Lords Institute of Engineering and Technology
(An Autonomous Institution)

IT Policies
2024

Index

Vision of the Institution

Lords Institute of Engineering and Technology strives continuously for excellence in professional education through quality, innovation and teamwork and to emerge as a premier institute in the state and across the nation.

Mission of the Institution

- To impart quality professional education that meets the needs of present and emerging technological world.
- To strive for student achievement and success, preparing them for life, career and leadership.
- To provide a scholarly and vibrant learning environment that enables faculty, staff and students to achieve personal and professional growth.
- To contribute to advancement of knowledge, in both fundamental and applied areas of engineering and technology.
- To forge mutually beneficial relationships with government organizations, industries, society and the alumni.

Quality Policy

Lords Institute of Engineering and Technology (A) imparts quality education by practicing a system of quality assurance that enables continued improvement in the teaching-learning process and enhances student's skills and talents.

Need for IT Policy

As a premier educational institution, Lords Institute of Engineering and Technology (LIET) relies heavily on Information Technology (IT) to support its academic, administrative, and operational functions. Implementing robust IT policies is essential to ensure the security, efficiency, and compliance of these activities. Here are the key reasons why LIET needs comprehensive IT policies:

1. Data Security and Protection

In an era where data breaches and cyber threats are increasingly common, safeguarding the personal information of students, faculty, and staff is paramount. IT policies at LIET will ensure that sensitive data, such as academic records and personal details, are protected against unauthorized access and breaches. By setting stringent data protection standards, LIET can maintain the confidentiality and integrity of its information assets.

2. Academic Integrity and Fair Use

To foster a culture of academic integrity, IT policies are necessary to prevent plagiarism and cheating. These policies will establish clear guidelines for the ethical use of digital resources, ensuring that students use technology responsibly. Furthermore, regulating the use of digital resources like software and online databases prevents misuse and promotes fair access.

3. Operational Efficiency

Standardized IT procedures contribute to operational efficiency by streamlining the management of the institution's IT infrastructure. This reduces downtime, enhances productivity, and ensures that hardware and software resources are utilized effectively. Clear IT policies help avoid confusion, improve resource allocation, and ensure that all IT operations run smoothly.

4. Risk Management and Business Continuity

Effective IT policies are vital for identifying and managing IT-related risks. By outlining protocols for risk management, data backup, and disaster recovery, LIET can protect its assets and ensure business continuity. These policies ensure that the institution can quickly recover from IT disruptions, maintaining continuous operations and minimizing the impact of potential incidents.

5. Access Control and User Management

IT policies define access rights, ensuring that only authorized personnel can access sensitive data. By preventing unauthorized use and regulating access to the institution's IT resources, these policies

help protect against data breaches and misuse. Clear guidelines on user management enhance security and accountability.

6. Training and Awareness

Regular training sessions informed by IT policies educate students, faculty, and staff on cybersecurity, data protection, and proper IT practices. By promoting a culture of security and responsibility, LIET can ensure that all users are aware of best practices and emerging threats, reducing the risk of human error and enhancing overall security.

7. Legal and Ethical Protection

Implementing clear IT policies helps protect LIET from potential legal issues by ensuring compliance with relevant laws and regulations. These policies clarify the responsibilities of both the institution and its users, reducing the risk of misunderstandings and disputes. By establishing a legal and ethical framework, LIET can safeguard its interests and maintain its reputation.

8. Support for Innovation and Growth

IT policies provide a framework for integrating new technologies into the institution's operations, supporting innovation and growth. By ensuring that IT resources and initiatives align with LIET's strategic objectives, these policies facilitate the adoption of cutting-edge technologies and promote continuous improvement.

Essential IT Policies for LIET:

Acceptable Use Policy: Defines acceptable use of the institution's IT resources.

Data Protection and Privacy Policy: Outlines measures to protect personal and institutional data.

Password Management Policy: Sets standards for creating and managing passwords.

Incident Response Policy: Provides guidelines for responding to IT incidents.

