Corporate Records Management Standards

UPR IM11 Appendix II version 07.0

Policies superseded by this document

This document replaces version 06.0 of UPR IM11 Appendix II, with effect from 1 September 2024.

Summary of significant changes to the previous version

See Appendix I, UPR IM11.

Glossary

A glossary of approved University terminology can be found in **UPR GV08**.

Table of contents

1 Managing Records

Records are a vital asset to any organisation and need to be managed efficiently for it to be able to conduct business, account for what has happened in the past and to make decisions about the future. Specifically records are required:

- to provide evidence of actions and decisions
- to support accountability and transparency
- to support decision making
- to protect the interests of staff, students and other stakeholders
- to comply with legal and regulatory obligations, including employment, contractual and financial, as well as the UK General Data Protection Regulation (UK GDPR), Data Protection Act (DPA) 2018 and Freedom of Information Act~~s~~ (FOIA) 2000.

1.1 Aim of standards

These standards provide practical guidance for all University staff on key aspects of managing records including creation (or receipt), capture into recordkeeping systems, storage and maintenance, retention and disposal. They will be applied to all University records, in all formats, including use of the University’s document management system. They have been formulated in accordance with the University of Hertfordshire’s Records Management Policy UPR ‘Records Management and the

Archiving and Retention of Prime Documents' (UPR IM11), relevant University Information Management policies (see section 8) and national standards including, BS ISO 15489 for Records Management.

1.2 What is records management?

Records Management is the efficient and systematic control of records (both paper and electronic) throughout their life-cycle from their creation or receipt until the time of their disposal (see figure 1).

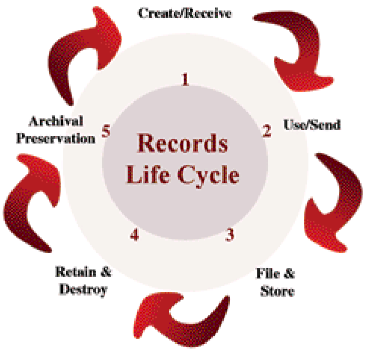

Figure 1: Records Lifecycle

It aims to ensure that records:

- are accurate and reliable
- can be retrieved quickly and easily
- are kept for no longer than necessary

1.3 What are records?

Records can be in any format (paper documents, electronic files, e-mails, databases or scanned images) and broadly speaking are those which have a corporate governance, academic, business, legal, financial or historical value to the University.

Important records to be retained include those which:

- Provide evidence of key decision-making processes and responsibilities (eg Board and Committee records, programme and course validation)
- Are created as a result of a key business transaction (eg Student records, contracts and related records, building projects)
- Are required for legislative or other statutory requirements (eg QAA Institutional Audit purposes)
- Have long-term research value (eg research projects)
- Have historical value (eg major events and initiatives)

1.4 What is not a record?

To make sure that the University does not waste valuable resources keeping unnecessary records it is important to identify those documents which do not need to be managed as records and can therefore be destroyed routinely once they are no longer required. Such records include:

- duplicate records held for reference purposes where the original is held as a formal record elsewhere (eg Board or Committee records, strategy, policy or regulatory documents etc)
- draft documents where a final version has been created and approved, which do not track major policy development
- working papers where results have been written into an official document and are not required to support it
- copies of external and internal Publications, promotional material and similar materials that are publicly available elsewhere
- administration arrangements for lectures, room requests/ changes, meetings, events, conferences etc, which have all taken place
- individuals' day files – these may need to be checked for any important records prior to destruction
- personal diaries, address book etc.
- any other records being kept 'just in case…', there must be a valid reason for holding onto a particular record

1.5 Why manage Records: the benefits

Time	Saves time by ensuring information can be found quickly and easily
Space	Saves space by ensuring records are kept for no longer than necessary
Money	Saves money by reducing storage costs and maintenance costs
Efficiency	Improves efficiency by ensuring information is accurate and accessible
Legal compliance	Improves compliance by keeping documentation in line with and legal regulatory requirements, including Data Protection and Freedom of Information
Control	Keeps information under control by preserving important data and preventing the accumulation of ephemeral material
Quality	Improves the quality of information by reducing unnecessary duplication and providing version control
Security	Increases the security of confidential information
Risk	Supports risk management and business continuity planning
Continuity	Ensures continuity by preserving the corporate memory (regardless of organisational restructuring and turnover of staff)

