Records Management Policy
of
University of Kelaniya

Table of Content

1. Introduction

The University of Kelaniya recognizes that the management of its records is necessary to support its core functions, to comply with its legal, audit and regulatory obligations, and to contribute to the overall management of the institution. This policy sets out principles for ensuring that the university has an effective process to manage its records.

This policy relates to all types of records created or used by university staff and students, and fulfils the requirements of laws of the country, regulations, business processes and policies of the university.

Records exist in a wide variety of formats and can include, but are not limited to, paper-based documents and files, electronic documents (including e-mails), spreadsheets, presentations, databases, clinical data, medical records, photographs, microfiche; social-media, webpages, film, slides, video and in electronic (digital) or hard copy (physical) format.

2. Purpose

The records of the university are a vital corporate asset. They provide evidence of its actions and decisions, and must be managed in a consistent, controlled way to ensure transparency, accountability, and legal compliance. The purpose of this Policy is to:

1. Ensure that, regardless of format or structure, the university's records possess the characteristics of authenticity, reliability, integrity and usability, and to be considered authoritative evidence of events or transactions and to fully meet the requirements of the university;
2. Ensure efficiency and consistency in the creation, maintenance, retention and disposal of records;
3. Support decision making by maintaining accurate and reliable documentation;
4. Provide robust audit trails to evidence decisions and the reasons for decisions;
5. Support operational efficiency by ensuring that information can be quickly located and retrieved;
6. Comply with statutory and regulatory requirements affecting the use and retention of records;
7. Protect the interests of the institution, its staff, students and other stakeholders by maintaining high-quality documentation for appropriate lengths of time;
8. Prevent unauthorized or unlawful disclosure by ensuring information is held securely;
9. Support business continuity by protecting information that is vital to the continued functioning of the university;
10. Ensure the timely, secure destruction of information as per retention schedules; and
11. Preserve corporate memory by preserving records of historical significance.

3. Scope

This Policy applies to:

1. All records that are created, received, or held in any format (e.g. physical, digitized or born-digital) within an information system, electronic document management system or a physical store during their lifecycle. This includes all records created and received as a result of transactions, research, teaching and learning, student administration and services, and all software applications that generate records including email, databases, office applications and websites; and
2. All employees of the university and all other parties conducting business on behalf of or acting as a representative of the university.

4. Key elements of the Policy

The Records Management Policy sets out principles for managing the university's information effectively. It applies to all records – whether paper or electronic – that are created or used by staff. The key elements of the policy are:

1. The university's records are a vital, corporate asset: they provide evidence of its actions and decisions, and must be managed in a consistent, controlled way to ensure transparency, accountability and legal compliance;
2. Staff shall know what information they hold and where it is held;
3. All records – whether paper or electronic – should be organized in a systematic way to ensure they can be quickly and easily retrieved;
4. Information shall be held securely to prevent unlawful disclosure and to protect expectations of privacy;
5. Where appropriate, data should be shared across the university to avoid recreating information that already exists and storing duplicate data unnecessarily;
6. Faculties/Departments/Centres/Units/Branches shall control the disposal of their core administrative records as per agreed retention schedules so that they are managed efficiently and only destroyed legitimately;
7. Vital records shall be protected to ensure business continuity;
8. Emails record the university's actions and decisions, and shall be managed as effectively as paper and other electronic records;
9. Records documenting the history and heritage of the university shall not be destroyed; and
10. There must be a clear allocation of responsibility within each organizational unit for all aspects of record-keeping, including classifying records, applying retention schedules and safely discarding documents.

5. Definitions

Archives: The term 'archive' is often used to describe records that are no longer in daily use and are stored separately from an office's current files (see semi-current). The term is also applied to records that are to be kept permanently because they have historical value.

Authentic record: An authentic record is one that can be proven to be what it purports to be; to have been created or sent by the person purported to have created or sent it; and created or sent when purported.

