

IT POLICY



(ITP-2024)

(Revised version of ITP-2018)

KARE/IQAC/ITP/2024/01

Approved by BoM on: 16-12-2023

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(Deemed to be University)

(Under the section 3 of UGC act 1956)

Anand Nagar, Krishnankoil-626126, Srivilliputtur(Via), Tamilnadu, 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 the section 3 of UGC act 1956)
Anand Nagar, Krishnankoil-626126, Srivilliputtur(Via), Tamilnadu, India.

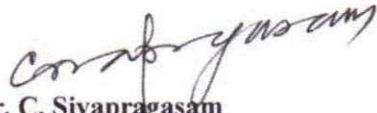
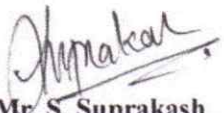
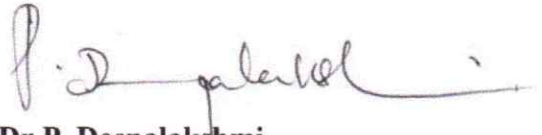


**RECOMMENDATIONS OF THE EXPERT COMMITTEE FOR THE REVISION OF
APPROVAL IN IT POLICY**

IT threats like ransomware, phishing, and data breaches are increasing so Cybersecurity Policy is added in 3.3.8. Many students, faculty, and guests use personal laptops and phones in the campus policy is added in 3.1.12 for the usage guidelines. Digital Rights Management and Intellectual Property guidelines are added in 3.9.

History of changes in IT Policy

Sl. No.	Newly Added / Revised	ITP 2018	ITP 2024
1	Cybersecurity Policy	Not available	Added in subsections 3.3.8
2	Bringing Own Device Policy	Not available	Updated in subsection 3.1.12
3	Digital Rights Management and Intellectual Property	Not Available	Added in subsection 3.9

IT Policy Preparation and Verification Team

Prepared by	 Dr. C. Sivapragasam Director(IQAC)
Reviewed by	 Mr. S. Suprakash IT Administrator
Complied by	 Dr.P. Deepalakshmi Dean(SoC)
Approved by	 Dr. R. Ramakashmi Director CDOE
Approved by	 Dr. S. Narayanan Vice-Chancellor

INDEX

S. NO	TITLE	PAGE NO
1	Preamble	1
2	Scope	1
3	Policy	1
	3.1 Responsibilities of Users	2
	3.2 Software usage policy	3
	3.3 Network Usage and Security	3
	3.4 Remote Access Policy	4
	3.5 Data Retention Policy	4
	3.6 Hardware and Software Procurement	5
	3.7 Hardware Installation policy	5
	3.8 Maintenance	6
	3.9 Digital Rights Management and Intellectual Property	7
4	Violations in Policy	7

TITLE AND APPLICABILITY: IT POLICY TO ACCESS KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION's INFORMATION TECHNOLOGY RESOURCES

1. Preamble

The Kalasalingam Academy of Education and Research (KARE) recognizes the role of information technology for achieving its missions and related administrative activities and also the importance of academic environment for protecting information in all forms. As more information are maintained and shared in a digital format by the stakeholders of the institute including students, faculty and staff, both within and outside the institute, efforts should be made to protect the information and the technology resources that support it. Increased availability, usability and protection of the institute's information, user's information and information technology resources by defining rules and requirements is the primary purpose of this policy. If the IT infrastructure accessed by unauthorized people, the policy restricts the usage to avoid the possible damages including loss of confidential data, intellectual property, alteration of data leading to damage among the public, damage to critical IT hardware systems, and other financial liabilities that could be incurred because of those losses. The user department initiating the requirement along with specification is submitted for administrative sanctions along with the competitive quotations from different suppliers. The purchase and procurement are handled by the Purchase Department. KARE's funding policy, the cost for procurement is borne by the purchaser.

2. Scope

This policy applies to all students, employees, parents, alumni, contractors, vendors, guests, and others who connect to the institute's information technology resources owned by Kalasalingam Academy of Research and Education. This policy applies to both on-campus network connections and remote access connections used to interact through the internet on behalf of the institute. By accessing the institute's Information Technology Resources, the user agrees to comply with this Policy.