1.6 Managing records: A quick guide

Responsibilities
• Make sure that you are aware of the University's policies which affect the way you manage records and information. A list of these is available in section 8.
• Define and assign records management responsibilities and authorities to roles and named individuals so that it is clear who is responsible for making decisions and taking necessary actions
• Ensure staff have the necessary records management knowledge and skills

Creating records
• Identify the records which need to be created and received to document business activities and ensure that they are complete, accurate and up to date
• Identify which is the latest version or master copy of a record and ensure it is managed appropriately
• Do not create unnecessary duplicate copies
Capturing records
• Develop adequate recordkeeping systems in shared areas, rather than personal systems, to ensure all records can be located when required by all relevant staff
• Base the arrangement of shared recordkeeping systems on the activities your SBU carries out and the agreed University file structures and file naming conventions. Contact Records Management for advice on this.
• Capture and attach relevant information (metadata) to help interpret, retrieve and manage records
Storing and maintaining records
• Store records in appropriate systems, locations, conditions and in equipment that is appropriate to their media, format and security and access requirements
• Develop strategies to ensure electronic information will remain accessible, readable, usable and can be relied upon and accessed for as long as is required by the University and all relevant external agencies
• Ensure access to records is controlled appropriate to the sensitivity, shared use or importance of the record
• Track and record the movement, location and use of a record
Retaining and disposing of records
• Establish and review how long records need to be kept to meet business needs and legal and regulatory requirements
• Make sure you are aware of the University's policy for retaining records
• Formally assign responsibilities for authorising the disposal of records
• Dispose of all copies of records in all formats securely, considering sensitivity and confidentiality of records
• Make sure destruction of records is recorded

2 Roles and Responsibilities

Records management is a key responsibility of the University and all records created in the course of business belong to the University and not the individual. It is the responsibility of all those working on behalf of the University to carry out their records management duties in accordance with these standards, the Records Management policy and all other related policies and procedures.

Where possible, record keeping responsibilities should be agreed and defined in job descriptions. Training requirements relating to records management should be identified by managers and staff and training provided by records management staff, where necessary.

The Records management Policy, Records Management and the Archiving and Retention of Prime Documents and Business Records (IM11) outlines the specific responsibilities as follows.

2.1 Vice-Chancellor

The Vice-Chancellor has overall responsibility for the authorisation of the records management policy and procedures and will oversee the management of policy and standards within the University.

2.2 Secretary and Registrar

As the chief administrative officer, the Secretary and Registrar is responsible to the Board of Governors for the maintenance of records management within the University.

2.3 Chief Information Officer

The Chief Information Officer is responsible for the implementation, promulgation and promotion of the policy; training; maintaining the technology for the University's records management systems; maintaining the integrity and authenticity of records and for the co-ordination of policy reviews.

2.4 Records Manager

The Records Manager is responsible for overseeing the design, implementation and maintenance of the records management policy and related standards and procedures, as well as monitoring compliance.

2.5 Managers

Managers at all levels are responsible for the management of policy and related procedures through resource allocation and other management support within those areas for which they have responsibility. They will embed the records management practices within normal business practices and ensure records are captured in the appropriate corporate system. They are also responsible for identifying training requirements in records management related issues. Managers will be responsible for nominating key users who will carry out the duties of a key user

2.6 Training, Awareness and Advice

For all training, awareness and advice on records management please contact the University Records Manager.

3 Creating Records

All employees are responsible for creating complete, accurate and up to date records to support the business activities and decision-making processes in which they are involved. The implications of specific legislation and codes of practice should also be considered when identifying what records are required to support this.