Classification: The process of devising and applying schemes based on the teaching, learning, research and administrative activities which generate records, whereby they are categorized in systematic and consistent ways to facilitate their capture, retrieval, maintenance and disposal. The classification includes determining document or file naming conventions, user permissions and security restrictions on records. In broad terms, it is the process by which records are categorized or grouped into retrieval units, whether by function, subject or other criteria.

Destruction: Process of eliminating or deleting a record, beyond any possible reconstruction.

Electronic records: Records processed and retrieved by a digital computer; these include text-based word-processed documents, email messages, spreadsheets, presentations, scanned documents, website and multimedia documents.

The integrity of records: Records will have integrity if they are complete, unaltered and protected from unauthorized alterations.

Record: Information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations on in the transaction of the university.

Retention schedule: Document setting out the length of time for which categories or series of records should be kept according to legal, regulatory, university and operational requirements.

Records Archive: A records archive contains material created or received by a person in the conduct of their affairs on behalf of the university and preserved because of the enduring value contained in the information they contain or as evidence of the functions and responsibilities of their creator, especially those materials maintained using the principles of provenance, original order, and collective control.

Version control: A process that allows for the precise placing of individual versions of documents within a continuum.

Vital records: Records that contain information needed to re-establish an organization in the event of a disaster. They are likely to be unique/irreplaceable or required immediately following a disaster. They will provide information for continuing/resuming operations, recreating legal and financial status of an organization or preserving the rights of an organization or fulfilling its obligations to its stakeholders.

6. Management of records

6.1 Creating records

1. The records must be accurate and complete so that it is possible to establish what has been done and why.
2. 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.
3. The integrity of the information must be beyond doubt. Not only should it be compiled at the time of the event/transaction to which it relates (or as soon as possible afterwards), but also it shall be protected from unauthorized alteration or deletion.
4. 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.
5. Where appropriate, branded templates should be used, so that records are produced consistently and quickly.
6. Wherever possible, records should be created in a way that enables accessibility by those with disabilities.
7. The university has a general claim of ownership of records created or received by its staff in the course of their duties, and subject to its control. This does not invalidate other claims of ownership, such as copyright and/or intellectual property rights. Employees leaving the university, or changing positions within it, must undertake steps to ensure that all records created, received and used are returned, filed and secured appropriately, including electronic records.

6.2 Classifying records

1. All records – whether paper or electronic – shall be organized in a uniform, logical way, so that they can be easily and speedily retrieved.
2. A classification scheme or filing structure shall be devised to ensure that documents are grouped appropriately and consistently.
3. Only items of a similar nature must be placed together. If the contents of folders and the folders themselves are too diverse, it will be difficult not only to locate the material but also to assign appropriate retention periods.
4. Standardized referencing and titling are essential, so that information can be readily identified and retrieved.
5. Faculties/Departments/Centres/Units/Branches shall develop naming conventions and glossaries to ensure consistent terminology is used for similar kind of records (e.g.: activities, committees and organizations).
6. The university shall develop a classification convention to maintain confidentiality requirements of the documents.
7. The titles of electronic documents and folders, as well as the covers of paper files, should describe the content or subject matter accurately and helpfully.

6.3 Access and security

1. Information that is only accessible to a single person should be kept to a minimum.
2. As far as possible records that other staff may require must be stored in a secure, shared area within a centralized filing system so that departments can operate efficiently when individual members of staff are absent.
3. Where appropriate, data should also be shared across the university to avoid wasting resources recreating information that already exists and storing duplicate data unnecessarily.
4. Appropriate levels of security must be in place to prevent the unauthorized or unlawful use and disclosure of information.
5. Paper records containing confidential information must be stored in locked cabinets within locked rooms when not in use, and access only granted to authorized staff.
6. Access to restricted electronic data should be controlled through the use of log-ins, passwords and, if appropriate, encryption.
7. Confidential electronic records shall be stored encrypted.
8. Computers must not be left unattended when logged on, even for short periods and staff should consider the placement of their display of the computer to prevent any sensitive information on their screens may be visible to students or visitors.
9. Information held in digital systems should be protected from accidental or unauthorized alteration, copying, movement or deletion.
10. If possible, the systems should maintain audit trails allowing all actions to be traced to specific people, dates and times.
11. It is essential that any data held on portable storage devices (such as USB memory sticks, CDs, DVDs), as well as laptops, is kept securely (using encryption where necessary) and protected from theft.

