

IT POLICY

Document	Policy and Procedures Compendium
Department	Administrative Office
Document Code	AO/P&P/12
Title	IT POLICY
Approved by	Maharani Lakshmi Ammanni College Trust (Regd.)

1. Need for IT Policy

The Information Technology (IT) Policy of the institution defines rules, regulations and guidelines for proper procurement, usage and maintenance of technological assets.

The IT policy ensures legal and appropriate ethical use of computing facilities that include computer hardware, software, email, information resources, intranet and Internet access facilities, website hosting, online content usage, data backup, safety and security of data, products, facilities and users in the campus. It also provides guidelines for purchase of technological assets, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used at work place. IT policy is required to set direction and provide information about acceptable actions and policy violations.

Due to the dynamic nature of Information Technology, IT policy should be modified regularly to reflect technology changes, user requirements and operating procedures.

2. Elements of IT Policy

2.1 Users

The policies will be applicable at two levels:

- ✓ End Users' Groups (Principal, Faculty members, Students, Finance Officer, Administrative Officer, Controller of Examinations and other staff)
- ✓ IT Administrator, Network Administrator, System Administrator
- ✓ Guest User

The End Users may be UG/PG/Research Students. The Employees may be permanent/ temporary/ contractual. The Administrative Staff may be Non-technical/Technical. There may be guests who require to use the resources occasionally during Seminars/Workshops/Conferences/Inter-collegiate fests etc.

ATTESTED

2.2 Resources

The resources may be

- ✓ Wired/wireless Network Devices
- ✓ Internet Access

Sushree A

Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

- ✓ Official Websites/Web Applications
- ✓ Official Email services
- ✓ Data Storage
- ✓ Mobile/ Desktop/Server/Laptop computing facility
- ✓ Documentation facility (Printers/Scanners)
- ✓ Multimedia

2.3 Operations

The IT policy defines the operations of Purchase, Compliance, Equipment usage, maintenance and security, Inventory Management, Employee Training, IT Support and IT Audit.

2.3.1 Purchase

1. All approved technological equipment, services or software will be purchased through the Purchase Department assisted by IT Department while evaluating best and most cost-effective hardware or software to be purchased for a particular department/ project/ purpose based on the requirement.
2. The IT Department will also make sure all hardware/software standards defined in the IT Policy are enforced during such purchases.

2.3.2 Compliance

IT policy rules and guidelines should be complied by all employees while purchasing, using and maintaining any equipment or software purchased or provided by the institution. All approved software will be purchased through the Purchase Department, unless informed/permited otherwise.

1. Any employee who notices misuse or improper use of equipment or software in the college must inform his/her Head of Department immediately.
2. No employee is allowed to install pirated software on official computing systems.
3. Software purchased by the organization and installed on computer systems must be used within the terms of its license agreement.
4. Any duplication, illegal reproduction or unauthorized creation, use and distribution of licensed software within or outside the college is strictly prohibited. Any such act will be subject to strict disciplinary action.

2.3.3 Equipment Usage, Maintenance and Security

1. All employees are to take responsibility to ensure safe and judicious use of the technological assets being used by them.
2. Any observation of malfunctioning of any equipment of the college must be immediately informed to the designated staff in IT Department.

ATTESTED


Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

Malleswaram, Science Post, Bangalore - 560 012.

Tel. : 080-2334 9311 email : mlacw@mlacw.org, www.mlacw.edu.in

3. Any repeated occurrences of careless use, wastage of supplies or any such offense compromising the safety or health of the equipment and people, will be subject to disciplinary action.

2.3.4 Inventory Management

1. The Purchase Department is responsible for maintaining inventory of all technological assets and software purchased by the college.
2. The inventory sheet should contain the following information:
 - a. Item Name
 - b. Brand/ Company Name
 - c. Serial Number
 - d. Basic Configuration
 - e. Physical Location
 - f. Date of Purchase
 - g. Cost
 - h. Person In-Charge
3. Proper information about all technological assets provided to a specific department, project or centre must be regularly maintained in their respective Inventory Sheets by an assigned coordinator of the respective department, project or centre on a regular basis. This information must be shared with the Purchase Department as and when requested.
4. Whenever an Inventory Sheet is to be updated or modified, the previous version of the document should be retained and the date of modification should be recorded in the sheet.
5. All technological assets of the organization must be physically tagged with Bar codes for easy identification.
6. Periodic inventory audits will be carried out by the IT Department to validate the inventory and make sure all assets are up-to-date and in proper working condition, to achieve maximum efficiency and productivity.

