University for the Creative Arts

Records Retention Policy

V2

January 2021

Approved by: University Executive Group
Date originally approved 11 March 2019
Review period: 1 year (thereafter 3 years)
Approved: 19th January 2021
Review Date: 19 January 2024

Document History

Version History

Version no	Status	Policy Author	Approved by	Date
1	Approved	Marion Wilks, University Secretary	UEG	11 March 2019
2	Approved	Marion Wilks University Secretary	UEG	19 January 2021

UNIVERSITY FOR THE CREATIVE ARTS

Records Retention Policy

1. Introduction

The aim of this Policy is to ensure that records are managed consistently across all departments and Schools and are retained for as long as necessary to meet operational and business needs, and to demonstrate compliance with legal, regulatory and audit requirements. It applies to all records in whatever format they are held (paper or electronic). The retention schedules to which this Policy refers also take into account relevant requirements of the University's regulations and policies, as well as recommendations of the Joint Information Systems Committee (JISC) Retention Schedule and common practice within higher education.

The University Solicitor is responsible for the University Retention Policy. It is the responsibility of departments and Schools to retain the items listed in the schedules and within the departments themselves specific individuals should be assigned responsibility for each category.

2. What is a retention schedule?

The University Retention Schedules are the practical implementation of the Records Retention Policy and their aim is to help staff to control their records effectively, preventing information from being either destroyed prematurely or retained unnecessarily.

Retention Schedules are developed by departments with overarching responsibility for key functions as listed in Appendix 1.

A retention schedule lists the length of time for which categories of records should be retained in order to meet business and operational needs, as well as to comply with legal, audit and regulatory requirements. It records:

- The subject of the records being held by the University
- The format in which the master records will be retained and kept secure (electronic or paper)
- The storage system (name of system)
- The maximum retention period and the event which triggers that start of the retention period (e.g. the expiry of the contract, the end of the current academic year)
- The rational for the retention period (e.g. time limit in the Limitation Act 1980)
- The method for the destruction of records

Where a schedule indicates the retention period as 'N/A', this indicates that the record should be disposed of as soon as the trigger event occurs.

The rationale column provides the reason for the retention schedule (often based on legislation). Subsequent columns deal with where the master record is stored.

Any records that cannot be assigned definite retention periods (because it is not possible to determine the length of their continuing value) should be reviewed at regular intervals. When the time for the review comes, the records must be appraised and a decision made whether to keep them permanently, discard them or review them for a second time. If a second review is to take place, a date for this must be agreed and recorded.

3. Why are retention schedules required?

Retention schedules are central to achieving organisational efficiency, as well as legal and regulatory compliance. Retention schedules:

- Provide a consistent, controlled system for the disposal of material
- Prevent records from being discarded prematurely
- Ensure information is not kept unnecessarily
- Help to save space, time and money

Article 5 (1) (e) of GDPR requires personal data to be 'kept in a form which permits identification of data subjects for no longer than is necessary'. Assigning retention periods to records is therefore a critical part of ensuring that data protection is not breached.

The Freedom of Information Act requires transparent, auditable systems for the management of records. The Lord Chancellor's Code of Practice on the Management of Records (issued under section 46) states that 'disposal of records should be undertaken only in accordance with clearly established policies which have been formally adopted and enforced by staff.'

In addition, under section 77 of the Act it is an offence to destroy any document held by a public body to prevent disclosure of information. It is therefore essential that departments use coherent, clearly defined procedures for discarding records, so that they can demonstrate that their information has been destroyed legitimately and not to avoid disclosure.

4. ICO advice on how long to keep information

When deciding how long to keep information, the ICO suggests that organisations need to consider:

The needs of the University
The current and future value of the information
The costs, risks and liabilities associated with retaining the information
The ease or difficulty of making sure the information remains accurate and up to date.

Detailed points to consider, together with the limitation periods during which legal proceedings can be commenced, are set out in Appendix 2.

5. Deviation from the Published Retention Period

Deviation is where a department or School decides to retain some or all of their records for a longer/shorter period of time than that specified by a University retention schedule. Deviations should be by exception only and must be justifiable.

Example of a justifiable deviation

Under the Limitation Act 1980, people aged 18 years or over have six years in which to raise a civil claim against the University. Therefore, retention schedules affected by this act often state that records should be retained for the current year, plus a further six years (i.e. up to seven years), in order that they are available in the event of a civil claim. However, where a person is under 18, the six-year period in which they can raise a claim does not begin until their 18th birthday. Therefore, a record may be kept for a longer period, dependent on when the individual's 18th birthday occurs).