Backup and Disaster Recovery Policy: Ensures data is regularly backed up and can be recovered in case of an IT failure.

Network Security Policy: Establishes rules for securing the institution's network infrastructure.

BYOD (Bring Your Own Device) Policy: Regulates the use of personal devices on the institution's network.

By implementing these comprehensive IT policies, Lords Institute of Engineering and Technology can ensure a secure, efficient, and compliant IT environment that supports its educational mission and operational needs.

IT Hardware Installation Policy

Purpose:

The IT Hardware Installation Policy at Lords Institute of Engineering and Technology (LIET) is established to ensure proper, secure, and efficient installation of all IT hardware. This policy aims to standardize procedures, maintain system integrity, protect institutional data, and support the institution's operational needs.

Scope:

This policy applies to all IT hardware installations at LIET, including but not limited to computers, servers, networking equipment, and peripheral devices. It encompasses installations performed by IT staff, faculty, and any third-party service providers.

Policy Guidelines:

1. Authorization and Approval

- **Approval Requirement:** All hardware installations must be authorized by the ICT Committee Coordinator or System Administrator. No installation should proceed without written approval or request via official email to designated authority.
- **Request Submission:** Requests for new hardware installations or upgrades must be submitted through the official IT request form, detailing the purpose, specifications, and intended use.

2. Standardization and Compatibility

- **Standard Hardware Specifications:** The System Admin will maintain a list of approved hardware standards to ensure compatibility and support. All hardware installations must conform to these standards.
- **Compatibility Check:** Before installation, hardware must be checked for compatibility with existing systems and network infrastructure to prevent conflicts and ensure smooth integration.

3. Installation Procedures

- **Qualified Personnel:** Only IT personnel or authorized third-party service providers are permitted to perform hardware installations. All personnel must have the necessary training and expertise.
- **Pre-Installation Testing:** Hardware should undergo pre-installation testing to verify functionality and performance. Any defective components must be reported and replaced before installation.
- **Installation Documentation:** Detailed records of each installation, including hardware specifications, installation date, and responsible personnel, must be maintained. This documentation is essential for future reference and troubleshooting.

4. Security Measures

- **Physical Security:** Ensure that hardware is installed in secure locations to prevent theft, damage, or unauthorized access. Servers and critical network equipment should be housed in locked, climate-controlled environments.
- **Configuration and Updates:** Newly installed hardware must be configured according to security best practices and updated with the latest firmware and patches before being connected to the network.
- **Access Controls:** Appropriate access controls must be implemented on all installed hardware to protect against unauthorized use. This includes setting strong administrative passwords and limiting user access based on role requirements.

5. Post-Installation Procedures

- **Testing and Validation:** After installation, the hardware must be thoroughly tested to ensure it is functioning correctly and meets performance expectations. This includes network connectivity, system stability, and application compatibility.
- **User Training:** If necessary, training should be provided to users to familiarize them with the new hardware, including operational instructions and any new software interfaces.
- **Maintenance Scheduling:** A maintenance schedule must be established for regular inspections, updates, and servicing of the hardware to ensure long-term reliability and performance.

6. Disposal and Decommissioning

- **Decommissioning Process:** When hardware is to be decommissioned, it must be done following the IT Department's decommissioning procedures, which include data wiping, environmental considerations, and proper disposal methods.

7. Compliance and Monitoring

- **Policy Compliance:** Compliance with this policy will be monitored regularly. Any deviations must be reported to the IT Manager, and corrective actions will be implemented as needed.
- **Review and Updates:** This policy will be reviewed annually and updated as necessary to reflect changes in technology, security practices, and institutional requirements.

Software Installation & Licensing policy

Purpose:

The IT Software Installation and Licensing Policy at Lords Institute of Engineering and Technology (LIET) ensures the proper, secure, and legal use of software across the institution. This policy aims to standardize software installations, maintain system integrity, comply with licensing agreements, and support educational and operational needs.

