LeMoyne-Owen COLLEGE

LEADERSHIP. OPPORTUNITY. CHANGE.

SUBJECT:	**Effective Date:**	**Policy Number:**
Acceptable Use Policy	September 2024	05-1-013
	Supersedes: Policy: Date:	**Page 1 Of 4**
	Responsible Authority: VP of IT & CIO	

I. Purpose and statement of operational policy underlying the procedure.

This Acceptable Use Policy defines the acceptable use of LeMoyne-Owen College's technology resources, including networks, systems, devices, and data. It ensures that IT resources are used responsibly, ethically, and in compliance with legal and institutional requirements

The purpose of this policy is to ensure responsible and secure use of LeMoyne-Owen College's IT resources. Users are expected to promote educational, research, administrative, and community service functions consistent with the college's mission. This policy provides guidelines for acceptable use, outlines prohibited activities, and establishes accountability and enforcement measures

II. Applicability/Scope

Users are expected to utilize LeMoyne-Owen College's IT resources in a manner that promotes educational, research, administrative, and community service functions in accordance with the college's mission. All users must adhere to the following acceptable use guidelines:

General Usage

- IT resources must be used for purposes directly related to education, research, administration, and other authorized activities of the college.

- Personal use of IT resources is permitted on a limited basis, provided it does not interfere with academic responsibilities, professional duties, or network performance. However, personal data may not be available upon separation.
- Users must respect the intellectual property rights of others, including complying with copyright, licensing, and software agreements.

Security and Privacy

- Users are responsible for maintaining the confidentiality of their account credentials (e.g., usernames, passwords) and must not share them with others.
- Users must not attempt to access IT resources or data for which they do not have explicit permission or authorization.
- Sensitive or confidential information, including student records, financial data, and personally identifiable information (PII), must be handled and transmitted securely using encryption where appropriate.

Internet and Email Usage

- The college provides internet and email services to support its mission. Use of these services must align with the college's policies and applicable laws.
- Prohibited activities include:
    - Sending, receiving, or accessing content that is illegal, defamatory, discriminatory, harassing, or otherwise harmful.
    - Using email or internet services for personal gain, commercial purposes, or political campaigns.
    - Engaging in activities that degrade or disrupt the college's IT resources, including sending unsolicited bulk email (spam), distributing malware, or engaging in denial-of-service attacks.

Software and Hardware Usage

- Users must not install or use unauthorized software or hardware on the college's IT resources.
- Only licensed software approved by the IT department may be installed on college-owned devices.
- Any modifications to hardware or software configurations must be approved by the IT department.

Cloud and Third-Party Services

- Use of cloud-based services or third-party applications to store or process college data must comply with the college's data protection and security policies. Only IT department-approved services may be used to handle sensitive or confidential information.
- Users must not use personal cloud accounts to store institutional data.

Prohibited Activities

The following activities are strictly prohibited:

- **Unauthorized Access or Hacking:** Attempting to gain unauthorized access to networks, systems, or accounts, including the use of hacking tools or social engineering tactics.

- **Distribution of Malware:** Introducing or distributing malicious software, such as viruses, worms, or ransomware, onto the college's IT resources.
- **Network Interference:** Engaging in activities that disrupt, degrade, or impede the performance of the college's networks or systems.
- **Harassment:** Using IT resources to harass, threaten, or abuse others, including the distribution of offensive, discriminatory, or defamatory content.
- **Piracy:** Using IT resources to engage in illegal activities, including downloading, sharing, or distributing copyrighted materials without proper authorization.

Monitoring and Privacy

LeMoyne-Owen College reserves the right to monitor the use of its IT resources to ensure compliance with this policy, protect the integrity of its systems, and investigate potential violations. The college may inspect, without prior notice, any data or communications transmitted via its networks or stored on its systems, subject to applicable laws.

- **Privacy Expectations:** While the college seeks to respect users' privacy, users should have no expectation of privacy when using college IT resources. All communications and data transmitted through or stored on the college's systems may be monitored or accessed.

Enforcement and Disciplinary Actions

Violations of this Acceptable Use Policy may result in disciplinary actions, including but not limited to:

- Suspension or termination of access to the college's IT resources.
- Disciplinary action up to and including termination of employment or expulsion from the college.
- Legal action or prosecution for violations of local, state, or federal laws.

Reporting Violations

Users who become aware of a violation of this policy are encouraged to report the issue to the IT department or their supervisor. Reports of potential violations will be investigated, and appropriate actions will be taken based on the findings.

Review and Updates

This policy will be reviewed annually by the IT department to ensure its relevance and alignment with current technologies, legal requirements, and institutional priorities. Any updates will be communicated to the college community.

III. Process for Implementing Procedure

Responsibility	Action	Timeline
IT Department	Maintain and update the Acceptable Use Policy annually	Annual review
All Users	Comply with acceptable use guidelines (general usage, security/privacy, internet/email, software, cloud/third-party)	Ongoing
Supervisors/IT Dept.	Investigate reported violations	As needed
Authorizing Official	Approve updates and communicate changes	Upon revisions

IV. Related policies/References for more information

- Data Management Policy
- Cybersecurity Awareness and Training Control Policy
- Artificial Intelligence (AI) Policy
- Student Records and Privacy Policy (FERPA compliance)
- Institutional Disciplinary Procedures

Authorizing Official: _____ Authorization Date: _____

Title: _ _____