2.3.5 Employee Training

1. Basic IT training and guidance is to be provided to all new employees about using and maintaining their Personal Computer (PC), peripheral devices and equipment in the college. Also training has to be provided in accessing the organization network and using the required application software.
2. IT training can be conducted on a regular or requirement basis depending on employees requisition and/or the Management decision.

ATTESTED


Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

2.3.6 IT Support

1. Employees may need hardware/software installations or may face technological issues which cannot be resolved on their own.
2. Faculty members of the college can register a call log through IT Support Email ID specifying the details of the issues. The IT Department should provide IT support to all departments and faculty members.
3. Any IT Support work informed or assigned via emails sent on employee email IDs, chats or any other media except the IT Support Email ID would not be entertained.
4. For major issues like PC replacement, non-working equipment, installation of application software and more, it is mandatory for all employees to inform the IT Dept.
5. For any damage to Personal Computers, approval from Principal would be required for Personal Computer replacements.
6. Employees should expect a reply from the IT Department within 1 working day. The IT Department may ask the employee to deposit the problematic equipment to the IT Service Centre for checking and will inform the timeline for repair/maintenance/troubleshooting/installations or the required work.
7. If there is no response in 1 working day, then the IT Department designated staff should be asked for an explanation for the delay. If no response is obtained in 3 working days, a complaint can be raised through an email to the Principal and IT Department designated staff.
8. Issues will be resolved on a First-Come-First-Serve basis. However, the priority can be changed on request at the sole discretion of the designated team in IT Department.

2.4 IT Audit

1. The IT Department will conduct periodic audit of software installed in all company-owned systems to make sure all compliances are being met.
2. Prior notice may or may not be provided by the IT Department before conducting the Software Audit.
3. During this audit, the IT Department will also make sure the anti-virus is updated, the system is scanned and cleaned and the computer is free of garbage data, viruses, worms or other harmful programmatic codes.
4. The full cooperation of all employees is required during such audits.
5. Periodically IT Audit should be conducted by a third party IT Audit firm.

3. IT Policy

IT policy includes the following:

1. IT Hardware Installation Policy
2. Software Installation and Licensing Policy
3. Network (Intranet & Internet) Usage Policy
4. Web Site Hosting Policy

ATTESTED


Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

5. E-mail Account Usage Policy
6. Online Content Usage Policy
7. Data Backup Policy
8. Information Security Policy
9. Database Usage Policy

3.1 Computer Hardware Policy

1. To accommodate varying needs in Administration, Academics and Research, computer purchases shall be standardized thus avoiding excessive variability and cost in equipment and software.
2. A list of preferred vendors should be maintained for procurement and maintenance of computing equipment.
3. The IT department will review computer hardware options available from the list of preferred vendors, at a minimum, annually to establish a list of standard configurations that will best meet the features and functionality requirements of all employees of the institution.
4. A five-year life cycle is to be established for computer hardware to meet the demands of new application requirements for instructional and administrative purposes.
5. Computer hardware deemed End-of-Life (EOL) will be properly disposed of by the Purchase Department. Hard drives/storage devices will be destroyed either internally by the IT department or through a third party.

Warranty & Annual Maintenance Contract

1. Computers purchased by any Section/Department/Project should come with 3-year on-site comprehensive warranty.
2. After the expiry of warranty, computers should be under Annual Maintenance Contract AMC. The maintenance should include OS re-installation and virus related problems.

3.2 Software Installation and Licensing Policy

Policy is defined to provide guidelines for appropriate installation, usage and maintenance of software products installed in organization-owned computers.

1. Any computer purchases made by the individual departments/projects should make sure that such computer systems have all licensed software (operating system, antivirus software and necessary application software) installed.
2. Respecting the anti-piracy laws of the country, the IT policy does not allow any pirated/unauthorized software installation on the college owned computers in the campus. In case of any such instances, university will hold the department/individual personally.

ATTESTED

Shasheela
Principal
Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.

responsible for any pirated software installed on the computers located in their department/individuals' rooms.