6.4 Storage and preservation of records

1. Records need to be preserved in a usable state (protected from damage and obsolescence) throughout the current and semi-current phases of their life cycle.
2. How long a document kept by the university shall be based on the official retention schedule.
3. Inactive records may also require preservation if they are selected for permanent retention.

6.5 Retention and destruction of records

1. Faculties/Departments/Centres/Units/Branches shall ensure the timely, secure destruction of information/records as per the retention schedule.
2. No person shall destroy or otherwise dispose of, or authorize the destruction or disposal of, any university record in their possession or under their control, except with the proper consent as per this policy and given as per the provisions of this policy.
3. Before authorizing the destruction of any university record, the head of Faculty/Department/Centre/Unit/Branch may consult with any person whom they consider qualified to provide advice as to the value thereof for permanent preservation.
4. A register of records disposal will be kept by the Office of the Registrar for the purposes of accountability. This register is a permanent record of the university.
5. Inactive records may also require preservation if they are selected for permanent retention.
6. Records to be retained permanently will be transferred to the university Archive.
7. The Registrar is the designated officer with the responsibility to authorize the disposal of university records.

6.6 Emails

1. Emails may record the university's actions and decisions, and must be managed as effectively as paper and other electronic records.
2. Emails of official email accounts used for official purposes of the University shall be preserved.

6.7 Vital records

1. Records that would be vital to the continued functioning of the university in the event of a disaster (e.g. fire, flood, ICT virus attack) must be identified and protected.
2. All critical data must be stored on a central server so that it will be protected by appropriate backup and disaster recovery procedures.
3. Whereas possible, vital records shall be digitized and stored on a secure central server.
4. Where vital records are only available in paper format it is a best practice that they are duplicated, and the originals and copies stored in separate locations.
5. If, however, duplication is either impracticable or legally unacceptable, fireproof safes should be used to protect the documents.

6.7 Records management

1. There must be a clear allocation of responsibility within each Faculty/Department/ Centre/Unit/Branche for all aspects of record-keeping, including classifying documents, applying retention schedules and discarding material.
2. The ownership of information shall also be clarified so that there is no ambiguity regarding responsibility for its maintenance and disposal.
3. Heads of Faculties/Departments/Centres/Units/Branches shall ensure that prior to a member of staff leaving, responsibility for his or her records is transferred to another person; and if any of the information is redundant, it should be deleted by either the departing member of staff or the line manager.
4. Records management systems of each Faculty/department/Centre/unit/branch shall be adequately documented so that their effective operation is not solely reliant upon the memory of individual members of staff.
5. Documents mention in above 4 shall also be periodically reviewed and, if necessary, modified to ensure that they continue to support the needs of the Faculty/Department/Centre/unit/branch.
6. Electronic systems storing data that may be required for evidential purposes should be regularly monitored and audited. It shall be possible to demonstrate the reliability of the system so that the integrity of the data cannot be questioned.

7. Responsibilities

1. All members of staff are responsible for ensuring that their work is documented appropriately and that the records which they create or receive are managed correctly. In addition, they have a responsibility to know what information they hold and where it is held.
2. The Vice-Chancellor on behalf of the Council of the University has the overall responsibility for ensuring that the university fulfils its legal and relevant obligations in relation to recordkeeping and that adequate resources are available for managing and maintaining university records.
3. Registrar of the university is the custodian of records of the university.
4. The Librarian is responsible for developing records management procedures, advising on good practice and promoting compliance with this policy.
5. Heads of Faculties/Departments/Centres/Units/Branches shall facilitate and promote the establishment and resourcing of appropriate record-keeping systems as per university policies and procedures.
6. Heads of Faculties/Departments/Centres/Units/Branches are to ensure that staff members have a clear understanding of recordkeeping requirements of their respective Faculty/Department/ Centre/Unit/Branch and provide adequate training and education. They are responsible for ensuring records are disposed of as per authorized disposal schedules, and for certification of entries made in the Register of Records Destroyed.
7. Director, ICT Centre is responsible for maintaining the databases and systems on which records and information are stored including undertaking system backups and developing, maintaining and testing the university's disaster recovery plan.