The following practice will help in the creation of full, accurate and up to date records:-

- identify where key evidence is required to document activities and decision-making. It may help to draw up process maps of your activities to identify points where the recording of evidence associated with each activity is required;

- do not create duplicate copies of the same record. Identify the master copy of the record and capture into a shared recordkeeping system;

- set up and use shared standard templates and forms for creating records where possible. Nominate specific staff to control the editing and creation of templates and save new templates as a .dot template format; this will create a new document based on the template each time it is opened and ensure the original template remains intact;

- when creating records ensure that they are a true, objective account of what has happened, particularly in the case of minutes or case notes on an individual;

- always attach the following information to a record as a minimum:

  - Title
  - Date
  - Author/ Creator
  - Unique ID (if available).

4 Managing Physical Records

University records will increasingly be managed electronically so the need to keep and store paper records will reduce. However, there are likely to always be a certain number of records which are in paper copy and the following guidance should be followed for paper records.

4.1 Organising Files

Organise files in a uniform, logical way (by date, invoice number etc.) so that documents can be retrieved easily and quickly. Personal files maintained by individual members of staff should only contain 'work in progress', reference or confidential material; all records that other members of the department are likely to need should be held within a centralised filing system. Maintaining departmental files will reduce duplication, allow information to be more easily located if someone is away and ensure greater consistency in the retention and disposal of information.

Only records of a similar nature should be grouped together because if the contents of files are too diverse it will be difficult, not only to locate material, but also to assign appropriate retention periods. In some cases files can be divided into sections for papers with differing retention schedules. The redundant material can then be easily removed at the appropriate time without the need to undertake time-consuming weeding.

N.B. Files which are held electronically do not need to be printed out and stored in physical format providing the proper standards have been applied to the electronic version (see section 5. Managing Electronic Records)

Files should be closed at regular intervals to keep them at a manageable size and also to ensure that the content of 'open' files only relates to current or recent work.

Suitable rules for closing files are:

- when the academic/financial year has ended;
- when a project has come to an end;
- when a file covers a period of more than **5** years;
- when nothing has been added for **2** years.

When a file is closed, no further papers must be added. The disposal date should be recorded on the cover and it should be separated from the active records.

4.2 Labelling and tracking files

To help identify and retrieve the information, record some or all of the following on the file:

- reference numbers/ unique ID codes where available;
- a title which is a brief, accurate and meaningful description;
- the name of the department/section that has created or owns the file
- covering dates of the contents of the file (e.g. Aug 2005-July 2006);
- destruction date.

Track the use and movement of files by using a form to record the name of the person retrieving the file, as well as its reference, title and the date of retrieval. The form can then be inserted in place of the file so that if other members of staff require access, they will know where to find it.

4.3 Storage of active physical records

Active paper and other physical record types (video/ audio tape, microfilm) records required for current business needs should be stored in filing equipment appropriate for storage and security needs as well as being near to where they are being used.

When considering where to store records the following will help.

- **Activity/ frequency of use** – records used on a regular basis should be stored near to the users; those with less frequent use but which have to be kept for several years should be stored in centrally managed University storage areas. Contact Records Management to arrange.

- **Protection required** – make sure records can be adequately secured and protected from environmental effects.

- **Cost** – Storage space is expensive and limited so must be used effectively to store active business records. Clear out unnecessary or duplicate documents regularly.

Storage Units must be strong and have sufficient space, to provide effective storage for records. They must also:

- be secure if holding personal or other confidential records;

- be able to be reached by a person of average height for health and safety reasons;

- protect records from environmental damage such as fire, flooding or vermin - where a flood risk exists the lowest shelf should be 85-100mm off the floor.

Records in all formats can deteriorate if not protected adequately. Simple, common sense measures can be taken to protect them from avoidable damage:

- store paper records away from extremes of temperature, humidity or light;
- avoid sticking important, additional notes onto documents as these can easily become detached. Photocopy these instead and add to the file;

- take care when hole punching paper to ensure content is not damaged;

- use appropriate folders to store paper documents. Avoid using ring-binders and lever arch folders where possible as these are most likely to cause damage and also take up valuable storage space. Cardboard document wallets should be used instead.

4.3.1 University storage areas

The University has a contract in place with a fit-for-purpose, offsite records storage provider for semi-active or inactive paper records and files but these will only be used to store business records as defined in section 1.4 of these standards. If you are in doubt about whether records need to be stored, contact Records Management who will carry out an appraisal of the documents and advise as necessary.

