



Laxmi Charitable Trust's

Sheth L.U.J. College of Arts & Sir M.V. College of Science & Commerce
Dr. S. Radhakrishnan Marg, Andheri (East), Mumbai 400 069.

INFORMATION TECHNOLOGY (IT) POLICY

Sheth L. U. J. and Sir M. V. College is dedicated to use information technology and services effectively to accomplish its administrative, service, research, and teaching purposes. These guidelines must be followed by stakeholders to utilize the IT facilities as efficiently and ethically as possible. College reserves the right to monitor technology usage to ensure compliance with this policy and investigate suspected violations.

Aims and Objectives:

- It is mandatory to make appropriate, ethical, and legal use of college IT resources by all users.
- It is completely forbidden to use college technological resources for any kind of criminal, unlawful, or disruptive activity.
- Users are prohibited from engaging in any actions, such as hacking, unauthorized access, or malware distribution, that might harm college systems or networks.

Implementation:

- Personal use of college digital resources should be kept to a minimum and shouldn't interfere with work or academic-related tasks.
- **Backup Policy-** Users should regularly backup their important information. On a user's PC, virus attacks frequently result in loss of data. It might not be possible to retrieve deleted files without adequate backups. Data backup of the machine should be maintained in such a way that formatting the machine should not lead to loss of data. In addition, users have to store their important data on external storage devices / storage Cloud (preferably google drive).
- **Software Installation and Licensing Policy-**
The softwares installed on college computers should be licensed / open source software. College promotes use of open source / freeware software. The Institute's IT policy prohibits the installation of any illegal or pirated software on any of the Institute's owned computers or computers connected to the Institute campus network to comply with national



anti-piracy laws. If such a situation arises, the Institute will hold the department or individual directly liable for any pirated software that is placed on the computers.

- **Data Security** - Users are responsible for safeguarding sensitive information and ensuring compliance with data protection laws and regulations. Users must use strong passwords and refrain from sharing their credentials with others.
- **Network Usage** - Users must refrain from unauthorized use of computer network resources. Bandwidth-intensive activities that may degrade network performance for others, such as excessive streaming or file sharing, are discouraged. Users should refrain from engaging in activities that may compromise network security, such as connecting unauthorized devices or running unauthorized servers.
- **Internet Policy** - Internet access provided by College is to be used for educational, research, and administrative purposes. Users must refrain from accessing or downloading inappropriate or offensive content, including but not limited to pornography, hate speech, or copyrighted materials without proper authorization. Users are prohibited from engaging in activities that may pose security risks to college systems, such as visiting malicious websites or downloading unauthorized software.
- **Social Media and Online Communication-** Users representing College on social media platforms must maintain professionalism and respect in their interactions. Users should exercise caution when sharing personal information online and avoid posting content that may harm the reputation of the college or its members.
- **Cyber Bullying-**
Cyberbullying, an unacceptable action that threatens the safety of individuals and the reputation of our college, shall not be tolerated under any circumstances. Strict action will be taken against individuals found to be involved in cyberbullying activities.




I/C PRINCIPAL