Scope:

This policy applies to all software installations on LIET-owned devices and systems, including desktops, laptops, servers, and any other institutional IT resources. It covers software installed by IT staff, faculty, students, and third-party vendors.

Policy Guidelines:

1. Authorization and Approval

- **Approval Requirement:** All software installations must be approved by the System Administrator. Unauthorized installations are strictly prohibited.
- **Request Submission:** Software installation requests must be submitted through the official IT request form, detailing the software name, purpose, and licensing information.

2. Licensing Compliance

- **Valid Licenses:** Only software with valid licenses will be installed. The IT Department is responsible for managing and verifying all software licenses.
- **Compliance Monitoring:** Regular audits will be conducted to ensure compliance with all software licensing agreements and to avoid legal and financial repercussions.

3. Installation Procedures

- **Qualified Personnel:** Only authorized IT personnel are permitted to install software to ensure proper configuration and compliance with institutional standards.

- **Standard Software List:** The ICT Committee maintains a list of approved software to ensure compatibility and support. All installations must conform to this list unless an exception is granted.

4. Security Measures

- **Security Checks:** All software must be vetted for security vulnerabilities and approved by the ICT Committee before installation.
- **Regular Updates:** Installed software must be regularly updated with the latest patches and security updates to protect against vulnerabilities.

5. Documentation and Records

- **Installation Records:** Detailed records of each software installation, including license information, installation date, and responsible personnel, must be maintained for future reference and compliance audits.

6. User Responsibilities

- **User Training:** Users must receive appropriate training on the use of newly installed software, including understanding licensing restrictions and compliance requirements.
- **Reporting Issues:** Users are responsible for reporting any software issues or violations of the licensing agreement to the ICT Committee immediately through official email.

Network (Intranet & Internet) Use Policy

Purpose:

The Network (Intranet & Internet) Use Policy at Lords Institute of Engineering and Technology (LIET) establishes guidelines for the appropriate use of the institution's network resources. This policy aims to ensure a secure, reliable, and efficient network environment for all students, faculty, and staff.

Scope:

This policy applies to all users of LIET's network, including students, faculty, staff, and any guests or third-party service providers. It covers all devices connected to the network, whether owned by LIET or personally owned.

Policy Guidelines:

1. Acceptable Use

- **Educational and Institutional Purposes:** The network should primarily be used for educational and institutional activities that support LIET's mission. Personal use should be limited and must not interfere with academic or administrative operations.
- **Prohibited Activities:** Users must not engage in activities that are illegal, unethical, or disruptive to the network. Porn sites will be strictly prohibited. This includes downloading or distributing pirated software, accessing inappropriate content, and conducting unauthorized commercial activities.

2. Security and Privacy

- **User Responsibilities:** Users are responsible for maintaining the security of their devices and accounts. This includes using strong passwords, regularly updating software, and avoiding sharing login credentials.
- **Confidential Information:** Users must protect confidential information and must not share sensitive data over the network unless it is encrypted and properly secured.

3. Network Access and Usage

- **Access Controls:** Network access is restricted to authorized users. Users must use their assigned credentials to access the network and must not attempt to bypass security controls.

- **Bandwidth Management:** Users should use network resources judiciously. Activities that consume excessive bandwidth, such as streaming high-definition videos or downloading large files for non-academic purposes, should be minimized.

4. Monitoring and Compliance

- **Network Monitoring:** LIET reserves the right to monitor network activity to ensure compliance with this policy and to protect the network from security threats.
- **Compliance Enforcement:** Violations of this policy may result in disciplinary action, including suspension of network access, disciplinary review, or legal action.

5. Incident Reporting

- **Reporting Security Incidents:** Users must immediately report any security incidents, such as suspected breaches or unauthorized access, to the ICT Committee by written application or through official mail.
- **Assistance and Support:** The System Admin will provide assistance and support for network-related issues and ensure that all reported incidents are addressed promptly.

Email Account Usage and Deletion policy

Purpose:

The Official Email Account Use Policy at Lords Institute of Engineering and Technology (A) (LIET) establishes guidelines for the proper use of institutional email accounts. This policy aims to ensure secure, professional, and efficient communication within the institution and with external parties.