The procedural document 'Managing Physical Records' provides further guidance on how paper records should be organised and managed. Also refer to the storage procedures made available on HertsHub when requesting to deposit new files and records.

These can be found at:

https://herts365.sharepoint.com/sites/Legal-and-compliance/SitePages/Documents-and-Records-Management.aspx

When filing records in boxes please note the following:

- weed out all unnecessary, duplicate or out of date material;
- only records of the same type and age should be stored together so that appropriate indexing data and retention periods can be applied;
- do not pack files and boxes too tightly. Boxes which are too full will damage the records and will also not be able to be lifted (10kg max. weight limit is accepted);
- take records out of lever arch files, plastic wallets and hanging files which all take up space and can be re-used and secure, instead, using treasury tags or cardboard document wallets which can be recycled.

4.3.2 Registering and tracking system using the University Document Management System

All paper and physical records held in central storage areas must be registered into the Physical Records system on the University Document Management System. The system will allow the University to effectively track and locate the movement of all its physical records through an auditable trail, preventing loss or misplacement of records. The system will also be used to monitor and record destruction of records.

5 Managing Electronic Records

The main recordkeeping system of the University will increasingly be the University Document Management System. All records must be captured into the Document Management System where this has been made available for the relevant function.

The Chief Information Officer is responsible for determining the arrangements for the electronic storage of the University's records and documents, in consultation with the Secretary and Registrar. Please consult the Chief Information Officer about any specific requirements prior to considering any local Strategic Business Unit or team arrangements.

The following guidance is recommended for documents and records not yet included in the University Document Management system to ensure appropriate availability and back up It is recommended that Records:

- are stored in a shared area (X:Drive, OneDrive, SharePoint or MS Teams as appropriate) where they can be stored and retrieved by all those who need access to the information;

- should not be maintained on computer hard drives (C: drives or external hard drives) because this is not automatically backed up so there is a greater risk of loss of information due to system or equipment failure;

- should not be stored on portable media (USB, external hard drives laptops) long term as these are insecure, not backed up and, therefore, at risk from damage or loss. If records are stored on portable media for home working purposes or because of system or equipment failure, they should always be stored onto the University's network at the earliest opportunity;

- the storage and use of personal and confidential information must comply with the University's 'Managing Personal and Confidential Information' guidance. Personal information (such as Student or staff records) should not be saved onto portable media as these can easily be accessed if lost or stolen. All staff are provided with secure access to University systems via the UHVPN (University of Hertfordshire's Virtual Private Network) from where they should access this kind of data;

- should only be stored on CDs for short term (up to **3** years); CDs are not suitable for long or medium term storage or for important business records as they are prone to corruption. Where CDs are used they should be stored in cool, dark, dry conditions

5.1 Classification: File structures

Electronic records must be arranged in a consistent, logical way to ensure they can be accessed quickly and easily, properly secured with relevant permissions attached and retained for the correct amount of time. A well-defined folder structure or file plan will enable this.

Wherever possible, folder structures should reflect the functions[1] and activities[2] of the Department or SBU rather than the organisational structure, which is prone to frequent change. Personal named folders should never be used as these do not adequately describe the contents and become out of date with personnel changes.

[1] things the University does to achieve its aims and obligations

[2] actions carried out to achieve the functions

The University's document and record management file structure is determined by the Secretary and Registrar based on national standards and with advice from the Records Manager from whom staff should request advice and guidance when creating and maintaining filing systems.

5.2 Adding Metadata (indexing)

Metadata is data describing the context, content and structure of records and their management through time. This information is used to help identify, retrieve and manage records. Metadata also helps to create an audit trail of a record, ie how it is used and accessed over its lifetime, making it authentic and reliable.

Examples of metadata include:

- Title
- Date created or received
- Version
- Date to or closed
- Author
- Subject
- Unique identifier (eg student number, personnel number)
- Retention and disposal information

The University uses the e-Government Metadata Standard (e-GMS) which recommends the following elements must be applied **as a minimum** to all records and documents:

- Creator
- Date created or published
- Title
- Unique identifier (if applicable)

In addition to these, there are a number of other recommended metadata elements which should be considered. These are:

- Subject (or keyword)
- Version
- Destruction Date

All SBUs should think about metadata requirements and develop local guidelines in line with University standards.