3. Policy

3.1 Responsibilities of Users:

- 3.1.1 Any regulation in existence with national and state must be applicable to all users in accessing the IT infrastructure.
- 3.1.2 Additional policies of KARE in accessing the IT infrastructure is also applicable to all users.
- 3.1.3 All users must follow the copyright laws in using software / hardware.
- 3.1.4 All users must use the IT infrastructure effectively without overloading or over harming the resources.
- 3.1.5 All the users can use any computer node / network points / WiFi access points that belongs to KARE / that is properly registered with KARE. KARE reserves the rights to block the access otherwise.
- 3.1.6 It is the responsibility of each user to ensure the safety of the resources. Any resource in case of theft / missing must be reported to the IT Administrator.
- 3.1.7 Any devices other than the one provided from KARE, must be used only after obtaining prior approval from IT Administrator. KARE will not be responsible for any damages / failure / theft for the personal devices.
- 3.1.8 All the users will be given a login id and password to access various resources like internet, email, Impartus Lecture Capturing System, student information system/faculty login.
- 3.1.9 It is the responsibility of individual users to keep their credentials safe with strong passwords.
- 3.1.10 It is recommended to use a combination of minimum 8 characters with at least one character, one number and one special character. It is also recommended to change the password for every 30 to 60 days.
- 3.1.11 Bring Your Own Device Policy -
- 3.1.12 All must follow the security requirements for personal devices (e.g., up-to-date OS, antivirus). Non-KARE-owned devices are allowed to use campus internet and campus wide licence. Ethical use of data, AI tools, and digital media must be maintained.

3.2 Software usage policy:

- 3.2.1 KARE will be providing all necessary software for the devices attached with the campus.
- 3.2.2 Any specific software required by the users can be installed only after obtaining prior approvals. Such software must adhere with the copyright laws. KARE reserves the right to uninstall / restrict any software which does not adhere copyright laws / risk to security of resources.
- 3.2.3 Any duplication or distribution of any software and license owned KARE is strictly discouraged.
- 3.2.4 Any upgrade or updates in the system will be done by the respective technician attached with the resources with prior intimation to IT administrator.
- 3.2.5 KARE reserves the rights secure all the resources through login credentials and strong passwords.

3.3 Network Usage and Security:

- 3.3.1 KARE is responsible for securing all the network devices in the campus.
- 3.3.2 KARE takes its security measures in restricting internal and external access to communication ports, bandwidth restrictions, and site restrictions through dedicated firewall to provide secure access to all its users. Any compromised systems detected will be blocked immediately without notification and remain blocked until it is repaired.
- 3.3.3 KARE reserves the rights to monitor all network activity to ensure safety and security resources. Further KARE reserves the rights to block such users with security risks.
- 3.3.4 Users are forbidden to access(view / download / save) any offensive content of any kind including pornographic material, promoting discrimination on race, gender, nation, age, marital status, sexual orientation, religion, disability, threatening or violent behaviour, illegal activities, messages of political or racial nature, gambling, forwarding e-mail chain, material protected under copyright laws, recreational streaming of internet material,

downloading / installing unauthorized programs and software, tampering of KARE credentials in any means.

3.3.5 Any violation to 3.3.4 will lead to immediate termination to all access to IT resources and may be recommended for disciplinary actions.

3.3.6 Users can use their login credentials to access internet through WiFi / LAN.

3.3.7 Any complaints regarding network / internet issues can be notified to the IT administrator through netadmin@klu.ac.in / e-ticketing system (<https://kafka.kalasalingam.ac.in>).

3.3.8 Cybersecurity Policy - It is mandatory anti-virus/malware protection in the devices. All must be aware of phishing and email safety. Multi-factor authentication (MFA) must be used for emails and other applications. Follow the guidelines under 3.8.2 to report a security incident or suspected data breach.

3.4 Remote Access Policy:

3.4.1 Resources other than e-mails, Impartus Lecture Capturing System, and web resources are not accessible outside the institution.

3.4.2 Any requirement to access internal systems must be connected with prior knowledge of IT Administrator and under supervision of responsible persons.

3.4.3 All the systems must be monitored and updated with latest antimalware systems timely; Strong passphrases must be used and updated frequently on every remote access to ensure security of systems.

3.5 Data Retention Policy

3.5.1 Any data available in electronic format will be maintained for five years in the same media.

3.5.2 Regular backup in local media and cloud storage wherever possible shall be used for recovery in case of any disaster.

