RECORDS MANAGEMENT POLICY

Policy No. RMP 2024

KARE/IQAC/RMP/2024/01

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(Deemed to be University)

(Under the section 3 of UGC act 1956)

Anand Nagar, Krishnankoil-626126, Srivilliputtur (Via), Tamil Nadu, India.

Phone: 04563-289042, Fax: 04563-289322

www.kalasalingam.ac.in **email:** info@kalasalingam.ac.in

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade
Anand Nagar, Krishnankoil, Srivilliputtur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

RECORDS MANAGEMENT POLICY

Policy Preparation & Verification Team

Prepared: 2024

Prepared by	Dr. R. Kottaimalai	
Reviewed by	Dr. C. Sivapragasam	
Recommended by	Dr. P. Deepalakshmi	
Approved by	Vice-Chancellor	

KALASALINGAM
ACADEMY OF RESEARCH AND EDUCATION
(DEEMED TO BE UNIVERSITY)
Under sec. 3 of UGC Act 1956. Accredited by NAAC with "A++" Grade
Anand Nagar, Krishnankoil, Srivilliputtur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

RECORDS MANAGEMENT POLICY

1. PURPOSE

The purpose of this Records Management Policy is to establish a comprehensive and systematic framework for the creation, classification, storage, maintenance, retrieval, retention, and secure disposal of records within Kalasalingam Academy of Research and Education (KARE). Records constitute critical institutional assets that support academic excellence, administrative efficiency, legal compliance, and strategic decision-making.

This policy aims to ensure that all records are managed in a manner that guarantees their authenticity, reliability, integrity, and usability throughout their lifecycle. Proper records management enables the institution to demonstrate accountability, respond effectively to audits and legal requirements, and preserve institutional memory.

Furthermore, this policy supports compliance with applicable statutory, regulatory, and accreditation requirements, while also aligning with best practices in information governance and data protection.

2. SCOPE

This policy applies to all units and stakeholders associated with KARE, including academic departments, administrative offices, research centers, and affiliated entities. It covers all individuals who create, access, manage, or use records in any form as part of their institutional responsibilities.

The scope includes all categories of records, irrespective of format, such as:

- Physical records (files, registers, reports, contracts, certificates)
- Electronic records (emails, databases, spreadsheets, digital documents, multimedia files)
- Research data, laboratory records, and project documentation
- Financial and audit records
- Student and employee records

The policy governs records generated through academic, administrative, financial, research, and collaborative activities, ensuring consistent practices across the institution.

3. DEFINITIONS

- Record: Any information created, received, and maintained as evidence of institutional activities
- Electronic Record: A record stored in digital format
- Retention Period: The duration for which a record must be kept
- Archival Record: A record preserved for long-term historical, legal, or research purposes
- Data Integrity: Accuracy and consistency of data over its lifecycle
- Confidential Information: Sensitive information requiring restricted access
- Disposal: Secure destruction or deletion of records after the retention period
- Official Record: Any physical or electronic document, including official emails, created or received in the course of University business and retained as evidence of institutional activities or decisions.
- Records Retention Schedule: An approved schedule specifying the minimum period for which different categories of records shall be retained before archival or disposal.

4. POLICY REQUIREMENTS

4.1 All Processing Activities

All record-related activities must be carried out in accordance with institutional policies, legal requirements, and ethical standards. Records must be processed only for legitimate, authorized, and clearly defined purposes. Unauthorized processing, manipulation, or misuse of records is strictly prohibited.

Each record must:

- Be accurate, complete, and maintained in a timely manner
- Reflect the true nature of the activity or transaction it represents
- Be protected against unauthorized access, alteration, or deletion
- Be accessible to authorized personnel when required

Departments must ensure that records are managed in alignment with principles of confidentiality, integrity, and availability, particularly when handling sensitive or personal information.

4.2 Records Retention Schedules

A structured and well-defined records retention schedule shall be established and maintained for all categories of records. The retention period for each type of record must be determined based on:

- Legal and statutory obligations
- Institutional and operational requirements
- Audit and compliance needs
- Historical and research value

Departments must strictly adhere to approved retention schedules and ensure that records are not retained beyond their useful or legally mandated period. Over-retention increases risks related to data breaches, storage inefficiencies, and compliance violations.

The University shall maintain an approved Records Retention Schedule specifying the minimum retention period for each category of records. The schedule shall be reviewed periodically and updated whenever statutory, regulatory, accreditation, or institutional requirements change.

At the end of the retention period:

- Records must be reviewed for archival value
- Non-essential records must be securely destroyed using approved methods (e.g., shredding, digital wiping)
- Disposal actions must be properly documented

4.3 Day-to-Day Recordkeeping Processes

Effective day-to-day recordkeeping is essential for maintaining operational efficiency and institutional accountability. All departments must adopt standardized practices for:

- Creating and capturing records at the point of activity
- Classifying and indexing records using consistent naming conventions
- Maintaining organized filing systems for easy retrieval
- Ensuring secure storage of both physical and digital records
- Official emails relating to academic, administrative, financial, legal, research, procurement, or policy matters shall be treated as institutional records where applicable and shall be retained in accordance with the University's Records Retention Schedule.

Records must be updated regularly to reflect current information, and obsolete or duplicate records should be identified and managed appropriately. Access to records must be controlled based on defined roles and responsibilities to prevent unauthorized use.