3. Any MS Windows OS based computer that is connected to the network should access <http://windowsupdate.microsoft.com> web site for free updates. Such updating should be done at least once in a week. Even if the systems are configured for automatic updates, it is users' responsibility to make sure that the updates are being done properly. Use of open source tools is encouraged provided it has been pre-approved by the IT Department.
4. Any external storage device like pen drive or hard disk connected to the PC needs to be completely scanned by the Antivirus software before opening it and copying files to/from the device.
5. Technical support will not be provided for hardware devices or software which are personally purchased, illegal or not included in the standard hardware/software list developed by the IT Department.
6. Software applications that cause problems with the college systems as evaluated by the IT Department will be removed.

Software Registration

1. Software licensed or purchased by the organization must be registered in the name of the organization with the Job Role or Department in which it will be used and not in the name of an individual.
2. After proper registration, the software may be installed as per the Software Usage Policy of the organization. A copy of all license agreements must be maintained by the IT Department.
3. After installation, all original installation media (CDs, DVDs, etc.) must be safely stored in a designated location by the IT Department.

Antivirus Software and its updating

1. Computer systems used in the campus should have anti-virus software installed, and it should be active at all times.
2. Individual users should make sure that respective computer systems have current virus protection software installed and maintained.
3. Employees are expected to make sure their antivirus is updated regularly. The IT Department should be informed if the antivirus expires.
4. Antivirus software that is running on a computer, should be periodically updated/renewed after its warranty period by the service provider.

ATTESTED

Software Usage Policy

1. Third-party software (free as well as purchased) required for day-to-day use shall be preinstalled onto all company systems before handing them over to employees. A designated


Principal

Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.

person in the IT Department can be contacted to add to/delete from the list of pre-installed software on organizational computers.

2. No other third-party software – free or licensed can be installed onto a computer system owned or provided to an employee by the organization, without prior approval of the IT Department.
3. To request installation of software onto a personal computing device, an employee needs to send a written request via the IT Ticket System or IT Support Email.
4. Any software developed & copyrighted by the organization belongs to the organization.
5. Any unauthorized use, storage, duplication or distribution of such software is illegal and subject to strict disciplinary action.

3.3 Internet Usage Policy

The Internet Usage Policy provides guidelines for acceptable use of the organization's Internet network so as to devote Internet usage to enhance work productivity and efficiency and ensure safety and security of the Internet network, organizational data and the employees.

1. All PCs being used in the college are enabled to connect to the organization's Local Area Network as well as the Internet. All the computers should follow the standard naming convention.
2. Network Security is enabled in all PCs through Firewall, Web Security and Email Security software. Any employee who attempts to disable, defeat or circumvent the firewall will be subject to strict disciplinary action.
3. Internet bandwidth acquired by any section/department of the college under any research programme/project should ideally be pooled with the Internet bandwidth of the college, and be treated as common resource.
4. As the Internet Unit is running the Firewall security, Proxy, DHCP, DNS, Email, web and application servers and managing the network, it should be used such that problems related to uncontrolled surfing by the users such as choking of available bandwidth, exposure to legal liability due to harmful and embarrassing content surfing, confidential information being made public, are avoided.
5. Internet is a paid resource and therefore shall be used only for office work. The organization has systems in place to monitor and record all Internet usage on the organization's network including each website visit, and each email sent or received. The Management Committee can choose to analyse Internet usage and publicize the data at any time to assure Internet usage is as per the IT Policy.
6. The campus network and its active components are administered, maintained and controlled by IT Department. The service levels are to be maintained as required by the College office, departments, and divisions served by the campus network within the constraints of operational best practices.
7. A neat network diagram is to be maintained and displayed for the benefit of all users.
8. Internet Activity is to be monitored actively by IT Department.
9. Wherever access through Fiber Optic/UTP cables is not feasible, in such locations Internet Unit considers providing network connection through wireless connectivity.

ATTESTED

[Signature]
 Principal

Maharani Lakshmi Ammanni College
 for Women, Autonomous
 Science Post, Bangalore - 560 012.

10. Electronic logs that are created as a result of the monitoring of network traffic need only be retained until the administrative need for them ends, at which time they should be destroyed.
11. All network failures and excess utilization are to be reported to the IT Department for problem resolution.

