

DATA PROTECTION POLICY

Policy No. DPP 2024

KARE/IQAC/DPP/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

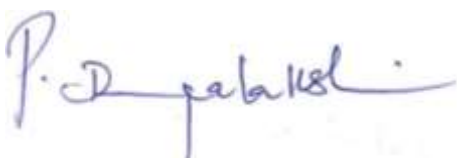


Anand Nagar, Krishnankoil, Srivilliputtur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

DATA PROTECTION 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, Krishnankottai, Srivilliputhur (Via), Virudhunagar (Dt) - 626126, Tamil Nadu | info@kalasalingam.ac.in | www.kalasalingam.ac.in

DATA PROTECTION POLICY

1. INTRODUCTION

Kalasalingam Academy of Research and Education (KARE) is committed to protecting the privacy and personal data of students, employees, researchers, alumni, applicants, visitors, vendors, and all other individuals whose personal data is processed by the University.

The University recognizes that personal data is a valuable institutional asset and shall process such data lawfully, fairly, transparently, and securely. Appropriate technical and organizational measures shall be implemented to safeguard personal data against unauthorized access, disclosure, alteration, loss, or destruction.

This Policy establishes the University's framework for responsible collection, use, storage, sharing, retention, and disposal of personal data in accordance with the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, applicable rules, and institutional policies.

2. PURPOSE

This Policy aims to:

- establish a University-wide framework for protecting personal data;
- ensure compliance with applicable legal and regulatory requirements;
- define responsibilities for processing personal data;
- protect the rights and privacy of individuals;
- promote accountability, transparency, and responsible data governance;
- minimize risks arising from unauthorized disclosure or misuse of personal data.

3. SCOPE

This Policy applies to all personal data processed by KARE, irrespective of whether such processing is carried out manually or electronically.

It applies to:

- students and applicants;
- faculty and staff;
- research scholars;
- alumni and donors;

- consultants, contractors and vendors;
- governing bodies and committees;
- visitors and other individuals interacting with the University.

The Policy covers all academic, research, administrative, financial, healthcare, outreach, consultancy, extension, and support activities undertaken by the University.

4. DEFINITIONS

Include concise definitions for:

- Personal Data
- Processing
- Data Principal
- Data Fiduciary
- Data Processor
- Sensitive Personal Data
- Consent
- Personal Data Breach
- Anonymisation
- Pseudonymisation

(Refer to Appendices A–F wherever applicable.)

5. DATA PROTECTION PRINCIPLES

KARE shall process personal data in accordance with the following principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

All University departments shall implement appropriate administrative, technical, and physical safeguards to comply with these principles.

6. PROCESSING OF PERSONAL DATA

6.1 Collection of Personal Data

Personal data shall be collected only for legitimate academic, administrative, research, healthcare, employment, or statutory purposes.

Privacy Notices shall clearly specify:

- purpose of collection;
- categories of personal data collected;
- lawful basis for processing;
- recipients of data;
- retention period;
- rights of the data principal;
- contact details of the Data Protection Officer.

(Refer to Appendix D.)

6.2 Lawful Basis

Personal data shall be processed only on a lawful basis in accordance with applicable legislation.

(Refer to Appendix A.)

6.3 Special Categories of Personal Data

Special categories of personal data shall receive enhanced protection and shall only be processed where legally permitted.

(Refer to Appendix B.)

6.4 Criminal Conviction Data

Processing of criminal conviction or offence-related data shall only be undertaken where authorized by law or institutional responsibility.

(Refer to Appendix C.)

6.5 Children's Personal Data

Although KARE is primarily a higher education institution, it may process personal data relating to children in limited circumstances such as:

- admissions involving minors;
- school outreach programmes;
- science camps;
- extension activities;
- research projects;
- competitions;
- healthcare services;
- other University-approved programmes involving children.

Such processing shall comply with applicable law and appropriate parental or guardian consent requirements. (Refer to Appendix E.)

6.6 Data Sharing

Personal data shall only be shared where necessary, lawful, and subject to appropriate safeguards.

6.7 Cross-border Data Transfers

Cross-border transfers shall be undertaken only where permitted by applicable law and subject to appropriate contractual, organizational, and technical safeguards.

6.8 Data Retention

Personal data shall be retained only for the period necessary to fulfil institutional, legal, regulatory, audit, or research requirements in accordance with the University's Records Management Policy.

7. RIGHTS OF DATA PRINCIPALS

Individuals have the right to:

- access personal data;
- request correction;
- request erasure where applicable;
- withdraw consent;
- object to certain processing;
- lodge complaints;
- receive information regarding processing activities.

Requests shall be handled in accordance with applicable legal requirements.

8. DATA SECURITY AND BREACH MANAGEMENT

KARE shall implement appropriate safeguards including:

- encryption where appropriate;
- role-based access controls;
- secure storage;
- authentication mechanisms;
- backup and recovery procedures;
- cybersecurity monitoring;
- periodic security audits.

