principal activities and ensuring that it creates and maintains records that serve its functions and the standards detailed above.

The records must be accurate and complete, so that it is possible to establish what has been done and why. The quality of the records must be sufficient to allow staff to carry out their work efficiently, demonstrate compliance with statutory and regulatory requirements, and ensure accountability and transparency expectations are met. The integrity of the information contained in records must be beyond doubt; it should be compiled at the time of the activities to which it relates, or as soon as possible afterwards, and be protected from unauthorised alteration or deletion.

Where appropriate, templates should be used, so that documents are produced consistently and quickly. In addition, version control procedures are required for the drafting and revision of documents, so that staff can easily distinguish between different versions and readily identify the latest copy.

Individuals or roles must be identified within units to take responsibility for records or record sets and fulfil the role of Information Asset Owner.

The retention of duplicate records presents enhanced risks regarding their management, use and alteration. Whereas there may be a need to keep local versions of records held centrally, it should be avoided where possible and a system enabling use of a single central version implemented. Where practical, to reduce the need for duplication documents should be stored in central folders that are accessible by relevant staff. Digital information should be filed in shared corporate workspaces wherever possible. File titles should be brief but comprehensible with a consistent format used.

Where possible, both paper and electronic records systems should contain metadata (information about the structure of the records system or series) to enable the system and the records to be understood and operated efficiently, providing an administrative context for effective management of the records, and to enable individual records to be identified and accessed efficiently. The metadata could include details of the structure of the records, dates of access, use, alterations, disposal etc.

7.2 Organising records

Records should be organised and described in a uniform, logical manner that facilitates fast, accurate and comprehensive retrieval so that they are easily accessible when required. A filing structure or records series should be used, i.e. a group or unit of related records, documents or information that is normally filed or kept together because they relate to a particular subject or function, or result from or document a particular activity.

Classifying records and holding them in an appropriate structure or scheme will enable suitable retention periods to be assigned. Keeping diverse records together in a less structured manner makes it more difficult to identify and retrieve them when required, and to apply responsible retention policies.

Standardised referencing and titling must be employed, so that information can be readily identified and retrieved. Naming conventions will assist with using consistent terminology to improve efficiency. Titles given to digital and hard copy records and files should describe the content or subject matter accurately and helpfully. Section 8 of the Document Management Policy (IGP-05) provides specific guidance on naming conventions for documents and folders.

Digital storage solutions enabling more sophisticated tagging and searching functionality will become more widely available for University staff to use. These developments will assist with the correct storage, classification and retrieval of records.

Section 7 of the Document Management Policy (IGP-05) provides specific guidance on document management practices and should be read in conjunction with this document.

7.3 Off-site storage and scanning

When storage space for hard-copy records is an issue the University uses a contracted off-site storage provider. This can be a cost-effective way of managing records but careful thought should be given to the types of records that are selected for offsite storage, in particular how quickly and frequently such records may need to be accessed. There are additional costs for retrieval of records and there can also be a short delay.

A scanning service is also available which can assist with storage needs and make records more accessible. It can bring significant benefits but careful consideration should be given to whether scanning is a suitable solution, as it can impact on the legal or evidential integrity of documents, and may not be suitable for a series of records to which information is still being added. Further details of the [off-site storage and scanning services can be found here](#).

7.4 Security and access

Appropriate levels of security must be in place to prevent the unauthorised or unlawful use and disclosure of information. All records in any format must be held in accordance with the University's [Information Security Policy](#) and [data protection guidance](#). Records must be stored in a safe and secure physical and digital environment taking account of the need to preserve important information in a useable format enabling access commensurate with frequency of use.

The University's [Information Classification Scheme](#) describes the following five categories of confidentiality which should be used to classify information and records held by the University. It will assist with determining appropriate practice regarding storage, access, handling and disposal of records.

Classification	Definition
Public	May be viewed by anyone, anywhere in the world
Open	Available to all authenticated members of University staff
Confidential	Available only to authorised and authenticated members of staff
Confidential & Sensitive	Access is controlled and restricted to a small number of named, authenticated members of staff
Secret	Known only to a very small number of authenticated members of staff

An access policy, taking into account the confidentiality of information, should identify who is permitted to have access to which records and to highlight if special security measures are required for any records. Records should not be only accessible by a single person but should be stored in centralised storage or filing systems or on a shared drive, so that departments can operate efficiently when individual members of staff are absent. Where appropriate, access to central records should be appropriately available across the University in order to avoid recreating information that already exists and storing duplicate data unnecessarily.

Records that would be vital to the continued functioning of the University in the event of a disaster must be identified and protected. These include records that would recreate the University's legal and financial status, preserve its rights, and ensure that it continues to fulfil its obligations to its stakeholders. All critical business data must be protected by appropriate preservation, backup and disaster recovery policies. Where vital records are only available in paper format it is best practice that they are duplicated, and the originals and copies stored in separate locations. If, however, duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect vital documents.

