This policy defines the corporate framework for appropriate creation, maintenance, storage, use and disposal of UWE records.

Records Management Policy

December 2025

dataprotection@uwe.ac.uk

Contents

1. Version Control

Written by	**James Whitbread, Head of Data Protection Office**
Reviewed by	**Jodie Anstee, Chief of Staff and Clerk to the Board of Governors / Director Governance and Legal Services**
Approved by	**Digital and Data Executive Committee; Vice-Chancellor's Executive**
Next review	**July 2028**
Published	**December 2025**
Version	**2.0**

2. Purpose

The purpose of this policy is to define the corporate framework for the appropriate creation, maintenance, storage, use and disposal of UWE records to:

- Facilitate compliance with statutory and regulatory requirements;
- Reduce the risk of unauthorised or unlawful disclosure of information by ensuring records are managed in a controlled way;
- Protect the interests and reputation of UWE Bristol, staff, students, and other stakeholders by maintaining high quality information for as long as required, and to ensure its timely and secure destruction;
- Support continuous improvement in the University's core activities such as teaching, research and decision making, by maintaining accurate and reliable records;
- Provide evidence of corporate governance;
- Support business efficiency and continuity by ensuring information can be quickly located and protecting vital information for the continued functioning of UWE following a major incident;
- Provide evidence in litigation and any other discovery process; and
- Maintain and promote the corporate memory by preserving records of archival value and historical significance.

3. Scope

This policy applies to all records created and processed by, or on behalf of UWE Bristol. This includes records accessed or used by UWE Bristol staff, as well as, for example, contractors, consultants, and postgraduate research students engaged in UWE Bristol-led research.

The policy covers all records created during UWE business and activities.

4. Roles and responsibilities

This policy applies to **all staff** employed by UWE Bristol, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5. Records and information life cycle management

A record is defined as recorded information, in any form (e.g., an electronic file, email, database, system record, hard copy record), created or received by UWE or individual members of staff to support and show evidence of UWE's activities and decisions.

To understand what constitutes a record, the following steps have been defined to describe a records life cycle:

- **Creation and/or receipt**: This part of the life cycle is when we put pen to paper, make an entry into a database/system or start a new electronic document. It can be created by internal employees or received from an external source, and it is complete and accurate.
- **Distribution:** This involves managing the information once it is created or received whether it is internal or external. It occurs when records are sent to someone for which they were intended or were copied. Records are distributed when photocopied, printed, attached to an email, hand delivered or regular mail, etc. After records are distributed, they are used.

- **Use**: This stage takes place after information is distributed. This is when records are used on a day-to-day basis to help generate organisational decisions, document further action, or support other operations. It is also considered the Active Phase.
- **Maintenance** is when records are not used on a day-to-day basis and are stored in the shared drive or relevant system. Even though they are not used on a day-to-day basis, they will be kept for legal or financial reasons until they have met their retention period. The maintenance phase includes filing, transfers, and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision.
- **Disposition** is when a record is less frequently accessed, has no more value to the Organisation or has met its assigned retention period. It is then reviewed and if necessary, destroyed under confidential destruction conditions.

6. Standards

When managing corporate records, the following standards must be adhered to at all times:

- Records must be managed in line with this policy, related procedures, and guidance documents such as UWE's retention schedule;
- UWE will provide guidance on how to effectively access and use records as corporate resources of information;
- All records should be stored and managed digitally where feasible with all necessary provisions made to maintain the integrity, reliability, and accessibility of records during their lifespan;
- Records must be stored efficiently, using appropriate storage methods, and disposing of them appropriately and securely when they are no longer required;
- Records will be managed in accordance with the University's Information Security, Information Handling, Data Protection Policy, and associated guidance;
- Appropriate protection must be provided from unwanted environmental (fire, flood, infestation) or human impact (alteration, defacement, theft);
- Staff must identify and protect records which would be vital to the continued functioning of UWE in the event of a disaster (such as fire, flood, and virus attack). These include records that would recreate UWE's legal and financial status, preserve its rights and ensure that it continues to fulfil its obligations to stakeholders; and
- The University will identify and make provisions for the preservation of records of long term and historical value.

Further practical guidance and information relating to these standards continue throughout this policy.

7. Record keeping quality

The following standards are a minimum requirement to ensure quality records are created:

Records should:

- Be factual, consistent, and accurate;
- Be written legibly, concisely and in such a manner they cannot be misinterpreted;
- Be consecutive when describing events;
- Not contain unnecessary abbreviations, jargon, meaningless phrases, irrelevant speculation, and offensive subject statements;
- Not contain personal opinions regarding individuals, unless documented in a professional capacity i.e., providing opinions on academic performance; and

- Accurately reflect any amendments to ensure a full audit trail. This may include 'voiding' inaccurate records, merging system entries, and documenting manual changes.

Please note, subject to exemptions in law, individuals have a right under data protection legislation to request a copy of the personal information held about them through the submission of a subject access request (SAR). If you are involved in the creation of corporate records, it is important that the content is appropriate and completed with the knowledge that it may be disclosed to the individual should a valid request be made. This includes electronic communications i.e., email, Microsoft Teams, and your work issued mobile phone.

