# LeMoyne-Owen College Information Technology Acceptable Use Policy

## 1. Overview

In keeping with the spirit of free intellectual inquiry that is fundamental to our mission and the principles of academic freedom and individual privacy, LeMoyne-Owen College has outlined this policy for the use of information technology on and off campus.

Information Technology (IT) organization’s intentions for publishing an IS Security Policy are not to impose restrictions that are contrary to LeMoyne-Owen College’s established culture of openness, trust and integrity. IT is committed to protecting LeMoyne-Owen College's students, employees, partners and the college from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of LeMoyne-Owen College. These systems are to be used for academic and business purposes in serving the interests of the college, and of our students, faculty, and staff in the course of normal operations. Please review Student Handbook and/or Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every LeMoyne-Owen College student, employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2. Purpose

The purpose of this policy is to outline the acceptable use of electronic equipment at LeMoyne-Owen College. These rules are in place to protect the student, the employee and LeMoyne-Owen College. Inappropriate use exposes LeMoyne-Owen College to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct LeMoyne-Owen College business (i.e., classes and general operations) or interact with internal networks and business and academic systems, whether owned or leased by LeMoyne-Owen College, the student, the employee, or a third party connected by wire or wireless to the campus network, and to off-campus computers that connect remotely to the

College's network services.  All students, employees, contractors, consultants, temporary, and other workers at LeMoyne-Owen College are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with LeMoyne-Owen College policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

Individuals covered by the policy include LeMoyne-Owen College students, faculty, staff, alumni, or guests accessing LeMoyne-Owen College information technology resources or network services.

Information technology resources include all LeMoyne-Owen College owned, licensed, or managed hardware and software, and use of the College's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

## 4. Policy

### 4.1 General Use and Ownership

4.1.1 LeMoyne-Owen College proprietary information stored on electronic and computing devices whether owned or leased by LeMoyne-Owen College, the student, the employee or a third party, remains the sole property of LeMoyne-Owen College. You must ensure through legal or technical means that proprietary information is protected.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of LeMoyne-Owen College proprietary information.

4.1.3 You may access, use or share LeMoyne-Owen College proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties or academic requirements.

4.1.4 Employees and students are responsible for exercising good judgment regarding the reasonableness of personal use. Students and employees should be guided by LeMoyne-Owen College policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager and students should consult the IT department.

4.1.5 For security and network maintenance purposes, authorized individuals within LeMoyne-Owen College may monitor equipment, systems and network traffic at any time.

4.1.6 LeMoyne-Owen College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.1.7 You may use only the computers, computer accounts, and computer files for which you have authorization.

4.1.8 You may not use another individual's account, or attempt to capture or guess other users' passwords.

4.1.9 You are individually responsible for appropriate use of all resources assigned to you, including any computer, network address or port, software, or hardware. As an authorized user of LeMoyne-Owen College technology resources, you may not enable unauthorized users to access the network by using a LeMoyne-Owen computer or a personal computer that is connected to the LeMoyne-Owen College network.

4.1.10 The College is bound by its contractual and license agreements of certain third party resources and software; you are expected to comply with all such agreements when using such resources.

4.1.11 You should make a reasonable effort to protect your passwords and to secure resources against unauthorized use or access.

4.1.12 You must not attempt to access restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system administrator.

4.1.13 You must not use LeMoyne-Owen College technology and/or network resources in conjunction with the execution of programs, software, processes, or automated transaction-based commands that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users, or damage or degrade performance, software or hardware components of a system.

4.1.14 You must not use tools that are used to attack computer systems or networks.

**4.2 Security and Proprietary Information**

4.2.1 All computing devices that connect to the internal network must comply with the *Acceptable Use Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by students and employees from a LeMoyne-Owen College email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of LeMoyne-Owen College, unless posting is in the course of business duties.

4.2.5 Students and employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a student or an employee of LeMoyne-Owen College authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing LeMoyne-Owen College-owned or leased resources.

Technology users should observe the same standards of ethical conduct and courteous behavior that govern non-electronic vocal and written communications and other personal interactions whenever LeMoyne-Owen College's Information Technology resources are used. Ethical and courteous use of information technology resources is the responsibility of every student and employee. This principle is fundamental to the spirit of community and standards of consideration that should govern interactions among all members of the College community. Examples of activities that may violate this principle include, but are not limited to, the following:

- Repeated, unsolicited, or unwanted electronic communication with an individual after the sender has been asked to stop;

- Misrepresentation of the identity of the sender of an electronic communication or website host;

- Obscuring or forging of the date, time, physical source, logical source, or other header information of a message or transaction;

- Alteration of the content of a message originating from another person or computer with the intent to deceive;

- Acquiring or attempting to acquire passwords of other users;

- The unauthorized deletion of another user's postings, files, etc.

- Slanderous and/or denigrating postings regarding a member of the College community;

- Viewing pornography or incendiary sites using campus technology or any activity that violates state or federal laws, regulations or College policies.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

### 4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by LeMoyne-Owen College.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LeMoyne-Owen College or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting LeMoyne-Owen College business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a LeMoyne-Owen College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any LeMoyne-Owen College account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the LeMoyne-Owen College network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, LeMoyne-Owen College employees to parties outside LeMoyne-Owen College.

### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within LeMoyne-Owen College's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by LeMoyne-Owen College or connected via LeMoyne-Owen College's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### 4.3.3 Blogging and Social Media

1. Blogging by employees, whether using LeMoyne-Owen College's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of LeMoyne-Owen College's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate LeMoyne-Owen College's policy, is not detrimental to LeMoyne-Owen College's best interests, and does not interfere with an employee's regular work duties. Blogging from LeMoyne-Owen College's systems is also subject to monitoring.

2. LeMoyne-Owen College's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any LeMoyne-Owen College confidential or proprietary information, trade secrets or any other material covered by LeMoyne-Owen College's Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of LeMoyne-Owen College and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by LeMoyne-Owen College's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to LeMoyne-Owen College when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of LeMoyne-Owen College. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, LeMoyne-Owen College's trademarks, logos and any other LeMoyne-Owen College intellectual property may also not be used in connection with any blogging activity

## 5. Security, and Enforcement

LeMoyne-Owen College reserves the right to employ security measures. When the College becomes aware of violations, either through routine system administration activities, or from a complaint or report, it is the College's responsibility to investigate as needed or directed, and to take necessary actions to protect its resources and/or to provide information relevant to an investigation.

## 6. Policy Compliance

6.1 Compliance Measurement

The IT department will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by the IT, HR, or Student Judiciary organizations in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and legal action.

## 7. Related Standards, Policies and Processes

- Data Classification Policy
- Acceptable Use Policy
- Social Media Policy
- Password Policy

## 8. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

## 9. Revision History

| Date of Change | Responsible | Summary of Change |
|---|---|---|
| 9/1/2016 | IT, HR, Student Affairs | Updated and converted to new format |