ख़्वाजा मुईनुद्दीन चिश्ती भाषा विश्वविद्यालय,
लखनऊ

KHWAJA MOINUDDIN CHISHTI LANGUAGE UNIVERSITY, LUCKNOW

U.P. STATE GOVERNMENT UNIVERSITY

IT POLICY

1. Abbreviation

Sl. No.	Abbreviation	Description
	KMCLU	Khwaja Moinuddin Chishti Language University
	CA	Competent Authority
	IA	Implementing Agency
	LAN	Local Area Network
	GoI	Government of Indla
	IT	Information Technology
	ICT	Information and Communication Technology
	IP	Internet Protocol
	DHCP	Dynamic Host Configuration Protocol
	IR	Institutional Repository
	EULA	End User License Agreement
	CAPEX	Capital Expenditure
	OPEX	Operational Expenditure

2. Introduction

Khwaja Moinuddin Chishti Language University (KMCLU) provides IT resources to support the educational, instructional, research, and administrative activities of the University and to enhance the efficiency and productivity of the employees. These resources are meant as tools to access and process information related to their areas of work. These resources help them to remain well informed and carry out their functions in an efficient and effective manner.

This document establishes specific requirements for the use of all IT resources at KMCLU. This policy applies to all users of computing resources owned or managed by KMCLU. Individuals covered by the policy include (but are not limited to) KMCLU faculty member and visiting faculty member, staff, students, alumni, guests, external individuals, organizations, departments, offices and any other entity which fall under the management of Khwaja Moinuddin Chishti Language University accessing network services via KMCLU's computing facilities.

For the purpose of this policy, the term IT Resources includes all University owned, licensed, or managed hardware and software, and use of the University network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Misuse of these resources can result in unwanted risk and liabilities for the University. It is, therefore, expected that these resources are used primarily for University related purposes and in a lawful and ethical way.

3. Scope

This policy governs the usage of IT Resources from an end user's perspective. This policy is applicable to all individuals/users/entities, as defined in Section2, who use the IT Resources of KMCLU.

4. Objective

The objective of this policy is to ensure proper access to and usage of KMCLU's IT resources and prevent their misuse by the users. Use of resources provided by KMCLU implies the user's agreement to be governed by this policy.

- University IT policy exists to maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established by the University on the campus.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that are accessed, created, managed, and/or controlled by the University.
- Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

5. Roles and Responsibilities: Computer Centre Staff

Post	**Role**
System Manager	Administrate all the activities in the Computer Centre related to University Network and Computer Lab. Managing a team of staff including System Engineer, Programmers and Senior Technical Assistant and support specialists. Evaluating the functionally of systems. Selecting and purchasing appropriate hardware and software, managing IT budgets. Support and administer third-party applications. Testing and modifying systems to ensure that they operate reliably. Creating and Maintaining the institutional email IDs.
Network Engineer/ Administrator	Administrate the whole network of the University including network equipment configuration and management. Maintenance of all the servers. Maintenance and look after all the other activities related to Computer Centre. Look after the CCTV, database of CCTV footage. Maintenance of video conferencing servers in the University.
Computer Programmer cum Web Developer	Coding and debugging. Designing and testing computer structures. Troubleshooting system errors. Administrate and maintenance of University website, ERP & Support administer third-party applications.
Database Administrator cum Database Developer	Planning, designing, creating, testing, implementing, protecting, operating, managing and maintaining University databases. Designing database backup, archiving, and storage strategy. Coordinate with the System Manager and System/Network Engineer to design stable and reliable databases and Modify databases as needed. Work with Computer Programmers to establish best practices for database storage and organization.
Web Designer	Draw up detailed website specifications. Design sample web page layouts including font, text size and colours. Ensuring