Additionally, periodic reviews should be conducted to ensure the accuracy, completeness, and relevance of records maintained.

4.4 Digital Records Systems: Archival Preservation, Records Management, and Data Transfers

Digital records management systems must be designed and implemented to ensure secure storage, efficient retrieval, and long-term preservation of electronic records. The institution shall adopt reliable technologies that support:

- Centralized storage and document management
- Automated backup of critical digital records shall be performed at least once every twenty-four (24) hours. Full system backups shall be performed periodically in accordance with the University's Backup and Disaster Recovery Procedure, and restoration tests shall be conducted at least annually to verify backup integrity.
- Secure authentication and access control
- Audit trails for monitoring usage and modifications

For archival preservation:

- Critical records must be stored in durable and non-proprietary formats
- Periodic migration of data to updated systems must be ensured to prevent obsolescence
- Redundancy mechanisms must be in place to prevent data loss

Data transfers, whether internal or external, must be conducted securely using encryption and approved communication channels. Sensitive data must not be transferred without proper authorization and safeguards.

4.5 Version Control and Minimisation of Duplication

Proper version control is essential to maintain the integrity and reliability of records. Departments must implement systematic procedures to:

- Track changes and maintain version histories of documents
- Ensure that only the most recent and authorized versions are in active use
- Clearly label draft, final, and archived versions

Duplication of records should be minimized to avoid inconsistencies, confusion, and unnecessary storage usage. Redundant copies must be identified and eliminated in a controlled manner.

Effective version control ensures that decision-making is based on accurate and up-to-date information while reducing the risk of errors.

4.6 Staff Leaving the University

When an employee, faculty member, or staff leaves the institution, it is essential to ensure the proper transfer and safeguarding of records. The following measures must be implemented:

- All official records, documents, and data must be handed over to the designated authority
- Access to institutional systems, email accounts, and databases must be revoked immediately
- Sensitive or confidential information must not be retained or removed by the departing individual
- Digital records must be archived appropriately for future reference
- Before separation, departments shall ensure that all official electronic records, including institutional email accounts and digital documents, are transferred or archived in accordance with institutional procedures before account deactivation.

Departments must ensure continuity of operations by facilitating proper knowledge transfer and documentation handover.

4.7 Disposal of Records

- No record shall be destroyed or permanently deleted without prior approval from the Records Management Officer/Committee or such authority designated by the University.
- Departments shall prepare a disposal list identifying records proposed for destruction together with the applicable retention schedule.
- Approved disposal shall be carried out using secure methods such as shredding, pulping, secure digital deletion, or certified media destruction, as appropriate.
- A permanent record of all approved disposals shall be maintained for audit purposes, including the date of disposal, category of records, approving authority, and method of destruction.

5. ROLES AND RESPONSIBILITIES

Effective records management requires clearly defined roles and accountability across the institution.

5.1 University Management

University leadership is responsible for establishing the overall framework for records management and ensuring that adequate resources, infrastructure, and support systems are in place. Management must promote a culture of compliance and accountability.

5.2 Records Management Officer / Committee

The designated officer or committee is responsible for developing policies, monitoring compliance, conducting audits, and providing guidance on best practices. They act as the central authority for records governance.

- Approve the disposal of records after verifying compliance with the University's Records Retention Schedule.
- Maintain the University's Master Records Retention Schedule.

5.3 IT Department

The IT department is responsible for maintaining secure digital infrastructure, implementing data protection measures, ensuring system backups, and preventing unauthorized access or cyber threats.

5.4 Department Heads

Department heads must ensure that records within their units are properly managed, maintained, and disposed of in accordance with this policy. They are accountable for compliance at the departmental level.

5.5 Faculty and Staff

All personnel are responsible for maintaining accurate records, following institutional procedures, and protecting the confidentiality and integrity of information under their control.

6. NON-COMPLIANCE WITH POLICY

Failure to comply with this policy may result in serious consequences, including disciplinary action, legal liability, and reputational damage to the institution. Non-compliance may include:

- Unauthorized access, alteration, or deletion of records
- Failure to maintain or retain records as required
- Improper disposal of records
- Breach of confidentiality or data protection requirements

The University reserves the right to take appropriate action against individuals or entities found violating this policy, in accordance with institutional rules and applicable laws.

7. SUPPORTING DOCUMENTATION

This policy operates in conjunction with other institutional policies, including:

- Data Protection Policy
- Cybersecurity Policy
- Anti-Fraud Policy
- Disclosure (Whistleblower) Policy
- Financial Regulations & Audit Procedures
- IT Usage and Access Control Policy

These policies collectively ensure a comprehensive approach to information governance and institutional compliance.

8. POLICY REVIEW AND AMENDMENT

This Policy shall be reviewed at least once every three (3) years or earlier whenever required due to changes in legislation, regulatory requirements, accreditation standards, technology, or institutional needs.
Amendments shall be recommended by the Records Management Officer/Committee and approved by the Vice-Chancellor or the competent authority authorized under the University's Statutes.

CONCLUSION

This Records Management Policy provides a robust framework for ensuring that all records at Kalasalingam Academy of Research and Education are managed efficiently, securely, and in compliance with applicable standards. By adhering to this policy, the institution strengthens its governance, enhances operational effectiveness, and safeguards its valuable information assets.