8. Appropriate storage of records

There are several storage options available depending on the purpose of the record and the intended audience. This includes systems such as the student record system and ITOnline, storage solutions such as OneDrive, and collaborative solutions such as SharePoint, and Teams. Depending on the location of the record, the following actions should be taken to ensure all records are secure and accessible to the relevant members of staff:

- Where designated systems are in place, all records should be stored within these systems and complete;
- If there is a requirement to store records outside of designated systems, they should be easily accessible to all those who need to refer to them, especially in the case where business continuity should be considered;
- Records should only be made available to users who have a business need to view the data. This means that personal data should be stored securely in locked folders and sites, with appropriate user access levels applied. Access should be reviewed regularly and updated as and when required i.e., starters, leavers, and internal changes within Departments;
- Duplicating records should be avoided unless there is a business need; and
- Electronic records held outside of systems should be organised into a logical, structured, hierarchical filing system, using appropriately named electronic folders.

When using office 365 tools such as SharePoint and teams, particular attention to restricted access controls needs to be considered due to the usability functions of Microsoft apps. Many apps within 365 enables a user to locate documents for collaborative working purposes, so it is important that all source data made available within these apps is locked securely to ensure only the relevant individuals have access. Please ensure that:

- Membership of the site is accurate and current, and locked to approved members only; This is the responsibility of the Site / Teams Owner;
- If you invite external contacts, please ensure that all information is relevant and that the external contact is approved to be viewing the information; and
- Where data is stored elsewhere on a permanent basis i.e. designated systems, please ensure no duplicated data is retained within these areas if it is no longer required.

Please note, where records contain sensitive personal data an additional layer of security is required, as well as being stored within a secure location. This can be achieved by encrypting documents, or further reducing access levels appropriately. Further information in relation to encryption can be found on the Information Security Toolkit and Data Protection intranet page, referenced in section 19 and 20 of this policy.

9. Scanning of records

When scanning hard copy records where the original is to be destroyed, quality assurance checks must be undertaken. This includes:

- Checking that the document has been scanned correctly, and all information can be clearly seen. This may require you to store the original hardcopy for a limited period to ensure checks are completed prior to destruction; and
- Ensure there is no third-party data / information contained within the document that is not relevant i.e., any hard copy records that contain personal information of multiple individuals that will be stored on individual records.

Do not store any scanned documents on your local drive or desktop. Once you have filed any scanned records, any duplicated versions should be deleted.

10. Classification

Please see the University's Information Handling Policy for more information on classification.

11. Retention

In accordance with data protection legislation, personally identifiable data must not be kept longer than is necessary (i.e., not excessively), and an organisation must define the retention period of all data types. Further guidance relating to retention periods can be found in the Data Protection Guide available on the UWE staff intranet and linked in section 21 of this policy.

Occasionally documents and information held by a department may not be listed on the UWE records management retention schedule. This may be because the information does not constitute a record (for example, transitory information), or it may be a case that different terminology or a wider term is used.

If you hold records that are not included on the retention schedule, please contact the Data Protection Office who will review the entry and will provide guidance on an appropriate retention period, which will be decided based on a legal requirement or an identified business need supported by Data Protection legislation.

12. Confidential destruction

The destruction of records is an irreversible act and must be clearly documented. All records identified for disposal will be destroyed under confidential conditions and in accordance with the UWE records management retention schedule.

A decision for destruction of records must be made by a senior member of staff who has knowledge of the relevant business area to which the records relate. Destruction of records must not take place without recorded agreement to evidence the decision, and consideration should be made regarding the extension of retention periods as detailed in the UWE records management retention schedule.

All hard copy documents that are no longer required or have been scanned into a shared drive must be securely destroyed by use of the confidential waste bins. Information found in normal waste bins constitutes an information security incident and must be reported via ITOnline. Confidential waste bins are available in each site/premises.

13. Records involved in investigations, inquiries, litigation and legal hold

A legal hold, also known as a litigation hold, document hold, hold order or preservation order is an instruction directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit, investigation, or inquiry.

Organisations have a duty to preserve relevant information when a lawsuit, investigation or inquiry is reasonably anticipated. Staff must immediately notify the University's General Counsel if they have been notified of a Litigation, Investigation or Inquiry or have reasonable foresight of a future Litigation, Investigation, or Inquiry as this could result in records being held beyond their identified retention period.

The General Counsel will determine the Legal Hold decision. When a legal hold is terminated, records previously covered by the legal hold should be retained in accordance with the applicable retention period without regard to the legal hold and retained Non-Records or Records not previously subject to retention may be destroyed.

14. Training

All staff and governors are provided with data protection training as part of their induction process, which covers elements of Records Management. This training is renewed biennially as part of staff's mandatory training. Additional training will also form part of continuing professional development, where changes to legislation, guidance or UWE's processes make it necessary.

15. Policy monitoring

This policy will be reviewed and updated as required, at least every three years, by the Digital and Data Executive Committee. The document is managed through the University's Governance and Legal Service.

16. Related policies

This Records Management policy is linked to our:

- Information Security Policy
- Data Protection Policy
- Information Handling Policy
- Acceptable Use Policy
- Remote Access Policy

17. Related procedures

- Information Security Toolkit

18. Related guides

- https://intranet.uwe.ac.uk/tasks-guides/Guide/storing-data#part2
- https://intranet.uwe.ac.uk/tasks-guides/Guide/office-365
- https://intranet.uwe.ac.uk/tasks-guides/guide/using-microsoft-teams
- https://docs.uwe.ac.uk/sites/data-protection/_layouts/15/download.aspx?SourceUrl=https://docs.uwe.ac.uk/sites/data-protection/Documents/UWE%20Records%20Management%20Retention%20Schedules.xlsx