5.3 Titling records

Records need to be identified and retrieved by a number of different people over a period of time so it is important they are titled and indexed or described adequately to ensure this.

In general, titles should accurately reflect the content, be concise and should not include uncommonly understood abbreviations.

Standard University naming conventions have been written to allow for consistent titling to be carried out and can be found in the document Standard Naming Conventions for Electronic Files, folders and Records. These standards should be adopted and local guidelines written within each SBU.

5.4 Version Control

Version control procedures should be applied to documents which are frequently updated (policy etc.). Including a number and date on the title page (and within footers) will reduce confusion over which document is the current version, as well as providing an audit trail for tracking changes.

A version control table on the document could also be used to keep track of what changes have been made and by whom.
Decimal increments should be used so that a distinction can be made between major and minor changes. You can add ‘Draft’ or ‘Final’ to show the difference between drafts and published versions.

For example

- The first draft would be v0.1 draft then 0.2 draft etc.

- Once the document has moved to a final version, then the integer values should begin, so the first final version should be V1.0 Final. Any minor revisions made after this would then be V1.1, V1.2 etc. The second final version would be V2.0 Final etc.

5.5 Unique identifiers

Assign unique identifiers to records where available so they can be easier identified and retrieved. The title of a record alone may not be sufficient because two records could have the same title. Personal names are not adequate either because two people can often have the same name (e.g. Rachel Smith, John Brown etc.) or can change their name. The simplest form is to use a coding which is unique such as student number or staff number. Unique identifiers should also be used in place of personal names in compliance with Data Protection principles.

5.6 Managing Emails

Email is a major medium for business communication and a great deal of ‘corporate knowledge’ is contained in email correspondence which must be retained to protect the rights of the University of Hertfordshire.

Staff should be aware that emails may be evidential records and need to be saved appropriately. They are also legally admissible and may be released under access to information legislation (FOIA, UK GDPR, DPA) or in a Court of Law.

Inboxes should be actively managed to ensure non-business emails are deleted and business emails are managed efficiently. Business emails should be saved alongside related records in the University document management system where available, or in a shared storage area To save emails use the ‘File, Save As…’ option and save as an msg. file, remembering to give the email a clear title which should include the date the email was sent.

Business emails should be retained and disposed of in line with retention policies. It is always the content of the email which determines how long it should be kept for and not the format.

Further guidance on this is available in the best practice guidance ‘Identifying and Managing Emails as University Records’.

5.7 Scanning records

Scanning paper records is sometimes seen as a way of freeing up valuable storage space and, whilst this is true, it is not always necessary or resource efficient to do this. In general, records with a short to medium retention are not worth back-scanning unless frequently accessed by many people instead, they should be stored offsite and possibly scanned as required. Records which are created electronically should always be captured in their original format rather than printing then re-scanning.

The University has taken the overall decision not to undertake large-scale back-scanning of paper record, opting instead for a ‘from today forwards’ approach where required. However, there may well be valid business benefits to carrying out back-scanning in some areas – these will be assessed on an individual basis. Business Units should always consult the Chief Information Officer before undertaking any large-scale scanning exercise.

If scanning is to be carried out it is important to ensure the following:

- scanned images are an accurate duplicate of the original record, ie, all information is captured and of excellent quality;

- the correct dpi is used as follows to ensure readability:

    - Standard text documents – minimum 200 dpi
    - Drawings, maps and plans – minimum 300 dpi
    - Documents with faded text or fine detail – 600 dpi;

- written scanning procedures are in place;

- scanned records are authenticated, where necessary, with metadata etc;

- the quality of the scanned image is checked and verified before the physical record is destroyed. It is advisable to keep the paper record for up to **90** days in case of any problems with the scanned version;

- some important records (e.g. major contracts, deeds etc.) should also be kept in physical format but these can be stored elsewhere, records management can advise.

5.8 Preserving digital records

Electronic records should be reviewed periodically and, if necessary, migrated to new software so that they do not become inaccessible due to obsolete technology. Records with a mid to long-term life-span (i.e. over **5** years) may need to be part of a programme to ensure they are accessible and useable for as long as required by the University.