6. Professional, statutory and regulatory bodies

Some records (usually relating to academic courses or research) are governed by a variety of professional, statutory and regulatory bodies, all with their own requirements affecting the maintenance and disposal of their records. Where applicable, this should be highlighted in the notes section of the University Retention Schedules (see template in Appendix 3).

7. Implementation

Responsibility for implementing the schedule will need to be assigned to appropriate members of staff (e.g. Heads of Department) and a system (manual or automatic) should be devised to alert them when particular records are due for disposal or destruction. Staff assigned this responsibility, or staff who are delegated this responsibility, should be permitted adequate time to carry out their duties in an efficient and timely manner. For example, staff responsible for the disposal of records which expire at the end of an academic year, should be permitted time to carry out this disposal in July and/or August each year.

The master record should ideally be the only copy of a record, however it is acknowledged that in practice there may also be copies of the record held in other formats and/or by other departments for justifiable reasons. Some schedules may distinguish explicitly between retention of masters and copies. However, where no such distinction is made, the following applies:

- Copies made for convenience purposes (e.g. printed for meetings, put onto a data stick for use off-campus etc.) should be held for as short a time as is practicable;
- Copies made for other business reasons should be held for no longer than the master record.

Upon the disposal of the master, efforts should be made to ensure that all copies (paper and electronic versions, including those held on laptops or in email) have also been

eliminated, otherwise the information will be considered still held by the University and therefore accessible under the terms of GDPR and Freedom of Information legislation. Where feasible, all portable media devices should be encrypted.

8. Storage and preservation

Documents need to be arranged systematically and labelled so that it is possible to locate them with ease and respond promptly to enquiries. File covers for paper records should be labelled with disposal dates, so that it is easy to locate material due for destruction. In the case of electronic information, a logical hierarchical structure of folders, sub-folders and metadata should be used to ensure that documentation can be readily identified for deletion.

Departments should ensure that any records held electronically remain accessible and do not become inaccessible due to obsolete technology. It is advisable that departments review their data periodically (ideally every five years) and, if necessary arrange for it to be converted to new file formats.

There is always a risk of portable media (e.g. USB memory sticks, CDs, DVDs) degrading or becoming corrupted; it is therefore good practice for all critical, long-term data to be held on a central server.

9. Disposal

9.1 Implementing Disposal Decisions

Disposal decisions should be implemented in a timely and effective way. This means monitoring the retention periods and taking appropriate disposal action when they come to an end. The required disposal action should be documented in the retention schedule and should be one of the following:

- Destruction of records (electronic deletion or shredding)
- Transfer of records to an in-house archive or external archives service
- A further review of records, if necessary
- Transfer of records to a successor body, if applicable

The method of disposal should also be identified in the schedule; eg automated, manually triggered, manual)

9.2 Routine Destruction

There are many documents that can be routinely destroyed as part of normal business practice with only short-term value or containing unimportant/duplicate information such as:

- Convenience copies (see section 7 above)
- Compliment slips

- Notices of meetings
- Notifications of acceptances or apologies
- Trivial emails
- Draft letters / documents
- Out of date reference material
- Obsolete publications, manuals, directories
- Superseded address and distribution lists

9.3 Recording Disposal

It is essential to record what is disposed of, when and why (except with unimportant documents (as above).

Recording the disposal of information will ensure that there are transparent, accountable records that the retention policy and schedules have been implemented and prevent futile searching for material no longer in existence. Both the Freedom of Information and GDPR provide procedures and guidance, since explanations for the destruction of records may have to be given in response to requests for information.

9.4 Secure Destruction

Electronic and physical records of a restricted or sensitive nature must be stored and disposed of securely using either a third party confidential destruction process, shredding or by electronic deletion. Bins or sacks containing confidential waste or personal data must not be stored in public or insecure places.

9.5 Delaying Destruction

If there is any doubt concerning the destruction of records (because of pending litigation or investigation), it is advisable that they be retained and reviewed at a later date; a specific data for the review should be recorded. Similarly, if records are known to be the subject of a request under Freedom of Information or GDPR, destruction must be delayed until either disclosure takes place or the complaint/appeal procedures are concluded.

9.6 Monitoring Disposal

The University Solicitor or nominee will annually monitor the disposal of records in line with departmental retention schedules.