	website function and stability across devices i.e., desktop, mobile, tablet etc. Design graphics, animations and manipulate digital photographs. Register web domain names and organise the hosting of the website. Meet relevant legal requirements such as accessibility standards, freedom of information and privacy. Design the website's visual imagery and ensure it's in line with University policy. Liaising with programmers and DBA to ensure website and app logic is properly integrated. Resolve problems reported by end user. Support and administer third-party applications.
Network Assistant	The Network Assistant will assist the System/Network Engineer in the performance of a variety of duties. Assist in testing and the installation of network devices. Assist in checking of network data connections fabricate, punch down and terminate cables. Monitor network performance (availability, utilization, throughput, and latency) and test for weaknesses. Test and diagnose data communication problems. Assist in maintaining network documentation. Support and administer third-party applications. Set up user accounts, permissions and passwords. Resolve problems reported by end user.
Desktop Support Engineer	Addressing user complaints regarding hardware, software and networking. Walking users through installing applications and computer peripherals. Guide users with simple, step-by-step instructions. Test alternative pathways until you resolve an issue. Help create technical documentation and manuals. Advising on software or hardware upgrades. Providing basic training in computer operation and management. Monitor the performance of a University's desktop infrastructure and provide suggestions to improve efficiency. Train end users when new software or IT regulations arrive at a university.
Attendant	Responsible for cleaning and servicing the Computer Centre. Close and open Computer Centre on time. Clean and sanitize IT

	equipments.

Following guidelines/policies will be implemented/ look after through University Administration and Computer Center for various IT related work/activities.

6. Internet and Email Usage Policy Guidelines

- Internet facility is provided to all students and staff of University through registration process at the computer center.
- University website is maintained at the computer center.

  a) All updates and uploads are done by centre staff only after receiving written requests/emails from various Departments/Sections which are routed through Registrar.

  b) Contents of all pages shall be standardized as per the standard design pre-approved by the University Website Committee.

  c) All Content owners shall follow the pre-approved design while maintaining their respective web pages at the University website.

  d) Private, confidential, and sensitive information should not be uploaded by any individual/section/office/department to the web server. Data found in violation of this policy may be deleted by University, without warning.

  e) Archives of old Notices/orders etc. are maintained at the server as back-up and can be accessed only by authorized persons.

- Institutional Email ID is provided to all teaching staff (regular and contractual) and students of University through the submission of Non-Disclosure Agreement at the Computer Centre. Institutional Email ID may be provided to the any other employee of the University by the approval of Vice Chancellor and Registrar.
- Procurement of IT related services / Internet Services / Hardware, Software and other items as required time to time are done by following due procedure.

a) Identification of need for various items, justification and specifications etc. are finalized by various standing committees constituted by University for purpose.

b) Procurements are done mainly through computer centre and centralized department of University.

- Computer center staff provides primary services to maintain all computers / printers etc.

Non-Disclosure Agreement; NDA

1. Access to Internet Services and E-mail Services of Khwaja Moinuddin Chishti Language University will be subjected to an approval process for all users (i.e. for students, faculty members and other staff members of the University), on a need basis, as decided by the University from time to time.

2. E-mail and Internet Services provided by the University will be subjected to monitoring and surveillance from time to time, for checking compliance with policy guidelines.

3. Misuse and/or illegal usage of the E-mail/Internet Services provided by the University by any user (be it a student or staff) will make the concerned user liable to disciplinary actions as deemed appropriate by competent authorities (including suspension/termination of E- mail/Internet Services, imposition of fine, legal actions etc.)

4. Students and Staff Member(s) (other than those specifically authorized to do so) should not use E-mail/Internet Services provided by Khwaja Moinuddin Chishti Language University for any communication that may have legal or commercial implications for the University like sending LoIs (Letters of Intent), Purchase Orders, Tender Documents etc.

5. Owners of a User ID (be it an E-mail ID or Internet User-ID) are solely responsible for its usage and all the activities undertaken by the User ID allocated to them.

6. Users are expected to keep their e-mail accounts active by checking their emails regularly, managing their disk quota judiciously by archiving & purging old e-mails periodically and following the instructions communicated by the IT Helpdesk from time to time.

7. Recommended Good Practices for Internet/Email Usage:

1. Users should change the initially allocated password (on the first login itself), keep the password confidential, and keep changing it regularly and periodically.

2. Set your Homepage to an appropriate URL for fast access. Many people on campus use the KMCLU Website (www.kmclu.ac.in) as their Homepage.

3. Material downloaded from the Internet must be scanned with virus detection software before installation or execution.

4. When using information from an Internet site for important decision type purposes verify the integrity of the data. The fact that the information is there does not mean that it is correct. Many sites do not get updated regularly.