Consideration should be given to the long-term preservation needs of a particular record at all times. It is important to preserve records adequately in order to make sure they continue to provide an accessible, useable and authentic record of the University's activities.

To identify electronic preservation requirements, consider the following:

- identify the records you create and their overall value to the University;
- establish the retention on these records using the University retention schedule and advice from Records Management. In general, only those records with a retention of longer than **5** years need to be considered;
- determine the likelihood of losing the records and the impact to the University in terms of:
  - How serious the consequences would be;
  - How high the risks are to the records in their current format;
  - How expensive it would be to preserve or replace the records.

5.8.1 Methods for electronic preservation

There are three main options available, these are:

- **Emulation** – software is used to mimic a piece of hardware or software which preserves access to the electronic records. This method preserves the original feel of the record by maintaining its appearance and style. It will require IT specialists to create this software.
- **Migration** - transfers records from one generation of hardware/software to the next, for example converting a document from Word 6 to Word 7. The content of the record is preserved, though not always the original look and feel, and it is a labour intensive option.
- **Technological preservation** - involves keeping the original hardware and software. It can be an option for records that will only need to be kept for a very short period of time by simply maintaining them on their existing format and equipment. This option may be dependant on continuing maintenance contracts for the equipment and software and also carries a risk of breakdowns in the technology used.

6 Security

The management of the security of information and records is essential to protect the information assets of the University and its stakeholders. This ensures business continuity, minimises risk and protects the rights of individuals about whom we hold information.

In order to mitigate the risk of security breaches or accidental damage or loss, there are some general good practice procedures which should be followed, these are provided below. Staff should also read the IT and Computing Regulations (UPR IM20) for further information.

- Clarify the access requirements of staff to establish who needs to retrieve particular documents, who can edit those documents, and who is authorised to delete them.
- Information that is only accessible to a single person should be kept to a minimum: as far as possible, records that other staff may require should be stored within an appropriate folder on a shared network so that departments can operate effectively if individual members of staff are away.
- Access to confidential information (e.g. personal data) should be controlled through the use of ID log-ins, passwords and read-only settings, and computers must not be left unattended when logged-on.
- Screen lock computer screens when absent from your desk or work area when away at meetings so they are not left as readable. This can be done by selecting CTRL+ALT+DEL keys then selecting the Lock Computer option.
- Staff should be aware of the risks of transporting data and records on portable media such as USBs and laptops. This should be avoided as much as possible and staff should use the UHVPN (University of Hertfordshire Virtual Private Network) to access data and records.
- The integrity of data is of paramount importance if it is considered the primary, definitive record of a transaction. Adequate audit trails, allowing all actions to be traced to a person, date and time are essential.
- Store confidential paper and physical records in a lockable filing cabinet and storage facilities.
- Unencrypted sensitive or personal data must not be sent via email as this can easily be intercepted.

7 Retaining and Destroying Records

The University needs to make sure its business records are retained for as long as necessary for it to be able to carry out its core functions and comply with relevant legal obligations. It also needs to destroy records in a timely manner to ensure the efficient use of both physical and server storage space and minimise the risk of breaching the Data Protection Act.

The University Retention Schedule in the UPR Records Management and the Archiving and Retention of Prime Documents and Business Records – IM11 sets out the amount of time that the University needs to keep certain types of records. It applies to records in all formats, including paper and electronic information. The UPR identifies the main University business records (Boards and Committee minutes, student files etc.) which need to be retained but it is constantly being updated and developed to include more records series.
Where records are not on the retention schedule it may help to consider the following before you decide to destroy a record:

- how likely is it that we will need the records again for business purposes?
- how serious would the consequences be if we did not have the records?
- how expensive is it to keep the records?
- what long-term research/ historical value do these records have?

If you are in any doubt about what to do you should contact the Records Manager for advice.

7.1 Records retention and Data Protection

A retention schedule also helps the University to comply with specific pieces of legislation. The Data Protection Act stipulates that information should be held for as long as necessary and no longer so it is vital that a policy for how long we should be keeping data on individuals is in place.