3.5.3 Individual data will not be shared with anyone without the concern of individual. Any other information will not be shared unless it is approved by concerned department heads / Management.

3.5.4 Outdated data shall be maintained in CD/DVD discs for long term use.

Any data more than 15 years life time, whichever is not required will be destroyed.

3.5.5 E-Mails IDs of students and faculty will be immediately suspended once they leave the campus. Further data will be maintained for 5 years.

3.6 Hardware and Software Procurement

3.6.1 The procurement of all computing and communication facility is done through IT Administrator.

3.6.2 Any special requirement from departments can be procured after consultation with IT Administrator. KARE is not responsible for interfacing / maintaining such hardware or software which are not approved by IT Administrator.

3.6.3 In accordance with the KARE's funding policy, the cost for procurement is borne by the purchaser.

3.6.4 All purchases for any hardware must be in line with the purchasing policy of the University. The purchase of all desktops, servers, portable computers, computer peripherals, mobile devices, Wi-Fi devices, CCTV's, Biometric devices and hence any device which suits the hardware specifications which is to be purchased must adhere to this policy.

3.7 Hardware Installation policy

- Any IT infrastructure installation including PCs, Servers, Storage, Network Points, Switches/Hub, Network Cables, WiFi access points, boosters, Printers, Scanners must be done with a prior knowledge of the IT Administrator.
- Any IT infrastructure under warranty period must be installed and serviced only through the provider. After the expiry of warranty the devices must be put under annual maintenance contract.
- All computers must be connected through Uninterrupted Power Supply (UPS). Power supply to UPS should never be turned off and proper earthing must be laid.

- All network points must be laid away from electrical points. All the network connections must be properly shielded.

3.8 Maintenance

3.6.1 Any system under warranty period must be serviced by the provider.

3.6.2 Any infrastructure under Annual Maintenance Contract (AMC) should not be opened / serviced by local technicians / third party.

3.6.3 Any minor updates like OS updates, antimalware updates, software updates must be done by the technicians.

3.6.4 Any problems with the infrastructure under AMC must be reported to the respective AMC vendor within 3 working days.

3.8.1 Lab System Maintenance

- **Regular Maintenance of the lab systems can be done by the laboratory technicians. These include**
 - Power connection problems / Network cable connections / interfacing cable connections
 - Simple booting problems / software updates / installation and uninstallation
 - Network configurations
 - Cleaning Junk files
 - Any major network issues, software / operating system issues will be addressed by IT Admin Team

3.8.2 End User System Maintenance

- Office systems other than the systems maintained in laboratory are maintained by IT Admin Team.
- An escalation to IT Admin Team can be done by concerned to initiate the process. This can be done through
 - Ticketing System <https://kafka.kalasalingam.ac.in>
 - E-Mail to netadmin@klu.ac.in

- General problems including cable connections, booting, software and OS installation and updates will be carried out by the IT Admin Team

3.8.3 Network Maintenance:

- All major network maintenance is done by the AMC Team. These include
 - Laying new network lines / Serving old lines
 - Network Switch Configuration
 - VLAN Creation
 - Port Security
 - Adding / Updating / Servicing WiFi access points

3.9 Digital Rights Management and Intellectual Property:

- 3.9.1 Faculty lectures, research content, software developed under KARE's name is the intellectual property of the institution unless otherwise licensed.
- 3.9.2 Content-sharing platforms (e.g., Moodle, Impartus, Google Classroom) must not be used to upload copyrighted third-party material without proper licensing.

4. Violations in Policy:

- 4.1 Separate committee will be constituted to review individual cases headed by IT Administrator
- 4.2 Any violations on the above said policies done by individuals will be given notice and warning and continuously monitored further. Further cases from the same may lead to permanent suspension of access to any IT resources.
- 4.3 Any group / bulk violations intentionally made to damage IT resources will be seriously viewed and immediate suspension of access to IT resources will be done. Further any disciplinary actions may be recommended by the committee.

4.4 During the period of investigation by the committee, the access to IT resources by the users remain suspended.

4.5 The management reserves the rights to take the final decisions and in case of any conflict or dispute.



Vice-Chancellor
Dr. S. Narayanan

Copy submitted to the Chancellor & Vice Presidents – for the favour of information

CC to: Registrar, Controller of Examinations, Directors and Deans

CC to: All HoDs with request to circulate among Faculty members and IT Admin