Inappropriate Use

1. The following activities are prohibited on organization's Internet network. This list can be modified/updated anytime by the Management as deemed fit.
2. Any disciplinary action considered appropriate by the Management (including legal action or termination) can be taken against an employee involved in the activities mentioned below:
 - Playing online games, downloading and/or watching games, videos or entertainment software or engaging in any online activity which compromises the network speed and consumes unnecessary Internet bandwidth
 - Downloading images, videos and documents unless required to official work
 - Accessing, displaying, uploading, downloading, storing, recording or distributing any kind of pornographic or sexually explicit material
 - Accessing pirated software, tools or data using the official network or systems
 - Uploading or distributing software, documents or any other material owned by the organization online without the explicit permission of the Management
 - Engaging in any criminal or illegal activity or violating law
 - Invading privacy of co-workers
 - Using the Internet for personal financial gain or for conducting personal business
 - Deliberately engaging in an online activity which hampers the safety & security of the data, equipment and people involved.
 - Carrying out any objectionable, frivolous or illegal activity on the Internet that shall damage the organization's reputation.

Internet Login Guidelines

- 1) All employees may be provided with a Username and Password to login to the Internet network in the office and to monitor their individual usage.
- 2) An employee can also get a local static IP address for internet and intranet use. All employees will be responsible for the internet usage through this local static IP.
- 3) Username and password for a new employee must be requested by the Head of the Department.
- 4) Sharing the Username and Password with another employee, visitor or guest user is prohibited.
- 5) A visitor or guest user who wants to use the office Internet will be given a Guest Username and Password.

ATTESTED

Sleshlee A

Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

- 6) The IT Department will define guidelines for issuing new passwords or allowing employees to modify their own passwords.
- 7) Any password security breach must be notified to the IT Department immediately.
- 8) Username and password allotted to an employee will be deleted upon resignation/termination/retirement from the organization.

3.4 Website Hosting Policy

The faculty, administrators, and students of mLAC seek to provide up to date, accurate and meaningful information on college website. The integrity and reputation of mLAC relies on consistent and strong content on the "mlacw.edu.in" domain and on any websites that relate to, refer to, or could be perceived as representing the college.

This policy provides requirements for such websites, to ensure that they are accurate, current, useful, accessible and attractive.

All members of the college with responsibility for creating, maintaining or managing mLAC Website and Web-Enabled content are responsible for ensuring that such website and content are compliant with this policy and the related standards and guidelines.

Site Disclaimer

The materials and information on the college website may include technical inaccuracies or typographical errors. The materials, information and services on the site are provided "*as is*" without any conditions, warranties or other terms of any kind.

Copyright & Limited License

1. The website and all content and other materials, the mLAC logo and all designs, text, graphics, pictures, information, data, software, other files and the selection and arrangement thereof are the proprietary property of mLAC and are protected by copyright laws.
2. Any use of the site or site materials other than as specifically authorized herein, without the prior written permission of the college, is strictly prohibited.
3. Such unauthorized use may also violate applicable laws, including, without limitation, copyright and trademark laws and applicable communications regulations and statutes.
4. A limited, non-exclusive right to create text hyperlinks to this site for noncommercial purposes is granted, provided such links do not portray mLAC in a false, misleading, derogatory or defamatory manner and provided further that the linking site does not contain any obscene, pornographic, sexually explicit or illegal material or any material that is offensive, harassing or otherwise objectionable. This limited right may be revoked at any time.
5. mLAC makes no claim or representation regarding, and accepts no responsibility for, the quality, content, nature or reliability of third-party websites accessible via hyperlink or websites

ATTESTED


Principal

Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.

linking to this site. Such sites are not under the control of the college is not responsible for the content of any linked site or any link contained in a linked site.

Modifications to the Site

mLAC reserves the right to modify or discontinue, temporarily or permanently, this site or any features or portions thereof without prior notice. mLAC will not be liable for any modification, suspension or discontinuance of the site or any part thereof.

Information Collection & Storage

When anyone visits mLAC website, automatically information is gathered and stored so that the use of website can be tracked to make improvements.

Information gathered includes:

- IP address from which you access our site
- Name of the domain from which you access the internet
- Type of browser and operating system used to access our site
- Date and time you access our website
- Pages, files, documents and links that you visit
- Domain name of the website from which you linked to our site

mLAC has implemented procedures to safeguard the integrity of its information technology assets including authentication, authorization, monitoring, auditing and encryption.

These security procedures have been integrated into the design, implementation and day-to-day operations of www.mlacw.edu.in as part of our continuing commitment to the security of electronic content as well as the electronic transmission of information.

Appropriate security measures are in place to protect against the loss, misuse or alteration of information that is collected from website visitor.