Appendix 1

Responsibility for Devising and Maintaining Retention Schedules

Function	Responsible department/role
Marketing and Student Recruitment (outreach, UK partnerships, enquiries, alumni)	Student Recruitment, Marketing & Engagement
International recruitment (agents, progression partners, exchange partners)	International Studies
Student Application and Admissions	Student Recruitment, Marketing & Engagement (Admissions)
Student Administration (enrolment, assessment, graduation, certification, tuition fees, scholarships and bursaries, student loans, study trip assessments)	Academic Registry
Student support (library, disability, welfare, learning support, bursary/hardship administration, cause for concern, support to study, careers, VADs)	Library & Student Services
Student Complaints, Appeals, Mitigating Circumstances, Academic Misconduct	Quality Assurance & Enhancement
Student Disciplinary	Deputy Vice-Chancellor (Academic)
Student Safeguarding (FE)	Head of the School of Further Education
Prevent Duty Records	Deputy Vice-Chancellor (Academic)
Research Students (administration, enrolment, supervision, examination)	Research Office
Quality Assurance (programme/unit specification, validation, review, annual monitoring, external examining, academic committees, examination boards (inc chairs actions), collaborative partnership agreements)	Quality Assurance & Enhancement
Information governance (Breaches, FOI requests, Subject Access Requests)	University Solicitor
Governance (Governors, Board of Governors and Committees)	Clerk to the Board of Governors
Human Resources (staff recruitment, employment, DBS/immigration checks, contracts, personnel records, appraisal, disciplinary, grievance, leave, payroll, PAYE, training and development)	Human Resources
Health & Safety (accidents, near misses, emergency incidents)	Health & Safety Manager
Financial Records (Procurement, payments inc payroll and bursaries and scholarships, online store, student fees, debtor invoices, tax returns, statutory returns, insurance)	Finance

Estate records (Staff and Student Parking Permits; Security information; CCTV images; Reception visitor signing in records)	Estates

Appendix 2

How to decide how long to keep personal data for.

Topic	Points to consider	Examples given by the ICO
The purpose for which the University collected the information	Why did we collect the information in the first place? For what purpose are we using the information now? Does the reason we collected it in the first place still apply? Are there any other purposes for holding the personal data? (take care not to delete information because one purpose has expired when another purpose is still valid. Ensure there are sound reasons for retaining the data and that we are not keeping it 'just in case' Is this a copy of the information; is the master held centrally?	If a bank holds personal data about customers and uses this information as part of its security procedures, it is appropriate to retain this data for as long as the customer has an account with the bank. After the account has been closed, the bank may also need to continue holding some of this information for legal or operational reasons. CCTV images collected to prevent ATM fraud may need to be retained for several weeks because suspicious transactions may not become clear until the victim gets their statements. Conversely a pub CCTV system may only need to retain images for a short period because incidents will generally come to light quickly, unless crime is reported to the police and the police need to see the images.
Is the data being kept for historical, statistical or research purposes?	Is there a value in retaining the records for historical, statistical or research purposes?	Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of technical

Topic	Points to consider	Examples given by the ICO
	For how long will it be used for these purposes before it can be deleted? Are we sure we are not using it to make decisions that affect individuals or in a manner likely to cause damage or distress? Can any of it be anonymised?	and organisational measures in order to safeguard the rights and freedoms of the data subject.
Should the information still be kept if the relationship has ended?	What information is no longer necessary given the ending of the relationship?	You may need to keep some information in case a complaint is raised, reference requested, tribunal action brought, to verify (or help alumni evidence) qualifications awarded. You may need to keep information that can confirm the relationship existed and that it has ended; as well as some of its details.
Should the information be kept in case someone brings a claim against the organisation?	Is the information needed to defend the University against potential legal claims in the future? If so, is there information that could not possibly be relevant to such a claim, that can be deleted? Is there no longer a possibility of a claim arising (i.e. has the relevant statutory time limit expired – See below) When and how should routine destruction of documents be suspended, if it is suspected that the individual may be involved in litigation, investigation or criminal proceedings.	Where an employer receives many applications for a job, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

Topic	Points to consider	Examples given by the ICO
Are there any legal, regulatory or professional requirements for keeping the information?	For example is the information needed for tax, audit or health and safety reasons?	Statutes may set out periods defining how long certain types of data should be kept: Public companies must keep accounts for a minimum of six years FSA guidance says companies must keep certain tax information for at least six years. The table below sets out limitation periods within which to commence legal proceedings. These are minimum periods, there may be an operational need to retain the information for a longer period. Recommendations about retention of certain recorded material are set out in the ICO's CCTV Code of Practice.
Should certain information be kept because it is shared with another organisation?	What has been agreed with the other organisation about how long the information is needed and what should be done with it when it is no longer needed? Should the information be deleted or returned to the other organisation? Should the other organisation be asked to return or delete information that it is processing on our behalf?	Data about Company A's customers is shared with Company B, which is negotiating to buy Company A's business. It is agreed that Company B will keep the information confidential and use it only in connection with the proposed transaction. When the sale does not go ahead, Company B should return the customer information to Company A without keeping a copy.