7.2 Records retention and Freedom of Information

Freedom of Information does not require that all records are retained forever, just in order to comply with a request for information, as is a common misconception. Instead, the University must retain its records and information for as long as required to support its decision making processes and business activities. The University needs to dispose of its records in a timely, compliant manner and be able to have the policy to support its disposal decisions and actions.

7.3 Records disposition

When a record comes to the end of its retention there are three (**3**) possible actions to be taken, these are:

- record is destroyed;
- records is reviewed and retained for a further retention period;
- record will be retained permanently for research or historical purposes.

The vast majority of the University's records that have reached the end of their retention period will be destroyed with a very small number being retained permanently.

7.3.1 Destruction

When records are destroyed, the proper procedures need to be in place to make sure they are disposed of correctly and that there is an audit trail of their destruction.

Good Records Management practice ensures that destruction is done in a timely secure manner with the following:

- destruction should be authorised by a designated officer in line with retention policies and destruction procedures;
- sensitive and personal information should be destroyed in a confidential manner;
- all duplicates of the records authorised for destruction should also be destroyed;
- appropriate evidence of what has been destroyed should be retained.

Confidential paper records, including those stored off-site, will be destroyed confidentially by the University's contractor. A record should be kept of all those records that have been destroyed along with the date they were destroyed.

Records stored in Offices which are due for destruction should be put into confidential waste sacks for collection by the Estates department. If you have confidential waste to be collected please keep in a locked office and contact the Estates department for collection at the earliest opportunity. Confidential waste sacks should not be left where they can be accessed freely.

7.3.2 Permanent records

Governance Services is responsible for managing the University's Board and Committee papers.

The University also has a small archive relating to the history of the University. This houses a collection of business and historical material from the 1950s to the present day including: Annual Reports, Photographs from Graduations, University publications such as the Prospectus and other historical documents from Hatfield Polytechnic and other colleges (Balls Park, Wall Hall). All records which are deemed to have a long term, historical value to the University, and need to be managed as such, should be stored here.

8 Relevant Legislation, Standards and Guidance

8.1 Relevant UK legislation and Records Management Standards

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act (DPA) 2018
- Freedom of Information Act (FOIA) 2000
- Code of Practice on Records Management under Section 46 of the Freedom of Information Act 2000
- Environmental Information Regulations 2004

- BS ISO 15489 Information and Documentation – Records Management – Part 1: General
- BS ISO 15489 Information and Documentation – Records Management – Part 2: Guidelines
- BIP 0008:2004 Code of Practice for legal admissibility and evidential weight of information stored electronically
- PD 00016:2001 Document Scanning – Guide to scanning business documents

8.2 University Records management Policies and guidelines

- Guidelines for creating and maintaining electronic filing areas
- Identifying and Managing Emails as University Records
- Managing and organising Physical Records
- Records Management and the Archiving and Retention of Prime Documents and Business Records - UPR IM11
- Scanning Records: Guidelines (in draft, available later in 2009)
- Standard Naming Conventions for Electronic Files, folders and Records

8.3 Associated University Information Management policies and guidelines

- IT and Computing Regulations – UPR IM20
- Data Protection Policy and Privacy Statement – UPR IM08
- Freedom of Information – UPR IM09
- Information Management Principles – UPR IM02
- Data Management Policy – UPR IM16

9 Glossary of Records Management Terms

Term	Description
Active Records	See ‘Current Records’
Appraisal	The process of evaluating an organisation’s activities to determine which records should be kept, and for how long, to meet the needs of the organisation, the requirements of accountability and the expectations of researchers and other users of the records.
Archives	Records that are recognized as having long-term (including historical and cultural) value.
Authenticity	An authentic record is one that can be proven to be what it purports to be, to have been sent by the person purported to have created or sent it and to have been created or sent at the time purported.
Classification	The process of devising and applying schemes based on business activities which generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal.

