CENTRAL UNIVERSITY OF KERALA, PERIYE

IT POLICY

POLICY STATEMENT

All individuals of Central University of Kerala using ICT resources of the university shall take the proper measures for the economical, ethical and efficient use of all the IT resources and apply IT knowledge for teaching, learning and research.

PURPOSE OF POLICY

The Purpose of this policy is to optimize the usage of various IT resources and services with respect to their usage, maintenance and security.
The term "resources" and "services" includes but not limited to computational resources (computers), networks (wired and wireless), servers, software systems, network access from off-campus, the gateway used for world wide web, e-mail, university portal, file tacking system , e-tutorial system, web page hosting and others.

PRINCIPLES

The University's IT resources are maintained to support the work of the institution. The University reserves the right to monitor the use of these resources and to deal appropriately with users who use these resources contrary to the conditions of use set out in this policy.

The University accepts no responsibility for loss or damage, consequential loss or damage, or loss of data arising from the use of its ICT Resources or the maintenance of its ICT Resources.

ENTITIES AFFECTED BY THIS POLICY

All stakeholders of the university

WHO SHOULD READ THIS POLICY

All members of the university community

WEB ADDRESS FOR THIS POLICY

http://www.cukerala.ac.in/itpolicy

TABLE OF CONTENTS

CENTRAL UNIVERSITY OF KERALA

INFORMATION TECHNOLOGY POLICY (IT Policy)
June 2021

The **objective** of the Information Technology policy (IT Policy) is to ensure the security, support and maintenance of the Institute's computing and networking resources.

The **scope** of this document is to define the IT policy and its procedures. All users of these facilities, including faculty, non-teaching staff (including outsource staff), research scholar, students and others who process the information on behalf of the University are bound to follow this IT policy. This policy is effective at all University locations and applies to all system users at any location, including those using privately owned computers or systems to access University Computer and Network Resources.

Any user requesting for any type of digital information will be made available only if the user have legitimate rights for access to that data. It is the responsibility of all users who have been granted access to information asset to handle it appropriately by ensure the integrity, confidentiality, and authenticity, wherever applicable. Incidences of actual or suspected non compliance of this policy should be reported to the authority immediately.

This policy is not meant to supersede or replace, but should be read together with, other University policies.

Notwithstanding anything in the policy, stake holders shall not be held responsible for information security incident/data loss caused due to incidents such as act of God, or specific cause reasonably beyond their control

The policy is subject to periodical review and amendments. Central University of Kerala reserves the rights to make an exception of all or any of the terms of policy on a case to case basis.

1. IT POLICY RELATED GOVERNACE COMMITTEES

1.1 Information and Communication Technology Committee (ICT Committee)

The Information and Communication Technology Committee (ICT Committee) provides guidelines, directions and standards for the establishment and implementation of IT policy of Central University of Kerala. The ICT committee will provide directives to ICT Wing with regards to procurement, setting up of new ICT facilities, Computer Labs and all major ICT related policy matters. The committee also will plan and design the annual ICT budgets (including yearly investment required, upgrade and maintain the ICT Infrastructure of the University) for placing before the finance committee for approval.

The members of the ICT committee are constituted as follows.

ICT committee

SI.No.	Position	Members
(i)	Chairman	Vice-Chancellor or Registrar or Professor of IT related discipline nominated by VC
(ii)	Member	HoD, Computer Science
(iii)	Member	One Faculty nominated by VC
(iv)	Member	Finance Officer or One Member Nominated by Finance Officer
(v)	Member Secretary	Section Head of ICT Wing
(vi)	Any other special invitees	As approved by Chairman

1.2 Standing Purchase Committee

A "Standing Purchase Committee" shall be responsible for all technical and financial evaluations of procurements of all ICT facilities related to this IT policy. This committee will also act as local purchase committee for all IT related procurements binding with this IT policy.