Scope:

This policy applies to all users of LIET's official email accounts, including students, faculty, staff, and any authorized external partners.

Policy Guidelines:

1. Acceptable Use

- **Institutional Communication:** Official email accounts should be used primarily for LIET-related communications, including academic, administrative, and operational purposes. Personal use should be minimal and must not interfere with institutional activities.
- **Professional Conduct:** Emails should be written in a professional manner. Users must avoid inappropriate language, offensive content, and unprofessional behaviour in their communications.

2. Security and Privacy

- **Account Security:** Users are responsible for maintaining the security of their email accounts. This includes using strong passwords, enabling two-factor authentication if available, and not sharing login credentials.
- **Confidential Information:** Sensitive information must be handled with care. Users should avoid sharing confidential data via email unless it is encrypted and necessary for institutional purposes.

3. Compliance and Monitoring

- **Legal Compliance:** Email use must comply with all applicable laws and LIET policies, including those related to data protection and privacy.

- **Monitoring and Access:** LIET reserves the right to monitor email accounts to ensure compliance with this policy. Users should have no expectation of privacy for emails sent or received through official accounts.

4. Prohibited Activities

- **Spam and Phishing:** Sending unsolicited emails, spam, or engaging in phishing activities is strictly prohibited. Users must be vigilant against phishing attempts and report suspicious emails to the ICT Committee
- **Misuse of Email:** Users must not use official email accounts for unauthorized commercial activities, political campaigns, or personal gain.

5. Incident Reporting

- **Reporting Issues:** Any security breaches, suspicious activities, or violations of this policy must be reported immediately to the ICT Committee.
- **Support and Assistance:** The ICT Committee will provide support for email-related issues and ensure prompt resolution of reported incidents.

6. Retention and Archiving

- **Email Retention:** Official emails must be retained according to LIET's data retention policies. Users should archive important communications as required and avoid unnecessary deletion of institutional emails.

7. Provision of Official Email Accounts to Newly Joined Faculty and Students

Faculty:

a. Timing of Provision

- **Pre-Joining Preparation:** Official email accounts should be set up and ready for new faculty members within 2 days after official joining date. This ensures they can access necessary resources and communications promptly.
- **Immediate Access:** New faculty should receive their email account credentials during their orientation or on their first day of joining LIET.

2. Procedure

- **Account Creation:** The HR Department will notify the IT Department of new faculty hires, providing necessary details such as name, department, and joining date.
- **Credential Distribution:** The ICT Committee or System Admin will create the email accounts and provide login credentials securely to the new faculty members.
- **Orientation:** During the orientation session, new faculty will be briefed on the usage policies, security measures, and best practices for using their official email accounts.

Students:

1. Timing of Provision

- **Pre-Enrollment:** Official email accounts for new students should be created and distributed before the start of their academic session or need basis.

2. Procedure

- **Account Creation:** The Admissions Committee will provide the ICT Committee with the necessary details of newly admitted students, including names, courses, and enrolment status.
- **Credential Distribution:** The ICT Committee will create the email accounts and distribute login credentials securely through the Admissions Office or directly to students or need basis.
- **Orientation:** As part of the orientation, students will be informed about the email usage policies, security protocols, and guidelines for effective communication.

8. Deletion of Official Email Accounts for Departing Faculty and Students

Purpose:

This guideline establishes the procedures and timing for deleting official email accounts of departing faculty and students at Lords Institute of Engineering and Technology (LIET).

Scope:

This guideline applies to all faculty and students leaving LIET, whether due to graduation, resignation, retirement, or any other reason.