8. Retention

The Freedom of Information Act Section 46 Code of Practice on the Management of Records states:

“As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required.”

Records must only be kept for as long as is required to meet operational, business and legal needs. It is a legal requirement established by the Data Protection Act to only retain records containing personal data for as long as is strictly necessary, and organisations can be subject to enforcement action for failing to comply. By having clearly defined procedures for the retention and disposal of records, the University can demonstrate corporate responsibility in the management of its information and records.

The University's Records Retention Schedule is intended to provide guidance to all sections of the institution regarding appropriate retention periods for different categories of record. It applies to all formats of records. It promotes consistency and the retention of the minimum volume of records while accounting for requirements imposed by legislation and regulation. The Records Retention Schedule will not provide direct guidance for every conceivable type of record but should be used as an aid to develop more comprehensive local retention policies.

Information Asset Owners must agree retention periods for the information assets which they are responsible for, using the Records Retention Schedule, and these must be set out in the Information Asset Register. With assistance from the Information Governance Manager and other resources, Information Asset Owners are responsible for ensuring that the retention periods are regularly reviewed (at least annually) to determine whether any retention periods

applying to information within their Division or School have expired. Once the retention period has expired, relevant action must be taken.

Retention can be complicated if records of a dissimilar nature, with different retention requirements, are filed together. Departments should consider retention periods when designing their records storage systems and practices to avoid this issue. Files should be weeded regularly to ensure records are not kept for too long. If there is no alternative, the entire file should be retained for the longest relevant retention period.

The Records Retention Schedule includes the following information:

- i) **Record description** – The type of record or asset, applying to all formats of record.
- ii) **Retention period** - The recommended length of time for which the records should be kept by the University of Bristol. The retention period is often expressed as a starting point plus number of additional years to be kept, though it can permanent retention may be advised for some records.
- iii) **Action at end of retention period** – There are three potential disposal outcomes for a record at the end of its retention period:
 - a) Reappraisal
 - b) Permanent preservation / Send to University archives
 - c) Destruction
- iv) **Record Owner** – The Division, sub-division or other high-level area of the University that owns the record and is ultimately responsible for its retention and disposal. The Record Owner is responsible for the implementation of their section of the Records Retention Schedule wherever it may apply across the University, although operational practice may rest within other areas, requiring close collaboration, including ensuring that all relevant Information Asset Owners are fully appraised of their requirements of the Retention Schedule and apply accordingly. This may include auditing compliance. In coordination with the Secretary's Office, they are responsible for reviewing and developing this document.

9. Disposal

When a record reaches the end of its retention period a decision must be taken on its disposal, with the three possible outcomes:

- a) Reappraisal
- b) Permanent preservation / Send to University archives
- c) Destruction

9.1 Reappraisal

Before action is taken to permanently preserve or destroy a record at the end of its retention period, a reappraisal of any need to retain it for present functions should be undertaken, but it should only be necessary to attribute a revised retention period on rare occasions.

In some circumstances it may be necessary to retain a record for longer than its defined retention period. A new operational function requiring its retention may have arisen, or it may be required for investigation or litigation purposes, or because it is needed in order to respond to an access request received under data protection or freedom of information legislation. If a record needs to be retained for longer, then a new retention timescale should be assigned to it. It is recommended that this date should not be too far in the future, enabling regular review of the decision while taking circumstances into account. A period of one year is recommended.

9.2 Permanent preservation

Some of the University's records are retained permanently because they have long term evidential or historical value. The University's Records Retention Schedule should help to identify records that have archival value. The following records are examples of items that may be worthy of permanent preservation:

- Records that document policy formation
- Records that show the development of the University's fabric and infrastructure
- Records that show evidence of important decisions or precedent
- Records showing the development of the relationship between the student body, academic departments and the corporate functions
- Records documenting the University's relationship with external parties and stakeholders, and the University's place in the local, national and international community
- Records that show the development of academic departments and corporate divisions
- Papers relating to the University's charter, statutes, ordinances & regulations, including agendas, minutes, supporting documents and reports relating to senior committees and decision-making bodies.

Guidance on arrangements for the permanent preservation of records and transfer to archives are available [here](#).

If electronic records have been identified as having archival value then consideration should be given to whether they are retained in a format deemed to be future proofed, and how they can be transferred and stored for permanent preservation.

9.3 Destruction

The Information Asset Owner is responsible for ensuring that records are destroyed in a timely and secure manner, and that senior staff within the relevant department are aware that the destruction is taking place. All copies, including security copies, preservation copies and where possible backup copies, held in any format must be destroyed at the same time.