Standing Purchase Committee

SI.No.	Position	
(i)	Chairman	HoD, Dept. of Computer Science Or Any Professor from ICT related disciplines nominated by VC
(ii)	Member	Deputy/Assistant Registrar (Finance) OR Section Officer (Finance)
(iii)	Member	Deputy/Assistant Registrar (Purchase) OR Section Officer (Purchase)
(iv)	Member	Deputy/Assistant Registrar (Admin) OR Section Officer (Admin)
(v)	Member	Deputy/Assistant Registrar (Academic) OR Section Officer (Academic)
(vi)	Member Secretary	Section Head of ICT Wing
(vii)	Any other special invitees	As approved by Chairman

1.3 ICT Co-ordinator

Every department shall nominate one of the faculty members as the ICT Co-ordinator of the department. The ICT Coordinator shall be responsible for

a) Proposing ICT facilities for the department with the approval of Faculty council
b) Co-ordinating with concerned sections for maintenance of ICT facilities in the department
c) Ensuring compliance with the IT Policy of Central University of Kerala
d) Maintaining the Stock/Inventory of Hardware/Software in the department.

2. ICT WING

The ICT Wing of the University design, support, monitors, maintains and secure the Information Technology infrastructure of the University. Besides these the ICT Wing maintains and updates the official Website of the University and provides all the ICT related data supports to ensure solving problems. Also, it provides complete web service support for the online activities. It makes smooth coordination with different section and departments and giving responsible relation between central authorities as a feed backup and ensures better relationship with general public by way of different notification and news from the University Website. ICT Wings provides various services to pertained Faculty members, staffs, and students of the University. Moreover, it develops, configure and implement necessary software for different offices, sections and examination activities with a view to improve productivity, reduce expenses with optimum result. It also provides support for Open-Source technologies and implementations and to encourage their use in the University activities. ICT Wing provides the requisite central facility for the growth and development of Teaching, Research and all other section of the University.

A group of employees/trainees/outsource staff from ICT Wing will act as Central University of Kerala's Desktop Support Staff (DSS).

To ensure that all significant risks to the University are identified, assessed and where necessary treated and reported to the ICT committee, once in year by the ICT Wing by conducting hardware/software audit through the respective section/department ICT co-ordinators.

3. INFORMATIONS SECURITY GUIDELINES

-

3.1 Risk Management

Like every Organizations the University faces numerous risks. These risks have the potential to disrupt achievement of the University's strategic and operational objectives. The University aims to use risk management to take better informed decisions and improve the probability of achieving its strategic and operational objectives. The Risk Management policy of the University aims at providing checks against external threats in the form of computer viruses and other malicious software. Besides using the network security measures, Central University of Kerala manages the information security risk by using up-to-data, firewalls, anti-malware and backup procedures.

In order to protect the security and integrity of Computer and Network Resources against unauthorized or improper use, and to protect authorized users from the effects of such abuse or negligence, the University reserves the rights, at its sole discretion, to limit, restrict, or terminate any account or use of Computer and Network Resources, and to inspect, copy, remove or otherwise alter any data, file, or system resources.

The University shall not be liable for, and the user assumes the risk of, inadvertent loss of data or interference with files or processes resulting from the University's efforts to maintain the privacy, integrity and security of the University's Computer and Network Resources.

3.2 Misuse of Facilities

No person shall deliberately or willfully cause damage to computer equipment or assist another in doing the same. Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary action and/or legal action.

Examples of unacceptable uses that are expressly prohibited include, but are not limited to the following:

(i) Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;

(ii) Using the University networks and Internet services for any illegal activity or that violates other Board policies, procedures and/or University rules; The disseminating of computer viruses, the installation of cookies or other data collection devices or devices that can be used by hackers, or software that can attack the computer system; Attempting to access restricted areas, or doing anything that restricts other people's ability to use the internet;

3.3 Disciplinary action on Violation and Appeal Process

The user is responsible for his/her actions and activities involving University networks and Internet services, and for his/her computer files, passwords and accounts. The user can appeal to the ICT committee and the decision of ICT committee shall be final on the matter.

The University reserves the right to disable your service access for the following reasons:

- Attempt to tamper/hacking the servers/network or overloading ICT resources and assets by excessive bandwidth usage or using misconfigured devices or knowingly using a false identity.
- Download/Use/Store or transmit illegal copies of copyrighted materials or patented software/movies/songs etc. is violation of the regulatory laws that involve protection of data or privacy.

Violation of this policy and guidelines will be viewed seriously and University shall have the rights to permanently disable access to the network of the University.