3.5 Email Account Usage Policy

1. All emails, chats and electronic messages stored, composed, sent and received by any employee or non-employee in the official electronic messaging systems are the property of the college.
2. The college reserves the right to intercept, monitor, read and disclose any messages stored, composed, sent or received using the official electronic messaging systems.
3. The college reserves the right to alter, modify, re-route or block messages as deemed appropriate.
4. IT Administrator can change the email system password and monitor email usage of any employee for security purposes.

Confidentiality

ATTESTED


Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

1. Proprietary, confidential and sensitive information about the organization or its employees should not be exchanged via electronic messaging systems unless pre-approved by the HOD/Principal.
2. Before composing or sending any message, it should be noted that electronic messages can be used as evidence in a court of law.
3. Unauthorized copying and distributing of copyrighted content of the organization is prohibited.

Email Security

1. **Anti-Virus:** Anti-virus software should be installed in the laptop/desktop used for office work. Employees are prohibited from disabling the anti-virus software on laptops/desktops. Employees should make sure their anti-virus is regularly updated and not out of date.
2. **Safe Email Usage:** Following precautions must be taken to maintain email security:
 - a. Do not open emails and/or attachments from unknown or suspicious sources unless anticipated by you.
 - b. In case of doubts about emails/ attachments from known senders, confirm from them about the legitimacy of the email/attachment.
 - c. Use Email spam filters to filter out spam emails.
3. **Inappropriate Use:** Official Email platforms or electronic messaging systems including but not limited to chat platforms and instant messaging systems should not be used to send messages containing pornographic, defamatory, derogatory, sexual, racist, harassing or offensive material.
4. Official Email platforms or electronic messaging systems should not be used for personal work, personal gain or the promotion or publication of one's religious, social or political views. Spam/bulk/junk messages should not be forwarded or sent to anyone from the official email ID unless for an officially approved purpose.

Password Guidelines

The following password guidelines can be followed to ensure maximum password safety.

1. Select a Good Password:

- a. Choose a password which does not contain easily identifiable words (e.g., your username, name, phone number, house location etc.).
- b. Use 8 or more characters.
- c. Use at least one numeric and one special character apart from letters.
- d. Combine multiple unrelated words to make a password.

2. Keep your Password Safe:

- a. Do not share your password with anyone.
- b. Make sure no one is observing you while you enter your password.
- c. As far as possible, do not write down your password.

ATTESTED


Principal

Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.

- d. Change your password periodically (every 3 months is recommended).
- e. Do not reuse old passwords. If that is difficult, do not repeat the last 5 passwords.

3. Other Security Measures:

- a. Ensure your computer is reasonably secure in your absence.
- b. Lock your monitor screen, log out or turn off your computer when not at desk.

3.6 Online Content Usage Policy

1. Employees are solely responsible for the content accessed and downloaded using Internet facility in the office. If they accidentally connect to a website containing material prohibited by the organization, they should disconnect from that site immediately.
2. During office hours, employees are expected to spend limited time to access news, social media and other websites online, unless explicitly required for office work.
3. Employees are not allowed to use Internet for non-official purposes using the Internet facility in office.
4. Employees should schedule bandwidth-intensive tasks like large file transfers, video downloads, mass e-mailing etc. for off-peak times.

3.7 Data Backup Policy

Data Backup is setup during installation of Operating System in a PC. As an additional security measure, it is advised that employees keep important official data in some external storage device also.

File Backup System

1. Organization will be installing a file server for backing up data of all employees. All employee are expected to keep official data on the file system.
2. IT Department will have access to that data.
3. All employees will login to the file server through Active Directory Domain Controller ADDC1 user ID and password.

Server backup:

1. IT Department is expected to maintain an incremental backup of all servers with at least 3 copies of all servers. At any time, 3 backups of all servers must be maintained.
2. Replica mode of all running servers will be offline and it should maintain half-hourly backup.

ATTESTED


Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

3.6 Information Security Policy

Information security means protection of the organization's data, applications, networks and computer systems from unauthorized access, alteration and destruction. The Information Security Policy provides guidelines to protect data integrity based on data classification and secure the organization's information systems.

1. Various methods like access control, authentication, monitoring and review will be used to ensure data security in the organization.
2. Security reviews of servers, firewalls, routers and monitoring systems must be conducted on a regular basis. These reviews should include monitoring of access logs and intrusion detection software logs.
3. Appropriate training must be provided to data owners, data users, and network & system administrators to ensure data security.