Faculty:

a. Timing of Deletion

- **Post-Departure Notice Period:** The email accounts of departing faculty members should be deactivated immediately upon their departure but retained in a suspended state for a specified notice period, typically 30 days. This period allows for the transition of responsibilities and retrieval of any important communications.
- **Final Deletion:** After the notice period, the email accounts should be permanently deleted.

b. Procedure

- **Notification:** The HR Department must notify the ICT Committee of the faculty member's departure date, providing details such as the reason for departure and any special considerations for account retention.
- **Account Suspension:** Upon departure, the ICT Committee will suspend the email account, preventing login access while retaining the account data.
- **Data Retrieval:** During the grace period, the departing faculty member or their department may request access to retrieve important emails or data. This access is typically granted in a controlled manner.
- **Final Deletion:** After the notice period, the ICT Committee will permanently delete the email account and all associated data, ensuring that any sensitive or confidential information is securely disposed of.

Students:

Timing of Deletion

- **Post-Graduation/Departure Grace Period:** The email accounts of graduating or departing students should be deactivated immediately after their departure but retained in a suspended state for a specified grace period, typically 15 days. This allows students time to transition to personal email accounts and save any important communications.
- **Final Deletion:** After the grace period, the email accounts should be permanently deleted.

Wi-Fi Use policy at Campus

Wi-Fi connectivity at Lords Institute of Engineering and Technology (LIET) is a valuable resource that enhances learning, research, and communication opportunities for students, faculty, and staff. To ensure efficient and responsible use of this resource, LIET has established the following Wi-Fi Use Policy.

Policy Statement:

1. **Access:**

   Wi-Fi access is provided to all registered students, faculty, and staff of LIET. Guests may access Wi-Fi through designated guest accounts, subject to approval and supervision by authorized personnel.

2. **Acceptable Use:**

a. Academic Purposes: Wi-Fi should primarily be used for educational and research-related activities, including accessing academic resources, collaborating on projects, and participating in online courses.

b. Responsible Usage: Users are expected to conduct themselves responsibly and ethically while using Wi-Fi, adhering to LIET's Code of Conduct and respecting the rights and privacy of others.

c. Bandwidth Management: Users should refrain from activities that excessively consume network bandwidth, such as streaming high-definition video, gaming, or downloading large files, especially during peak usage times.

d. Security: Users are responsible for maintaining the security of their devices connected to the Wi-Fi network, including implementing necessary antivirus software and avoiding the transmission of sensitive or confidential information over unsecured connections.

e. Prohibited Activities: Any activities that violate local, state, or federal laws, infringe upon intellectual property rights, or disrupt the functioning of the network are strictly prohibited.

3. **Compliance:**

a. Monitoring: LIET reserves the right to monitor Wi-Fi usage for compliance with this policy and to investigate any suspected violations.

b. Enforcement: Violations of this policy may result in disciplinary action, including temporary or permanent revocation of Wi-Fi access privileges, academic penalties, or legal consequences as appropriate.

4. Support:

a. Technical Support: LIET provides technical support for Wi-Fi connectivity issues through designated channels during specified hours.

b. Education: LIET offers educational resources and training to help users understand and comply with this policy, as well as to promote responsible digital citizenship.

5. Policy Review:

a. Periodic Review: This Wi-Fi Use Policy will be periodically reviewed and updated as necessary to reflect changes in technology, usage patterns, and regulatory requirements.

b. Notification: Any revisions to this policy will be communicated to the LIET community in a timely manner through official channels.

Digital Library Use Policy

The Digital Library at Lords Institute of Engineering and Technology (LIET) serves as a central repository of electronic resources to support research, learning, and academic endeavours. This policy outlines the guidelines and procedures governing the use of the Digital Library facilities and resources.

Policy Statement:

1. Access and Eligibility:

a. Access: The Digital Library resources are accessible to all registered students, faculty, and staff of LIET during designated operating hours.

b. Eligibility: Only individuals with valid LIET credentials are permitted to access and utilize the Digital Library resources.