3.4 Third party access to facilities

Any third party who request for access to the IT related facilities must be reported to the IT wing in all cases. Once such request is received from a third party, a risk assessment will be done prior to allowing a third party to have access to secure areas of the University where confidential information and assets are stored or processed. This assessment should take into account:

- what computing equipment the third party may have access to
- what information they could potentially access;
- who the third party is
- whether they require supervision
- whether any further steps can be taken to mitigate risk.

3.5 Compliance to India IT Act

Users of ICT facilities shall obey Indian Cyber Crime laws as detailed below holistically and respect other users' use of ICT resources.

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce. Secondary or subordinate legislation to the IT Act includes the **Intermediary Guidelines Rules 2011** and the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.** The **Personal Data Protection Bill 2019** as and when it is approved by Parliament will be part of this document.

The provisions of the above act further amendments/additions in future **mutatis-mutandis** shall be applicable for staff/students/third-party stakeholders of Central University of Kerala.

Any organization which receives, stores or transmits data on behalf of another person has an obligation to exercise "Due Diligence" which inter-alia includes

a) Identifying which of the information is "Sensitive Personal Information" and

b) Follow reasonable security practices to protect them (under Section 43-A of IT Act,2000)

c) Understand the data retention requirements and implement systems to comply with them

d) Understand that the GOI has the powers to block, intercept or ask for data decryption keys, information on data traffic etc (under Section 69,69-A of IT Act,2000)

e) Expect you to conduct e-audit of all the documents you maintain in the e-form

f) Adhere to the encryption policies as may be announced etc
g) Ensure that without the permission of the owner of an information does not even provide access to the information to others.
h) Ensure that any security obligations agreed to in a contractual agreement are not breached

Failure to comply with the above may result in damages payable for which there is no specified upper limit, besides possible imprisonment from 3 years to 7 years.

It is also necessary for organizations to understand that even if any of their employees contravene the provisions of the Act including committing of such personal offences such as searching for child pornography using the corporate network, then there could be vicarious liabilities on the organization and its Directors and Executives.

Telecom Regulatory Authority of India (TRAI), statutory body that controls the Internet Service Providers (ISPs.) in India directed all Universities to take strong steps in strengthening the security of networks and the users behind device should be registered with authorities and ensure that no other mobile clients, other than registered one, is allowed in network access. University (ISP) has rights to do lawful monitoring/logging of all internet user's activity without affecting his privacy and share it with statutory bodies, if warranted. Currently we are having a capacity to store one-year data.

4. ICT SERVICE MANAGEMENT

ICT wing provides seamless and hassle-free access to ICT resources and service to the Central University of Kerala community. The ICT Wing will support all computer-related equipment in use by faculty and staff on the Central University of Kerala campus. However, the enormous variety of this equipment makes it impossible to deliver the same level of service for all devices. All standard desktop computers (PCs and Macs) purchased through the Central University Computer Store and configured by ICT staff receive full support. Full support is also provided for departmental network-connected printers. Every effort is made to respond to all requests for help but the level of support may be limited for some computers and peripherals, depending on their hardware configuration, software configuration, function, age or other factors. The DSS group's approach is to take a proactive role and work with the university departments and individual faculty and staff members to make sure that the equipment purchased is supportable and ensure, through proper maintenance, that it continues to function reliably for its expected life span. An important part of this approach is to work with departments to plan for a realistic replacement cycle to eliminate unreliable and obsolete equipment before it becomes a liability.

4.1 Methodology followed for ICT service support

a) All requests are logged into ICTS' service management platform. Any faculty or staff member who would like assistance can submit a support request by sending a mail to help@cukerala.ac.in. If the user's computer or email program are not working or for extreme emergencies, faculty or staff may call a ICT staff.
b) The DSS provides the first level of support for ICT problems. If possible, these will be done on-site, otherwise the equipment will be brought to the ICT Wing. If the problem persists, an outside vendor will be called to make the repairs. If the call is authorized by DSS, there will be no charge to the department for these repairs.
c) Once a request is received, DSS will respond within 24 hours. The DSS will utilize remote control tools when appropriate to provide quick problem resolution (the user's permission is required for remote control access).
d) Requests are handled during normal working hours on weekdays.
e) Requests will be prioritized according to urgency and number of users affected. Problems affecting an entire department (i.e. the inability to connect to the network or access a departmental printer) will usually take priority over individual problems. Non-operational computers will receive a higher priority than machines which are experiencing non-critical or intermittent problems. Computer viruses are given high priority because of their destructive potential and ability to infect other computers. Requests of approximately the same urgency will be handled on a first-come-first-served basis.
f) The requestor will be notified via email when the request is complete. If the requestor indicates that problems still exist or that additional assistance is needed in this matter, the DSS will continue working on the problem. If new, unrelated problems have occurred, the user should submit a new request.