In the event of a personal data breach, the University shall:

- assess the breach;
- contain and mitigate the incident;
- investigate the root cause;
- notify affected individuals and competent authorities where required;
- implement corrective and preventive actions.

9. ROLES AND RESPONSIBILITIES

University Management

Provide governance, oversight, and resources.

Data Protection Officer

Monitor compliance, provide guidance, coordinate breach response, and conduct awareness programmes.

Heads of Departments

Ensure departmental compliance.

Faculty and Staff

Process personal data responsibly and report suspected breaches.

Students

Handle personal data responsibly during academic and research activities.

Third-party Service Providers

Comply with contractual and statutory data protection obligations.

10. SUPPORTING POLICIES AND PROCEDURES

This Policy shall be read together with:

- Information Security Policy
- Cybersecurity Policy
- Records Management Policy
- Research Ethics Policy
- IT Acceptable Use Policy
- Alumni Data Protection Notice
- Employee Privacy Notice
- Student Privacy Notice
- Data Breach Response Procedure
- Privacy Notice SOP
- Data Retention Schedule

11. POLICY REVIEW AND APPROVAL

This Policy shall be reviewed at least once every two years or earlier if required due to changes in legislation, technology, or institutional requirements.

The Policy shall be approved by the Vice-Chancellor or the competent authority authorized by the University.

Appendix A: Lawful Bases for Processing

Under applicable Indian data protection law, particularly the Digital Personal Data Protection Act, 2023, it is essential that every instance of personal data processing is supported by a valid legal ground. The following are the recognised lawful bases:

Consent from the Individual

The data principal must provide clear, informed, and specific consent before their personal data is processed. Consent must be given voluntarily and should be capable of being withdrawn at any time without negative consequences.

Performance of a Contract

Processing is permitted where it is necessary to fulfill obligations under a contract between KARE and the individual, or to take steps at the request of the individual prior to entering into such a contract.

Example: Processing applicant data during recruitment or admission procedures.

Compliance with Legal Obligations

KARE may process personal data where required to meet statutory or regulatory obligations under Indian law.

Example: Maintenance of employee records, financial records, academic records, or compliance with government regulations.

Protection of Vital Interests

Processing is allowed where it is necessary to safeguard the life, health, or safety of the individual or another person.

Example: Sharing emergency medical information during a health crisis.

Public Interest / Official Function

Processing may be carried out when KARE performs functions that serve public interest, particularly in its role as an educational and research institution recognized under law.

Legitimate Uses (as per Indian framework)

Processing may also be undertaken for reasonable and lawful purposes aligned with institutional functions, provided such use does not override the rights and interests of the data principal.

In cases involving personal data related to criminal records or offences, such processing must strictly comply with applicable Indian laws and institutional policies, ensuring additional safeguards.

If there are any uncertainties regarding the appropriate legal basis for processing, guidance should be sought from the University's designated Data Protection Officer (DPO) or relevant authority.

Appendix B: Conditions for Processing Special Categories of Personal Data

Under applicable Indian data protection law, particularly the Digital Personal Data Protection Act, 2023, certain types of personal data that are sensitive in nature require enhanced safeguards during processing.

Kalasalingam Academy of Research and Education (KARE) shall ensure that, in addition to having a valid lawful basis for processing personal data, specific conditions are satisfied before processing such sensitive categories of data.

Processing of such data may be carried out under the following conditions:

- the data principal has provided explicit and informed consent for one or more clearly defined purposes, unless restricted by applicable law;
- processing is necessary to fulfill obligations or exercise rights related to employment, social security, or similar legal frameworks as permitted under Indian law;
- processing is required to protect the vital interests of the data principal or another individual where consent cannot reasonably be obtained;
- processing is undertaken by a not-for-profit body or institution (such as an educational or research institution) in the course of its legitimate activities, provided appropriate safeguards are implemented and the data is not disclosed externally without consent;
- the personal data has been clearly made public by the data principal;
- processing is necessary for the establishment, exercise, or defense of legal claims, or for judicial proceedings;
- processing is required for reasons of substantial public interest, in accordance with applicable Indian laws, while ensuring proportionality and protection of individual rights;
- processing is necessary for medical purposes, including preventive or occupational health, diagnosis, treatment, or management of healthcare services, subject to confidentiality obligations;
- processing is required in the interest of public health, such as addressing health emergencies or ensuring safety and quality standards in healthcare systems;
- processing is carried out for research, statistical, archival, or historical purposes, provided appropriate safeguards are implemented to protect individual rights.

Note:

Relevant provisions under Indian law may provide additional grounds for processing sensitive personal data, including for purposes such as insurance, pensions, or regulatory compliance. KARE shall ensure adherence to all such applicable provisions.

Appendix C: Conditions for Processing Personal Data Related to Criminal Convictions or Offences

Personal data relating to criminal history, allegations, proceedings, or convictions is subject to additional protections under applicable data protection frameworks. While such data may not always fall under “special categories,” it requires careful handling due to its sensitive nature.