Destruction must be carried out in a way that takes full account of the confidentiality of the record using the Information Classification Scheme. For hard copy records the following requirements apply:

Information classification	Method of disposal
Public	Can be disposed of in ordinary waste or recycling bins.
Open	For some records in this category disposal in ordinary waste and recycling bins will be appropriate, but many must be disposed of in grey confidential waste bins or shredded and placed in paper rubbish sacks for collection by the University's contracted disposal firm. Open records must be assessed on their individual merits but if uncertain the latter will apply.
Confidential	Must be disposed of in grey confidential waste bins or shredded and placed in paper rubbish sacks for collection by the University's contracted disposal firm.
Confidential & Sensitive	Must be disposed of in grey confidential waste bins or shredded and placed in paper rubbish sacks for collection by the University's contracted disposal firm. If the record is subject to a contract or agreement then these must be checked for any further requirements.
Secret	Must be disposed of in grey confidential waste bins or shredded and placed in paper rubbish sacks for collection by the University's contracted disposal firm. Such information may have further requirements for secure disposal, for example information provided under the Official Secrets Act.

When an entire file or archive box is to be destroyed the whole file or box must be destroyed in line with the requirements of the most sensitive documents it contains.

It is very easy for multiple duplicate copies of digital information to exist so when disposing of digital records it is vital that all the various locations that a file could be stored have been considered. These include information that may be stored in:

- University shared filestores (e.g. H: drive or similar)
- Cloud suppliers whose services are provided by the University (e.g. Google Drive, OneDrive), and those that aren't (e.g. Dropbox)
- Emails and email attachments
- Individual devices such as laptops, hard drives and USB sticks, whether University-owned or personally-owned

Staff with access to digital records that are being deleted should ensure that any copies held anywhere in their email folders, files stores and recycle bin are also deleted to ensure completion. Items held in these locations are still held for the purposes of the Data Protection and Freedom of Information Acts. Deletion of an electronic file removes the link to the file but it is possible that the file contents could still be retrieved using technical measures. Consequently, adequate security must continue to be applied to file locations and devices used to hold them until they have been fully expunged or wiped.

System backups will continue to hold copies of deleted digital records until such time that the backup is deleted. Whereas the requirements of the Data Protection and Freedom of Information Acts technically still apply to such records, the Information Commissioner's Office have taken a pragmatic approach to this type of content, recognising that it is possible to put it 'beyond use' while still held so rendering it out of scope. This will only apply if there is no intention to access or use it again, and it would require disproportionate effort to retrieve. However, such records could still need to be retrieved if subject to a court order.

9.4 Records of disposal

For potentially significant information a record should be kept of what has been disposed of, why it was disposed of and who authorised it (i.e. the Information Asset Owner), covering both destruction and transfer to archive. This will ensure there is a transparent audit trail detailing evidence of records that have been destroyed in line with the University's stated procedures. A Records Disposal Form (see Annex 1) must be completed and retained by the relevant Information Asset Owner when records are disposed of. Completed forms should be retained for a period of 10 years for evidential purposes.

It is expected that Disposal Forms are completed when information of potential significance is disposed of, for example:

- Expunging data from a central database
- Bulk disposal of historic student files
- Disposal of financial records that have exceeded statutory retention periods
- Disposal of expired contractual agreements

9.5 Disposal of IT equipment

All disposal of IT equipment must be conducted via IT Services to ensure that it is done securely and that any information remaining on any storage device is securely wiped. IT Services have further information and advice in relation to the [disposal of IT equipment](#).

10. Policy review and ownership

This policy will be reviewed and updated as required, at least every three years, by the Information Governance and Security Advisory Board (IGSAB). The document is managed by the Information Governance Manager in the Secretary's Office.

Annex 1: Records Disposal Form

NOTE: Records must not be destroyed if any litigation, claim, negotiation, audit, Freedom of Information or Data Protection request, administrative review, or other action involving the relevant information is initiated before the expiration of the retention period. They must be retained until completion of the action and the resolution of all issues that arise from it, or until the expiration of the retention period, whichever is later.

Once completed, a copy of this form must be retained by the relevant Information Asset Owner.

Records Disposal Form

Records Disposal Form				
Department / School / Faculty / Division:				
Information Asset Owner (name and role):		Email:		
		Telephone:		
Record title/description:				
Record format:				
Classification: (tick as appropriate)	Public		Open	
	Strictly Confidential		Secret	
Reason for disposal:				
Method of disposal: (tick as appropriate)	Destruction:		Transferred to Archives:	
Method of destruction: (tick if applicable)	Non-confidential waste or recycling		Confidential shredding	
	Digital deletion from University network (e.g. central filestore, database etc)		Digital deletion from other location (e.g. cloud service, mobile device etc)	
Approximate number of records:				
Date of disposal:				

Annex 2: Document history

Version	Author / Primary reviewer	Details of changes	Date	Approved by	Approved date
d0.1 Draft	Information Governance Manager	Initial draft – composed using previous drafts of the Retention and Disposal Policy and Records Management Strategy/Guidance	January 2018	IGSAB	13/02/2018
d0.2 Draft	Information Governance Manager	Minor additions to reflect changes to Records Retention Schedule	February 2018	IGSAB	19/04/2018
v1.0 Approved	Information Governance Manager	Minor edits to sanitise against other policy documents	July 2018	IGSAB	19/04/2018