4.2 *Service support to ICT hardware*

A DSS will respond to all requests for assistance and evaluate the nature of the problem. Most problems can be corrected on site, including simple hardware replacements, software installation, upgrades, or re-configuration. In more complex cases, the specialist may consult with DSS staff. If the computer is not working for more than five days in administrative sections, a temporary replacement will be provided. This will probably not be the same make/model computer and may not have all of the same capabilities, but it will perform the basic functions required for desktop computing (email, Internet access, the standard software configuration).

The comprehensive Annual Maintenance Contract (AMC) is provided for the proper services to the institution. A manufacturer company provides the service through AMC by themselves or with the help of service providers. The

contract is usually for the period of 1 year and can be extended up to three years or five years as per the mutual understanding of both the parties. Usually the service providers gives service support and in some cases, few parts are replaced by the service engineer when it is mentioned in AMC contract that limited parts will be replaced. Desktops, Laptops, Printers, Switches, Scanners, etc. are included in AMC. Those systems/equipments which are under AMC, will be serviced as per the AMC agreement.

4.3 Service support to ICT Software

As with hardware, when the software installed on a computer is out of date, servicing becomes more difficult and time consuming. Beyond a certain point, technical assistance can no longer be obtained from vendors, compatibility problems arise, and familiarity of the DSS with the software diminishes. In order to comply with software licensing regulations, a DSS will install only legally licensed software, freeware, or shareware.

As software companies release newer versions of software, the old versions eventually become obsolete for the following reasons:

(i) The software vendor no longer offers technical support for problems encountered

(ii) The files or documents created by the software may be in a format no longer recognized by current software, making them un-sharable

(iii) The original disks from which the software was installed may have been lost and can no longer be replaced.

(iv) The software will no longer run under current computer operating systems

The DSS does not support software that falls into these categories. If a user or department needs assistance with such software, the DSS will recommend a currently supported software package that will perform the required functions and assist the user in making the transition to the new software.

DSS support all current versions Microsoft Windows and Mac OS operating systems. ICT also offers support for Linux/UNIX computers.

4.4 ***Backups of Desktop Data***

In the event the employee gets a new computer or hard drive replacement, the University will not be responsible for the restoration of data. It is recommended that the users of a computer make frequent backups as and when needed for the data.

5. DIGITAL INFORMATION SECURITY

Digital information is a vital asset to any organization, especially in a knowledge-driven organization, such as Central University of Kerala. This clause mainly deals with the management and security of critical/confidential/personally identifiable information (PII) which includes (i) preventing unauthorized access, (ii) dealing with cyber-attacks and malicious softwares (like virus, Trojan horse, worm etc.), (iii) misuse of ICT resources and services.

5.1 Information security implementation

Information security is implemented in the University through its technical controls (ie. administrative access controls to IT related facilities), firewalls, anti – malwares and backups of servers. The IT wing will ensure the that the latest updated security patches are always available. IT wing shall conduct periodic inspection to all IT related facilities to ensure security related compliance. IT wing shall co-ordinate with departmental IT-coordinators (nominated by the department) for implementing technical access controls.

There should be secure individual username and password combination for every service (ie. email, internet, wifi, access to servers) provided by the University. It shall be shared with other users. The users are responsible for the activities from their respective login account. Each common computer/device in department is secured with an administrative username and password which is known only to the concerned ICT Wing/ICT-Coordinators. However computers used by other faculty members or used in the Labs/Offices of other faculty members are exempt from this.

Currently there is no security classification for digital information. But it may be implemented, if needed, in future and the policy may be amended with suitable clause and procedures for the same.

5.2 Data retention Policy

In order to ensure that the critical data of Central University of Kerala is backed up regularly, the following important precautions shall be followed for minimizing risk by ICT wing

- Website data is backed up periodically
- Periodic backup from different servers that are used for specific functions.
- RAID to be configured on servers
- Data to be backed up in a separate Backup server
- Servers to be configured in DMZ

University currently do not have provision to provide server storage space to users. It will be enabled in the future based on the availability of the server storage space. In such cases, if the user request for space, based on availability, it will be provided to the user. Such space so allocated should not be used to store copies of personal photographs, music collections, etc. Multimedia documents stored for academic purposes are exempt from this clause.