For KARE to process such data:

- there must be a valid lawful basis under applicable Indian law, including provisions of the Digital Personal Data Protection Act, 2023;
- the processing must be supported by legal authority, statutory requirement, or official institutional responsibility;
- the purpose and justification for processing must be clearly identified and documented prior to processing;
- appropriate security and confidentiality safeguards must be implemented to prevent misuse or unauthorized disclosure.

In line with good governance practices:

- records relating to criminal data shall only be maintained where there is a legitimate institutional requirement and in accordance with applicable legal provisions;
- any comprehensive database or register of such information shall be maintained only under authorized supervision and control, ensuring compliance with relevant laws and institutional policies.

KARE shall ensure that all such processing activities are carried out with strict adherence to legal requirements, transparency, and respect for the rights of individuals.

Appendix D: Conditions for Consent

The Digital Personal Data Protection Act, 2023 lays down requirements for obtaining and managing consent for processing personal data:

- Where processing is based on consent, Kalasalingam Academy of Research and Education (KARE) must be able to demonstrate that the data principal has provided valid consent for the processing of their personal data.
- If consent is requested as part of a written document that includes other matters, the consent request must be clearly distinguishable, presented in a simple, understandable, and easily accessible format using clear language. Any unclear or misleading portion shall not be considered valid.
- The data principal shall have the right to withdraw consent at any time. Withdrawal shall not affect the legality of processing carried out prior to such withdrawal. Individuals must be informed of this right before giving consent. The process of withdrawing consent must be as simple as giving consent.
- While determining whether consent has been freely given, careful consideration must be given to whether services or contractual benefits are made conditional on consent for processing personal data that is not essential for the purpose of that contract.

Appendix E: Guidelines on Processing Personal Data Relating to Children

Children require enhanced protection when their personal data is collected and processed, as they may not fully understand the associated risks.

- KARE shall ensure that systems and processes are designed with child protection as a priority, incorporating safeguards from the initial stage of data collection.
- Adherence to data protection principles, especially fairness, transparency, and accountability, must be central when handling children's personal data.
- A valid legal basis must exist for processing children's data. While consent may be used, other lawful grounds may sometimes be more appropriate depending on the context.
- In accordance with the Digital Personal Data Protection Act, 2023, consent for processing children's data must generally be obtained from a parent or lawful guardian, particularly in the context of online services directed at children.
- Special care must be taken when using children's data for marketing, behavioural analysis, or profiling activities, ensuring that such processing does not harm their interests.
- KARE shall avoid making significant decisions based solely on automated processing involving children where such decisions may have legal or similarly impactful consequences.
- Privacy notices intended for children must be written in clear, simple language so that they can understand how their data will be used and what rights they have.
- Children enjoy the same data protection rights as adults, including:
 - right to access their personal data
 - right to correction
 - right to object to processing
 - right to erasure
- The right to erasure is especially important where consent was given during childhood.
- Additional guidance issued by relevant Indian authorities should be referred to for best practices in handling children's personal data.

Appendix F: Examples of Personal Data

The following are examples of information that may be considered personal data. This list is indicative and not exhaustive:

General Personal Data:

- Names of individuals
- Contact information (residential address, phone numbers, email IDs)
- Date of birth and age
- Place of birth, nationality, citizenship
- Gender
- Marital status
- Government-issued identification details (e.g., Aadhaar, PAN, Passport)

- Student or employee identification numbers
- Family details (next of kin, dependents)
- Photographs and images
- Curriculum vitae (CVs) and resumes
- Financial information (bank details, payment records)
- Donation or contribution details
- Salary or income information
- Biometric identifiers (fingerprints, facial recognition data)
- CCTV footage
- Audio/video recordings identifying individuals
- Employment records and history
- Medical records, health reports, or sick leave details
- Leave records (other than medical leave)
- Educational qualifications and academic records
- Performance evaluations
- References for staff or students
- Disciplinary or grievance records
- Examination and assignment results
- Memberships in professional bodies
- Signatures (including digital signatures)
- Passwords, PINs, and authentication credentials
- Professional development records
- Vehicle registration details
- Research-related data linked to identifiable individuals
- Online identifiers (IP addresses, login credentials)
- Location data
- Data relating to minors
- Consent forms collected for research participation

Special Categories of Personal Data:

- Racial or ethnic background
- Biometric identifiers used for unique identification
- Political views
- Health-related information
- Religious or philosophical beliefs
- Information about an individual's sex life or sexual orientation
- Trade union membership
- Genetic information

Criminal Data (Subject to Additional Safeguards):

- Information relating to criminal offences or alleged offences
- Details of legal proceedings, investigations, or court outcomes

Note:

- Although data protection laws primarily apply to living individuals, KARE shall also handle information relating to deceased persons with due sensitivity and confidentiality.
- While criminal offence-related data may not always fall under “special categories,” it is subject to enhanced protection requirements under applicable law and institutional policy.