Data Classification

1. The organization classifies data into three categories:
 - a. High Risk:** It includes information assets which have legal requirements for disclosure and financial penalties imposed for disclosure. E.g., Payroll, Personnel, Financial, Biometric data
 - b. Medium Risk:** It includes confidential data which would not impose losses on the organization if disclosed but is also not publicly available. E.g., Agreement documents, unpublished reports, etc.
 - c. Low Risk:** It includes information that can be freely disseminated. E.g., brochures, published reports, other printed material etc.
2. Different protection strategies must be developed by the IT department for the above three data categories. Information about the same must be disseminated appropriately to all relevant departments and staff.
3. High risk data must be encrypted when transmitted over insecure channels.
4. All data must be backed up on a regular basis as per the rules defined by the IT Department at that time.

Access Control

1. Access to the network, servers and systems in the organization will be achieved by individual logins and will require authentication.
2. All users of systems which contain high or medium risk data must have a strong password as defined in the IT Policy.
3. Default passwords on all systems must be changed after installation.
4. Where possible and financially feasible, more than one person must have full rights to any organization-owned server storing or transmitting high risk and medium risk data.

ATTESTED

Shesha

Principal

Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.

Virus Prevention

All servers and workstations that connect to the network must be protected with licensed anti-virus software recommended by the vendor. The software must be kept up-to-date.

3. Whenever feasible, system/network administrators must inform users when a virus/ other vulnerability has been detected in the network or systems.

Intrusion Detection

1. Intrusion detection must be implemented on all servers and workstations containing high and medium risk data.

2. Operating system and application software logging process must be enabled on all systems.

3. Server, firewall and critical system logs must be reviewed frequently.

3.9 Database Usage Policy

Data is a vital and important resource for providing useful information. Its use must be protected even when the data may not be confidential. It defines policies regarding the creation of database and access to information.

1. mLAC is the owner of all data generated in the institution.
2. Individual Sections or departments generate portions of data that constitute college database. The HOD may have custodianship responsibilities for portions of that data.
3. Data administration activities outlined may be delegated to some faculty member of each department by the HOD.
4. Distribution of data to persons outside the college is not allowed.
5. Data collected from various departments is for internal use only.

The database consists of the following information:

- ✓ Student Information
- ✓ Teaching/Non-Teaching Staff Information
- ✓ Financial Information
- ✓ Physical Resources (Infrastructure) Information
- ✓ Library Information
- ✓ Examination Results Information
- ✓ Placement and Higher Education Information
- ✓ Supplier (Vendor) Information

All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the IQAC Co-ordinator, Controller of Examinations and Finance officer of mLAC.

ATTESTED

[Signature]

Principal

Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 01

Tampering of the database by the department or individual user comes under violation of IT policy. Tampering includes, but not limited to :

- ✓ Modifying/deleting the data items or software components by using illegal access methods.
- ✓ Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals/ departments.
- ✓ Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- ✓ Trying to break security of the Database servers.

Such data tampering actions by any employee or outside members will result in disciplinary action against the offender by the college authorities.

If the matter involves illegal action, law enforcement agencies may become involved.

3.10 Video Surveillance Policy

The Video Surveillance system has been installed by college with the primary purpose of reducing the threat of crime generally, protecting college premises and helping to ensure the safety of all staff, students, and visitors consistent with respect for the individuals' privacy.

The Video Surveillance system comprises:

- ✓ Fixed position cameras
- ✓ Pan Tilt and Zoom cameras
- ✓ Monitors
- ✓ Multiplexers
- ✓ Digital recorders
- ✓ SAN/NAS Storage
- ✓ Public information signs

1. Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings.
2. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
3. Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.
4. The system assists the prevention and detection of crime.
5. It facilitates the identification, apprehension and prosecution of offenders in relation to crime and public order.

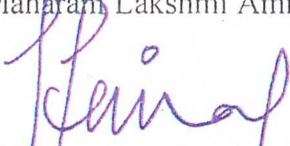
ATTESTED

[Signature]
Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**

6. It also facilitates the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to HOD and/or a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.

For Maharani Lakshmi Ammanni College Trust (Regd.)



Sri. K. Jairaj. IAS (Retd.)
Managing Trustee

MANAGING TRUSTEE

Maharani Lakshmi Ammanni College Trust (R.)
Malleswaram, Bangalore - 560 012

ATTESTED



Principal

**Maharani Lakshmi Ammanni College
for Women, Autonomous
Science Post, Bangalore - 560 012.**