5.3 Data Classification Policy

Central University of Kerala will classify its data under the following heads.

1. *Confidential*

   Any digital data which has to be protected from public/internal access which can result in legal ramifications (Eg:- Recruitment Data, E-Filing Data, Tendering Data, Student/Staff Personal Information) may be classified as confidential. This data shall be strictly protected with all access control measures to ensure that only concerned people have access to the data.

2. *Internal-Only*

   Digital Data which is required for conducting the day-to-day business of the University which will be processed and accessed by various staff shall use the Internal-Only Label. However, these details may be limited to access only to staff who has to process such data. (Eg:- Leave Details, Salary Details, Emails, Program Recordings etc)

3. *Public*

   Any data which has to be made publicly available through website/data coming under RTI shall be considered under public classification.

Procedure for moving data from a Higher Classification Level to Lower Classification Level

Data in the Confidential level can move to Internal-Only and then to Public. This has to be done with the approval of the Section Head handling the data. This has to be done in line with the "Central Secretariat Manual of Office Procedures".

6. NETWORK/WIFI SECUIRTY

6.1 Authentication methods

Security is implemented using authentication services like Firewalls, RADIUS/LDAP Authentication/ Wireless Access Point Authentication based on WPA/PSK2.

Issuance of an account to a system user must be given by the ICT Wing of Central University. The Username and password combinations are generated and controlled by Radius Authentication based on AAA (Authentication, Authorization and Accounting) procedures.

User will be held responsible for any misuse of account. Maximum Number of Concurrent (simultaneous) logins for a user account should be FIVE device either laptop/tablet/mobile.

6.2. WiFi Network Security

WiFi network access will be provided on a best effort basis to all desired locations including class rooms, seminar halls and locations frequented by faculty and students.

Any wireless network device that would extend the University network used by user and is not managed by the ICT Wing must be intimated. If ICT wing finds out any devices which are utilized as rogue devices, it will be subject to detection and immediate removal from the network.

The access points provided in the campus are the property of University and any damage or loss of the equipment will be considered as a serious breach of University's code of conduct and disciplinary action will be initiated on the student/faculty who found guilty for the loss or damage of the Wireless Infrastructure or the corresponding equipment in the campus.

7. MOBILE DEVICE USAGE POLICY

7.1 Definition of Mobile Device

As mobile devices further incorporate features traditionally found in a personal computer, their smaller size and affordability make these devices a valuable tool in a wide variety of applications. However, these devices are also subject to increased risk of loss, theft, and unauthorized use.

7.2 Purpose

These standards establish base configurations and management guidelines for mobile computing devices (e.g., cellular or smart phones, laptops, tablets, etc.) owned and/or operated by the Central University of Kerala or its workforce. As there are a wide variety of mobile device operating systems, software, and system configurations used across the University, this document is NOT intended to be a definitive and comprehensive guide to device security.

Compliance with these standards does not exempt a device from meeting federal, state, or local laws and regulations. For

example, if the device is collecting or storing credit card data, then the application and server must comply with all Payment Card Industry (PCI) standards.

Effective implementation of these standards will minimize the likelihood of unauthorized access to University computing resources and legally restricted and/or confidential information. All security events (e.g., loss of, or unauthorized access to device) must be reported to the appropriate personnel as soon as they are discovered, in order to ensure compliance with legal obligations.

7.3 Requirements

Physical Protection: Individuals must keep mobile devices with them at all times or store them in a secure location when not in use.

Password Protection: Access to the mobile device must be protected by the use of a password.

Encryption: University data classified as confidential must not be stored on a storage card or the device (including within cached email) without proper encryption, password protection and inactivity timeout.

Inactivity Time-out Protection: Inactivity timeout must be set. The recommended inactivity timeout is 5 minutes but must not exceed 60 minutes.

Proper Disposal: Any residual settings, data, and applications on the mobile device must be removed or wiped prior to disposal or transfer to another user. All attached storage cards that contain Perosnal Information must be destroyed or wiped so no data recovery is possible.