5. Never reply to spam or junk e-mails nor click on hyperlinks embedded in them you are merely confirming your existence to the spammers.

6. Do not use e-mail to discuss confidential information.

7. Avoid sending unnecessary attachments.

8. When replying to mail received as a member of the mailing list, take care to note whether your reply is to the individual sending the message or to the whole list.

9. The University will never ask you for your password or renewal of your account. If you receive any email asking for such information, consider it spam, block it in your mailbox and inform the IT Help Desk immediately.

8. It is prohibited to:

1. Access, create, copy or transfer web pages or other material accessible across the illegal Internet, offensive, harassing, defamatory, obscene, racist, sexist or threatening.

2. Exchange proprietary information, trade secrets or any other privileged, confidential or sensitive information.

3. Engage in activities that conflict with regulations relating to Respect and Dignity within KMCLU.

4. Create copy or transfer unauthorized advertisements, solicitations or viruses.

5. Play games on computing facilities available for general access except were required formally as part of research work, course work, KMCLU-sponsored events or other KMCLU approved activity.

6. Use the facilities for betting and gambling type purposes.

7. Download or display inappropriate content, play music, download movies or send messages that interfere with or are offensive too others.

8. Publish information or statements about other people which could harm the reputation.

9. Use the University's name or logo to imply the endorsement by the University of other organization's products or services without written permission from the University Administration.

10. Send or forward e-mails containing offensive or disruptive content, which includes, but is not limited to, defamatory, harassing, offensive, racist, obscene or threatening remarks. Do not flood another system, network or user account with mail. If you receive an e-mail of this nature, you should inform the ***gsuiteadmin@kmclu.ac.in***

11. Send or forward chain letters, junk mail, spam and viruses.

12. Forge or attempt to forge e-mail messages.

13. Use e-mail to unlawfully solicit or exchange copies of copyrighted software.

14. Use E-mail/Internet Services provided by Khwaja Moinuddin Chishti Language University for any communication that may lead to any financial liability for the University like sending LoIs (Letters of Intent), Purchase Orders, Tender Documents etc. unless specially authorized to do so.

9. IT Disposal/Hazard Management:

The University administration and computer centre is committed to follow best practices and standards for IT-Disposal/Hazard management. The policy shall be reviewed and revised from time to time. When equipment is no longer fit for purpose or is beyond economic repair the following options may be considered:

- Redeployment within other units/departments of University
- Donation to a charitable or community organization
- Disposal of IT E-Waste in a secure and environmentally friendly manner

10. IT Enabled Surveillance System

The University administration and computer centre is committed to plan, design, deploy, augment, upgrade and maintain appropriate CCTV Surveillance systems at strategic locations across the University campus, as per safety and security purposes. Safety and security purposes include, but are not limited to:

- Protection of individuals, including students, faculty, staff and visitors.
- Protection of University owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, special storage area, laboratories, and cashier locations.
- Monitoring of common areas and areas accessible to the public, including transit stops, parking lots.
- Protection against an illegal activity.
- Protection of Critical Infrastructure Monitoring of crowd movements during University events.

11. Use of External Service Providers

- University administration and computer centre is committed to engage external service providers/collaborate 3rd-party, after approval from the competent authority, as and when deemed appropriate. However, while using such services, KMCLU shall use IT POLICY appropriate and standardized formats for Non-Disclosure Agreements (duly vetted by legal experts) that will be signed with external service providers/3rd parties. External service providers/3rd parties are liable to follow the rules and regulation of the University.

- University administration and computer centre is committed to engage external service providers, after approval from the competent authority, for all the digitalization work related to the Registrar, COE, Finance, Website, ERP, LMS, GSuite and other departments of the University.
- Verification of digitalization work will be done by the relevant staff of Computer Centre.

12. Network Security

- University administration & Computer centre is committed to provision Network's Security, using relevant best practices of planning, designing, implementation, enhancement, maintenance & upgrades from time to time, as per University's IT- Policies and Procedures.
- Connecting unprotected networking equipment (such as routers and wireless access points, etc.) to the University Owned Campus Network is prohibited.
- For security reasons, users shall opt for Identity-based access to the campus networks for using Campus Internet/Wi-Fi Services.