8. OneDrives and Google Drives and other online storage

1. Whilst OneDrive and Google Drive provide document storage and the facility to share documents with others, each OneDrive or Google Drive remains intrinsically linked to the individual.
2. The university has no corporate oversight of, nor the ability to manage the content of the OneDrive or Google Drives or Shared Drives This makes such storage drives an unsuitable repository for the university records.
3. Such Drives may be used for the drafting of records, but once completed these shall be declared into the appropriate corporate system and then deleted from the online storage drive.

9. Enforcement

Reports of problems or violations should be informed to the Registrar, University of Kelaniya

Violations of policies of the university, including Records Management Policy, may result in appropriate disciplinary measures in accordance with the law of the country as well as regulations and policies of university.

Document title
Records Management Policy
Approving body
Council, University of Kelaniya
Enforcement Authority
Vice-Chancellor, University of Kelaniya
Operational responsibility
Heads of Faculties/Departments/Centres/Units/Branches Librarian, University of Kelaniya Director, Information and Communication Technology Centre, University of Kelaniya
Date of approval
10.08.2021
Review date (s)
XX
Edition no.
1
Date of effect
XX
Document classification (Public, Internal, Confidential, Secret)
Public

When drafting this policy, record management policies of other universities including the University of Portsmouth, University of Tasmania, University of Victoria, and University of Warwick. It also referred to the guidelines and requirements specified in ISO 15489: 2016 Records Management standard.

This policy document is authored by Dr Ruwan Wickramarachchi, Acting Director, ICT Centre and the initial draft was reviewed by Prof Janaka Wijayanayake, Department of Industrial Management; Dr Chaminda Jayasundara, Librarian; and Dr Chamli Pushakumara, Department of Applied Computing.

Classification Criteria

Public	Protected	Restricted	Confidential
Protection – None	***Protection - Low***	***Protection - Medium***	***Protection - High***
confidentiality is of no particular significance to this information	inappropriate disclosure would have minimum significance	disclosure could adversely affect the University's reputation or operations, substantial distress to individuals or breach statutory restrictions on disclosure of information; likely financial or legal penalties	disclosure could cause significant damage to the University's reputation or operations, great distress to individuals, pose a danger to personal safety or to life or impede the investigation or facilitate the commission of serious crime; substantial financial or legal penalties
Example documents			
Anonymised information Staff details shared publicly by the University Information on individuals made public with their consent including on social media sites or university websites Department and course details Marketing or press Information, factual and general information for public dissemination incl. annual reports or accounts Publicly available online identifiers (social media sites and online collaboration) Publicly available photographs	Staff names, detailed qualifications, and publication details (not required for public) Staff work Contact Details (job titles, office telephone no., Kelani mail address, office address) Student names and email addresses University policies, guidelines, by-laws, etc. Progress of corporate plan, aggregated information of surveys	Individual's name, home addresses, personal contact details, passport no, NIC no. and age University CCTV footage Student registration and attendance details Prospective Students' contact details References for staff or students 'Trade' secrets, intellectual property intended for commercialisation Financial documents such as procurement plans, fund allocations, vouchers, etc. Detailed responses to surveys Meeting (with restricted access) minutes such as Faculty board, CULTEC, BoS, Senate	Financial information relating to individuals e.g., banking information, salary details, indebtedness Information on individual's, racial or ethnic origin, political option, religious or other beliefs, physical or mental health, criminal record or trade union membership Exam papers before conducting the exam Exam scripts/ marks/ comments on student's performance Student academic progression details including details of disciplinary proceedings Provisional degree classification prior to formal approval and any publication Staff appointment, promotion or details of personal affairs