Lost or Stolen Device: If a mobile device containing Central University of Kerala information is lost or stolen, report the loss immediately to Central University of Kerala ICT Wing. They will initiate necessary action to protective/corrective action. In addition, the incident must also be reported immediately to the appropriate information technology Help Desk to determine if the device can be wiped remote

Secure Connectivity: Any Legally Restricted information transmitted to or from the mobile device (e.g., wireless or the Internet) should be encrypted. Communication protocols such as SMS (Text Messaging) are not considered secure and in some cases, like for Protected Identifiable Information (PHI), may result in a breach of confidentiality.

6.4 Additional Recommendations for Mobile Devices

Invalid Password Attempts: The device should be set to wipe after 10 invalid password attempts.
Disabling Unused Services: Wireless, infrared, Bluetooth or other connection features should be turned off when not in use.

Remote Wipe Capability: The mobile device should support the ability to remotely reset the device, including the deletion of all locally stored data.

8. EMAIL USAGE GUIDELINESS

Electronic mail (email) with domain @cukerala.ac.in is a primary means of communication both within the Central University of Keralaand externally. It allows quick and efficient conduct of digital communication, but if used carelessly or illegally, it carries the risk of harm to the University and members of itscommunity.

8.1 Eligibility for official Email-id.

The eligibility criteria for official email access is as following:

- Can be issued to all permanent staffs irrespective of their cadre.
- Can be issued to outsourced staffs based on approval from Registrar of the University.
- Students will be issued email authentication credentials on the request of the concerned HoDs. General format for the email ids for students should be as follows: "studentname.rollno"@cukerala.ac.in.

8.2 Email service

Email services are primarily intended to allow faculty and staff to conduct University business. Personal use of email is allowed, provided that personal use (a) does not materially interfere with performance of work responsibilities, (b) does not interfere with the performance of the University networks and (c) is otherwise in compliance with this and other University policies.

The University also reserves the right to inspect or check the access email accounts and contents with this policy in extreme cases, and to take such other actions as in its sole discretion it deems necessary to protect interests of the University based on approval of higher authorities. The University further reserves the right to enforce these provisions with or without prior notice to the user.

8.3 Email maintenance

Currently Central University of Kerala is having google education subscription for email service. Hence loss of email content is not the responsibility of ICT wing. In future if the University setup its own email server, then the ICT Wing will strive to ensure backups of data of all email account. In case of issue of hacking/ forgetting of password the faculty/student can contact the ICT Wing.

The official email ids of employees of the University will be deactivated within three months form the date of leaving Central University of Kerala. In the case of students/research scholars it will be deactivated within one week after the declaration of the result of the final semester.

Faculties relieved/retired from the University and PhD scholars who pass out of the University, their email ids may be permitted to retain for a few additional months based on the recommendation from the concerned head of the section.

9. SOFTWARE ASSET MANAGEMENT

The following general principles apply to Software Asset Management:

- It is the policy of the Central University of Kerala to respect all software copyrights and license agreement terms/conditions.
- Usage Non licensed/pirated software is strictly banned on University ICT facilities
- Non-University owned ICT facilities when connected to University network must comply with IT policy
- ICT facilities purchased with research and/or consultancy funds remain the property of the Central University of Kerala and are treated as University owned ICT facilities.
- Users may not give licensed or copyrighted software to any external parties (including, but not limited to clients, contractors, customers), unless expressly authorized to do so under the prevailing software agreement.
- Users may use software on local area networks, licensing servers, or on multiple machines only in accordance with the prevailing software agreement.
- Students/research scholar can obtain assistance with software copyright or license arrangements purchased in the departments through the corresponding ICT-coordinators of the concerned departments.
- Shareware, freeware and trial software users of the University are responsible for ensuring that their use of software is in accordance with IT Policy of University.

9.1 Acquisition of Software

To purchase software for the department/project/sections, a request from Faculty council/Principal Investigator of projects (PI)/section heads must be submitted to the purchase section.

Software should only be purchased after due approval from concerned authorities.
Once the software has been received and installed, ICT Co-ordinator/section heads/PI are responsible for ensuring that the original media, license documents, manuals and other associated material are securely and appropriately stored as University managed assets and maintained in a register.