2. Acceptable Use:

a. Academic Purposes: The Digital Library resources are intended for academic research, study, and educational purposes related to the curriculum and scholarly pursuits of LIET.

b. Responsible Usage: Users are expected to use the Digital Library resources responsibly, respecting copyright laws, licensing agreements, and intellectual property rights.

c. Authorized Access: Users should not share their login credentials or provide unauthorized access to Digital Library resources to individuals outside the LIET community.

d. Copyright Compliance: Users are responsible for adhering to copyright laws and licensing agreements when accessing and using digital materials from the Digital Library.

3. Resource Management:

b. Limitations: Users should adhere to any usage limitations or restrictions imposed on specific resources or materials by the Digital Library staff.

4. Conduct:

a. Respectful Behaviour: Users are expected to conduct themselves in a respectful and courteous manner while using the Digital Library facilities, refraining from disruptive behaviour that may disturb others.

b. Equipment Care: Users should handle Digital Library equipment and materials with care, reporting any damage or malfunctions to the library staff promptly.

c. Cleanliness: Users are responsible for maintaining cleanliness and orderliness in the Digital Library spaces, disposing of trash appropriately and leaving study areas tidy.

5. Compliance and Enforcement:

a. Monitoring: The Digital Library staff may monitor usage of resources and facilities to ensure compliance with this policy and investigate any suspected violations.

b. Enforcement: Violations of this policy may result in disciplinary action, including temporary or permanent loss of access privileges, academic penalties, or other appropriate consequences.

6. Policy Review:

a. Periodic Review: This Digital Library Policy will be periodically reviewed and updated as necessary to reflect changes in technology, usage patterns, and regulatory requirements.

b. Notification: Any revisions to this policy will be communicated to the LIET community in a timely manner through official channels.

CCTV Surveillance policy

CCTV surveillance at Lords Institute of Engineering and Technology (LIET) is implemented to enhance campus safety, security, and operational efficiency. This policy outlines the guidelines and procedures governing the use of CCTV cameras on campus.

Policy Statement:

1. Purpose:

a. Security: CCTV surveillance is primarily deployed to deter and detect criminal activity, safeguarding the campus community and property against theft, vandalism, and other security threats.

b. Safety: CCTV cameras is also be used to monitor areas prone to accidents or emergencies, facilitating timely response and intervention when necessary.

c. Operational Monitoring: CCTV surveillance is utilized for operational purposes, such as monitoring crowd flow, assessing facility usage, and ensuring compliance with campus policies and regulations.

2. Scope:

a. Coverage: CCTV cameras are strategically placed in public areas across the LIET campus, including entrances, corridors, parking lots, and common spaces.

b. Privacy: CCTV surveillance is conducted in accordance with applicable privacy laws and regulations, respecting the privacy rights of individuals within the campus environment.

3. Access and Use:

a. Authorized Personnel: Access to CCTV footage is restricted to authorized personnel, including security staff and designated administrators responsible for monitoring and managing the surveillance system.

b. Purpose-Limited Use: CCTV footage is accessed and used solely for the purposes outlined in this policy, with strict adherence to principles of necessity and proportionality.

c. Data Retention: CCTV footage will be retained for a limited period as necessary for security and investigative purposes, after which it will be securely deleted or overwritten in accordance with data protection guidelines.

4. Notification:

a. Signage: Signs indicating the presence of CCTV cameras are prominently displayed in areas under surveillance, alerting individuals to the use of video monitoring.

b. Privacy Notice: A privacy notice is provided to inform individuals about the collection, use, and retention of CCTV footage, as well as their rights regarding access to their personal data.

5. Compliance and Enforcement:

a. Compliance: LIET is committed to complying with all applicable laws and regulations governing CCTV surveillance, including data protection and privacy requirements.

b. Enforcement: Any violations of this policy, misuse of CCTV footage, or unauthorized access will be subject to disciplinary action and may result in legal consequences as appropriate.

6. Policy Review:

a. Periodic Review: This CCTV Surveillance Policy will be periodically reviewed and updated as necessary to reflect changes in technology, legal requirements, and best practices.

b. Stakeholder Input: Feedback from the LIET community, including students, faculty, and staff, will be solicited and considered during policy reviews to ensure alignment with campus needs and values.