Term	Description
Current Records	Those records which are being regularly used for the conduct of business (see also 'records lifecycle').
Data Protection Act 2018	Along with the UK GDPR, provides legal rights to individuals with regard to the personal information held about them by others (see: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted).
Disposal	The implementation of appraisal and review decisions. These comprise the destruction of records and transfer of selected records to the Archive. They may also include the movement of records from one system to another (e.g. paper to electronic) or the transfer of custody of the records.
Disposition	A range of processes associated with implementing records retention, destruction or transfer decisions (e.g. disposal, review, and archive)
Document	The smallest unit of filing, generally a single letter, form, report or other item housed in a filing system
Document Management System	An electronic system that is used to store, organise, retrieve and manage records received or created by the University. Such a system offers the functionality of organising (or classifying) records into a relevant structure, managing retention schedules and providing audit trails of how a record has been used and by whom.
Electronic Records	Records where the information is recorded in a form that is suitable for retrieval, processing and communication by a digital computer.
File	A group of related documents contained within a file cover and fastened together. A virtual file can be created for electronic documents.
Freedom of Information Act 2000	Provides a general statutory right of access to information of any age and in any format held by public authorities, subject to a number of limited exemptions (see: https://ico.org.uk/for-organisations/guide-to-freedom-of-information/)
Hardcopy	All information that is not held in an electronic format and can be read without additional equipment. Includes files, maps and plans, and bound volumes.
Indexing	The process of attaching key data (see Metadata) to a record to enable it to be described, identified and retrieved efficiently
Integrity	The integrity of records refers to its being complete and unaltered

Term	**Description**
Medium	The format on which a record is held, i.e. paper, microfiche, microfilm, electronic, optical disc, magnetic tape etc
Metadata	Information about an organisations records, including information about their nature, extent and location, the context of their creation or receipt, the means of access to them and decisions relating to their future management.
Non-current Records	Those records which have little or no business value, though they may be used for other purposes, such as historical research (see also ‘records lifecycle’).
Physical records	See ‘Hardcopy’ records
Record Series	A collection of records having a common subject or theme or function e.g. annual accounts, invoices, committee minutes, Head of Department’s correspondence files etc. A series is distinguished by the fact that it provides evidence of a particular process and as such may vary in size from a single document (e.g. School Strategic Plan) to many thousands in the case of invoices.
Records	Those documents required to facilitate the business carried out by the University and retained for a set period to provide evidence of its transactions or activities. Records may be created, received or maintained in many formats including hard copy, or electronic format.
Records Lifecycle	A concept for describing the various stages through which information passes. Records are **current** from their creation and for as long as their business/ administrative value remains at its highest. They become **semi-current** when their administrative value declines and reference to them becomes irregular and less frequent. When a record has ceased to have any administrative value at all it is **non-current.**
Records Management	The field of management responsible for the efficient and systematic control of the creation, maintenance, use and disposition of records.
Records Audit or Survey	A systematic exercise to locate and identify all the records held by a particular business area.
Registration	The process of records creation and its recording in an appropriate finding aid, such as a register, index, computer database etc.
Reliability	A reliable record is one whose contents can be trusted as a full and accurate description of the transactions, activities or facts to which they are evidence of.

Term	Description
Retention Schedule	An index to different types of records, detailing how long they should be kept for in order to meet operational and legal requirements. For example, to meet VAT and taxation regulations, there is an obligation to keep most financial records for the current year +6, making the effective period of retention 7 years
Semi-current Records	Those records whose business value has declined, but which may still be referred to on an irregular basis (see also 'records lifecycle').
Tracking	Capturing and maintaining information about the movement, use and transaction of records.
UK General Data Protection Regulation (UK GDPR)	The UK GDPR is the UK amended version of the GDPR post Brexit and, along with DPA 2018, provides legal rights to individuals with regard to the personal information held about them by others.
Usability	A useable record is one that can be located, retrieved, presented and interpreted.
Version Control	A procedure which seeks to identify and manage records which are subject to intensive redrafting, thereby enabling differences in authorship and content to be logged and controlled.
Vital Records	Those records crucial to the conduct of the University's business and without which the University would be unable to function should they be destroyed by fire, flood or any other catastrophe. Identification of vital records would form an integral part of any business continuity planning."

Sharon Harrison-Barker
Secretary and Registrar
Signed: **3 January 2023**

Alternative format
If you need this document in an alternative format, please email us at governanceservices@herts.ac.uk or telephone us on +44 (0)1707 28 6006.