9.2 Installation and Maintenance of Software

The software register should include the following information (as a minimum):

a. name of the software.
b. software vendor's name.
c. Date of purchase and installation.
d. Purchase cost
e. Purchase order no, invoice number and date
d. name of the authorised user(s) or installation location
f. a list of the associated documents/manuals and their location. In particular, this item should reference the location of the original software media and the license agreement document consisting of serial number (software key) of the software (where applicable).
h. software agreement expiry date (if applicable) / renewal date (if applicable)

All purchase related documents including the original media, license documents, manuals and other associated material must be maintained in the concerned sections for formal audits or license checks.

9.3 Legal Compliance

- Misuse or unauthorized use of University ICT facilities may constitute an offence under the ICT Act of Government of India or, as amended and/or other pieces of Government of India legislation.
- The University treats misuse of its ICT facilities seriously. Violations of the conditions of use of ICT facilities may result in temporary or indefinite withdrawal of access, disciplinary action under the University's, or relevant entities, discipline procedures, and/or reimbursement to the University.
- The decision on quantum of punishment will be made by ICT committee and the decision will be final. Most of the cases an initial warning will be given to the end-user. If the end-user repeatedly continues the same mistakes even after initial warning, the ICT committee may harden the punishments.
- Nothing in these guidelines or the associated Requirements Governing the Use of ICT Facilities may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.
- Under ICT Act of Government of India infringing copies of software may result in criminal penalties, including fines, imprisonment etc.

10. INTERNET USAGE

The University provides computing equipment and access to the internet to enable students/faculty/staff to carry out their work for the University.

a) The University will restrict access to certain categories of website and will manage this by classifying websites into three categories:
   (i) Sites that are available at all times, this is all sites except b & c below.
   (ii) Sites blocked during normal work hours, which is defined as between 9:00am to 5:30 pm Monday to Friday. These are categories of sites, as decided from time-to-time, that are very unlikely to have a legitimate work usage and include:
      - ✓ Auction sites
      - ✓ Dating sites
      - ✓ Gambling sites
      - ✓ Game sites
      - ✓ Hacking/Virus Sites
      - ✓ Social Networking Sites.

b) Sites that contain pornographic and/or objectionable material will be completely blocked as far as is practicable.
c) The ICT committee will determine the sites to be blocked upon a recommendation various stakeholder time-to-time.
d) Any staff member who has a legitimate need to access sites under categories b & c may apply through their Head to ICT Wing to gain access.
a) ICT Wing will be responsible for managing the internet restrictions and ensure that their internet access is filtered according to this Policy.
b) ICT Wing will advise the relevant Head of Department/sections and the Administration of any suspected breaches of this policy. Any concerns will be investigated in accordance with the procedures laid out per regulations of the University. Breaches of this policy may be viewed as serious misconduct which could result in disciplinary action being taken.

11. OPEN SOURCE POLICY

Central University of Kerala has resolved to adopt the open source policy of Government of India which has been issued by Government of India as part of Digital India programme.

Open Source Software: OSS is commonly known as Free and Open Source Software (FOSS). Here the "Free" refers to "Freedom to use" and not "Free of Charge". Here "Open Source" refers to the "availability of Source code for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software (without having to pay royalties to previous developers). The Open Source Software (OSS) shall have the following characteristics: The source code shall be available for the community / adopter / end-user to study and modify the software and to redistribute copies of either the original or modified software; Source code shall be free from any royalty.

Proprietary Software/ Closed Source Software: CSS/proprietary software typically prohibits the access to / modification of the source code. It restricts the copy, modification, distribution and reuse of the software. The restrictions may be applicable to the whole or part of the software so that the control is with the concerned company. Revenue, profit and IPR drive the development and marketing of the products and solutions.

Central University of Kerala has also been promoting the use of open source technologies, wherever possible, in order to leverage economic and strategic benefits. It is not mandatory and optional. However, in certain specialized domains where OSS solutions meeting essential functional requirements may not be available or in case of urgent / strategic need to deploy CSS based solutions

or lack of expertise (skill set) in identified technologies, the concerned sections/departments may consider exceptions, with sufficient justification

All Departments/Branches/Sections, while implementing/procuring software applications/hardware and systems must include a specific requirement in Request for Proposal (RFP) for all suppliers to consider OSS along with CSS while responding. Suppliers shall provide justification for exclusion of OSS in their response, as the case may be. Departments/Branches/Sections shall ensure compliance with this requirement and decide by comparing both OSS and CSS options with respect to need, necessity, capability, security and support requirements; where need and necessity will be given more importance during decision making process of selecting OSS or CSS.