			Biometric data (fingerprints, facial recognition data) Research data which is security-sensitive or has been similarly classified by an external body (e.g. Government, commercial partner with a confidentiality agreement) Legal advice or other information relating to legal action against or by the University Meeting (with restricted access) minutes such as Council, Finance Committee, Audit Committee

Annex B – Handling Electronic Information

Activity	University Information Classifications			
	Public	**Protected**	**Restricted**	**Confidential**
Creation/ Labelling	N/A	N/A	Visibly marked 'CONFIDENTIAL'	Visibly marked 'STRICTLY CONFIDENTIAL'; To be created (and stored) only in a secure environment and copies be limited and recorded
Can Email	Yes	Yes	Only to Kelani Mail addresses (take care to check recipient(s) addresses)	Only as encrypted/password protected attachment (take care to check recipient(s) addresses)
Can access remotely	Without restrictions	Using VPN/ secure authentication	Using VPN/ secure authentication	Using VPN/ secure authentication
Access controls	May be viewed by anyone, anywhere in the world	Available members of the University community (access restriction needed, staff and student restrictions may need)	Available only to specified authorised members of the university (requires authorisation to gain access)	Access is controlled and restricted to a small number of authorised members of the University (requires authorisation to gain access)
Can share via One Drive/ Google Drive	Yes	Yes	Only with encryption/ password protection (take care to check recipient(s) addresses) Using of personal drives are discouraged	Only for specific purposes with encrypted/ password protected (take care to check recipient(s) addresses) Should be removed once requirement is completed To use only shared drives attached to university accounts Should be removed once requirement is completed

Can keep on University laptops or other portable media	Yes	Only on temporary basis, taking care to avoid loss or theft	encrypted/password protected, taking care to avoid loss or theft	Only on temporary basis and encrypted/password protected, taking care to avoid loss or theft
Can keep on personally owned devices	Yes	Yes, with appropriate care	Discouraged	No
Store on University servers	Preferably in backed up personal or shared network spaces	Only in backed up personal or shared network spaces with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)	Only in backed up personal or shared network spaces with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)	Only in backed up personal or shared network spaces with access restricted to only those with a valid right to access the information (either by adding a password to the document, encrypting it or apply permissions to a folder)

Annex C – Handling Paper or other media

	University Information Classifications			
Activity	**Public**	**Protected**	**Restricted**	**Confidential**
Creation/ labelling	N/A	N/A	Visibly marked 'CONFIDENTIAL'	Visibly marked 'STRICTLY CONFIDENTIAL' To be created (and stored) only in a secure environment and copies be limited, numbered and recorded. Copies delivered by hand
Storage in University	N/A	Locked filing cabinet or equivalent	Locked filing cabinet or equivalent in office which is locked or attended at all times	Locked filing cabinet or equivalent in office which is locked or attended at all times
Can take off or around site	Yes	For shortest time possible and documents to be kept securely and with person	For shortest time possible documents to be kept securely and with person	Only exceptionally and with authorisation from line manager; documents to be kept securely and with person
Can Fax	Ensure fax number is correct and entered correctly	Ensure fax number is correct and entered correctly	Ensure fax number is correct and entered correctly	No (unless to 'safe haven machine')
Can Post	Yes	Yes	Double envelope with inner envelope marked as 'CONFIDENTIAL', hand delivered, registered or courier delivery	Double envelope with inner envelope marked 'STRICTLY CONFIDENTIAL', hand delivered, recorded or courier delivery
Disposal	Recycling	Recycling (shredding if available)	Shredding, confidential waste	Shredding, confidential Waste

Retention Schedule and Classification

No	Document/ Information	Designation of the Responsible Officer for the Document/Information	Faculty/ Department/ Unit/ Branch (Information Handling)	Classification (Public, Protected, Restricted, Confidential)	Accessibility	Retention Period
1	Senate minutes		Academic Branch	Restricted	Members of Senate	Perpetual