Limitation Periods

There are certain time limits by which a claim must be brought that are set out under statute. If the action is not begun within the relevant period then it will be time barred (unless a valid standstill agreement has been entered into).

In brief, the law on limitation periods is set out in the Limitation Act 1980. It provides for:

- 6 years for actions in respect of simple contracts and of tort (civil liability for breach of obligations imposed by law).
- 12 years in respect of an obligation contained in a deed.

Example limitation periods.

Nature of Action	Starting Point	Length of period
Simple contract	The date of the breach of contract	6 years
Tort (other than personal injuries, under the Consumer Protection Act; latent damage (usually property defects); defamation)	The date the damage is suffered	6 years
Defamation	The date of the cause of the action	1 year
Latent damage	Later of (a) The date of the cause of the action (b) Date of knowledge of the cause of the action	(a) 6 years (b) 3 years
Action under the Consumer Protection Act 1987	Later of the date of the cause of the action or knowledge of it	3 years
Action to recover land, proceeds of sale of land or money secured by a mortgage or charge	Date of the cause of the action (i.e. dispossession of discontinuance of possession)	6 years
Action to recover rent	Date arrears become due	6 years
Action for non-fraudulent breach of trust	Date of cause of the action	6 years
Action for fraudulent breach of trust		unlimited

Appendix 3 Retention Schedule Template populated with examples

Department/School owning the Records: Admissions

Record Category	Format	Master storage system	Retention Period Begins	Retention period	Disposal Action/Method	Rationale	Notes including any other systems to which data is tranferred	Responsibility for Disposal
Admissions data held in the UCA SITS student record system for applicants who start the online application form but don't submit it*	Electronic	SITS student record system	Date application is started	One year after the date of application or end of the following application cycle, whichever is later. Applicants can request for this data to be removed prior to this date and are told this in a privacy statement prior to submitting any data.	Electronic deletion triggered manually	To enable the applicant to return and complete the application form without having to enter details again.		Student Records & Systems
Admissions data held in the UCA SITS student record system for applicants who enrol at UCA*	Electronic	SITS student record system	Date of application	Concurrent to student data retention policy, six years after last year of student enrolment. Records which need to be retained for UKVI audit purposes may need to be retained for longer than this period, in line with UKVI regulations.	Electronic deletion triggered manually	To enable application data to be viewed and analysed against student data, as detailed in our data protection privacy notice(s), to conduct research and analysis, including to produce statistical research and reports. To respond to claims of a breach of contract.	Data will also be exported from the student record system for the purposes of research and depersonalised so as to be disconnected from any individual at the end of the admissions cycle they applied in.	Student Records & Systems
Admissions data held in the UCA SITS student record system for applicants who do not enrol*	Electronic	SITS student record system	Date of application	One year after the start date of the course, if no alternate student record exists. Otherwise, data will be held in line with student data retention policy to ensure we have a complete picture of the student's record. Records which need to be retained for UKVI audit purposes may need to be retained for longer than this period, in line with UKVI regulations.	Electronic deletion triggered manually	This enables applicants who re-apply in subsequent years to have a streamlined and fast-tracked application process, where they only need to update their details. It also enables us to access information about applicants who were unsuccessful.	Data will also be exported from the student record system for the purposes of research and depersonalised so as to be disconnected from any individual at the end of the admissions cycle they applied in.	Student Records & Systems

Department/School owning the Records: Registry

Record Category	Format	Master storage system	Retention Period Begins	Retention period	Disposal Action and Method	Rationale	Notes	Responsibility for Disposal
Facts of registration and academic performance (dates of study, progression, programme of study, marks, final award etc)	Electronic	SITS	Year following last year of enrolment	Perpetuity	N/A	Provision of references and confirmation of registration/final award etc.		
Full student records, including documents relating to academic progress, achievements and conduct; transfer, withdrawal or termination of studies	Electronic	SITS student record system	Year following last year of enrolment	6 years	Electronic deletion triggered manually	Limitation Act 1980	Award data and student profiles are archived and retained permanently	Student Records & Systems