ICT wing may conduct training depending upon the need/request and provide suitable support for moving towards OSS.

ICT wing shall actively collaborate with OSS communities in India as well as at the international level and contribute wherever appropriate.

12. GREEN COMPUTING

Metrics often used to assess the impact of sustainability-oriented programs include but are not limited to reductions of:

- Carbon footprint: CO2 and other greenhouse gases emitted by a human activity accumulated over the full life cycle of a ICT product or service (Wiedmann and Minx, 2008), expressed as equivalent Kg of CO2.
- Energy use: Generally expressed in KWH.
- Total cost of ownership (TCO).

ICT wing will strive to

- Raise awareness of the benefits of sustainable computing (**energy-aware** and **thermal-aware management** of computing resource. Spectrum of related issues such as applications of computing that can have **ecological** and **societal impacts)**.
- Reduce environmental impact of ICT resources, including but not limited to decreasing future energy demands, clean waste & obsolete equipment disposal.
- More importantly, reducing the carbon footprint of the organization.
- Redirect cost savings to improved ICT services.

Staff and Faculty of CU Kerala shall endeavor to:

1. Purchase energy efficient computers
2. Purchase hardware appropriate for the job
3. Replace a CRT monitor with an LCD monitor
4. Turn off your computer when it is not in use for several hours
5. Effective use of Printer
6. Effective management of Electronic Waste
7. Enable power management features on your computer
8. Avoid phantom power from connected devices
9. Recycle of old computers

Buy energy efficient computers

While procuring computers/hardware it may be ensured that they are BEE (Bureau of Energy Efficiency)/ BIS (Bureau of Indian Standards) certified. There are online tools to assist in making your selection of energy efficient computers easier. ENERGY STAR has an online product search tool to assists people seeking energy efficient desktop and laptop computers. You can also use the Electronic Product Environmental Assessment Tool (EPEAT), which will similarly assist in buying a computer.

Buy hardware appropriate for the job

Computers and other devices should be appropriate for the work that they are intended to support, and purchasing decisions have longer term ramifications.

Turn off your computer when you will not be using it for several hours

Frequent shut-downs will not damage computers, and they may even actually last longer if shut off regularly. Turning off computers at the end of the day is a way to decrease related energy costs by 60% and reduce the University's environmental footprint.

Print Efficiently

You can save money and the environment during printing by the following the instructions given below:

- Use recycled paper.

- Have a recycle bin at each community printer and copier location. Recycle your paper, as opposed to throwing it out.
- Print as little as possible. Review and modify documents on the screen and use print preview. Minimize the number of hard copies and paper drafts you make. Instead of printing, save information to disks, or USB memory sticks.
- Use e-mail instead of faxes or send faxes directly from your computer to eliminate the need for a hard copy.
- Don't leave your printer on when you're not printing.
- Use the electronic print preview to avoid waste of papers
- Print double-sided.
- Print draft copies when appropriate; these use less ink, and are still readable.
- Re-use hardcopies (i.e., printouts) with lots of blank space as scrap paper for notes.

Be Aware of Electronic Waste

- Use the campus network where possible to transfer files. This avoids the need to write CDs or DVDs or use floppy diskettes.
- Use USB memory sticks instead of CDs, DVDs, or floppies
- Use re-writable CDs and DVDs, if atmost necessary.

Enable power management features on your computer

Computers have power management functions such as hibernation or sleep modes to place the computer on low power after a period of inactivity. They are required to use 4 Watts or less of electricity when in lower power, which is less than 5% of the average computer's peak electrical demand.

Avoid phantom power from connected devices

Whenever plugged-in all electronic devices, including computers, still consume energy even if they turned off or in standby mode. To make eliminating phantom power usage easier, plug your computer and its peripherals into a power strip, and unplug the strip when you are not using your computer.

Recycling of old computers

When you no longer are able to find a use for your computer, consider ways to recycle it properly by following the e-waste policy of the CUK. The ICT devices aged more than 6 years may be replaced through the proper buyback policy as part of green computing.