LE MOYNE

Greatness meets Goodness

POLICY: ACCEPTABLE USE

DOCUMENT #:	POL-0002
EFFECTIVE:	01-JAN-2017
OWNER:	ISO

CONTENTS

LE MOYNE
Greatness meets Goodness

1.0 PURPOSE

Le Moyne College's (LMC) technology infrastructure exists to support the educational, instructional, research and administrative activities needed to fulfill the Institution's academic mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish that each member of the College community has a role in protecting LMC's information assets, and to communicate minimum expectations and requirements. Fulfilling these objectives will enable LMC to implement a comprehensive, system-wide Information Security Program.

2.0 SCOPE

This Policy applies to all users of computing resources owned, managed or otherwise provided by the College. Individuals covered by this Policy include, but are not limited to faculty, staff, administrators, students and service providers with access to the College's computing resources and/or facilities. Computing resources include all LMC owned, licensed, contracted or managed hardware and software, email domains and related services and any use of LMC's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network

3.0 PRIVACY

Users do not acquire a right of privacy for data or communications transmitted or stored on Campus resources. In addition, in response to a judicial order or any other action required by law or permitted by official LMC policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the College and/or the College community, the President or a Senior Vice President may authorize an LMC official or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or LMC rules, regulations or policy, or when access is considered necessary to conduct LMC business due to the unexpected absence of an employee or to respond to health or safety emergencies.

4.0 POLICY

Activities related to the Institution's academic mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the academic mission is prohibited.

Following the same standards of common sense, courtesy and civility that govern the use of other shared College facilities, acceptable use of information technology resources generally respects all individuals' privacy, but subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Le Moyne College computing resources must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

The Institution explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any Campus information systems, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

- Violate the rights of any individual or company involving information 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 the College.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the Institution does not have a legal license.
- Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her manager immediately.

If a user creates any liability on behalf of LMC due to inappropriate use of institutional resources, the user agrees to indemnify and hold the Institution harmless, should it be necessary for the Institution to defend itself against the activities or actions of the user.

4.2 CONFIDENTIAL INFORMATION

LMC has both an ethical and legal responsibility for protecting confidential information in accordance with its Data Classification Policy. To that end, there are some general positions that the Institution has taken:

- Transmission of protected information by end-user messaging technologies (i.e. e-mail, instant messaging, SMS, chat, etc.) is prohibited, unless secured by a method approved by the Information Security Committee. In certain circumstances, transmission of protected information may be prohibited to comply with with regulatory requirements (i.e. PCI-DSS).
- The writing or storage of confidential information on mobile devices (phones, tablets, USB drives) and removable media is prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimize the risk of unauthorized access.
- All workforce members and service providers will use approved workstations or devices to access Institution data, systems, or networks. Non-Institution owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing confidential information on home or other personal computing devices is prohibited.
- All Institution portable workstations will be securely maintained when in the possession of workforce members. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in areas containing protected information.
- All confidential information stored on workstations and mobile devices must be encrypted.

4.3 HARRASSMENT

LMC is committed to providing a safe and productive environment, free from harassment, for all employees. For this reason, users must not:

- Use Campus information systems to harass any other person via e-mail, telephone, or any other means, or
- Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels he/she is being harassed through the use of Campus information systems, the user shall report it as prescribed by student, employee, or faculty handbook or related policy.

4.4 MALICIOUS ACTIVITY

The Institution strictly prohibits the use of information systems for malicious activity against other users, LMC information systems themselves, or the information assets of other parties.

4.4.1 DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way disrupt LMC's information systems or network communications by denial-of-service methods;
- Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system; or
- Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

4.4.2 CONFIDENTIALITY

Users must not:

- Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a device, service or account that the user is not expressly authorized to access;
- Facilitate use or access by non-authorized users, including sharing a password or other login credentials with anyone, including other users, family members, or friends;
- Use the same password for accessing institutional and non-institutional computing resources (i.e. personal email, social media);
- Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password; or
- Make copies of another user's files without that user's knowledge and consent.

All encryption keys employed by users must be provided to Information Technology if requested, in order to perform functions required by this Policy.

4.4.3 IMPERSONATION

Users must not:

- Circumvent the user authentication or security of any information system;

- Add, remove, or modify any identifying network header information (“spoofing”) or attempt to impersonate any person by using forged headers or other identifying information;
- Create and/or use a proxy server of any kind, other than those provided by LMC, or otherwise redirect network traffic outside of normal routing with authorization; or
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

4.4.4 NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either LMC’s network or any other external network, unless this activity is a part of the user’s normal job functions, such as a member of the Office of Information Technology, conducting a vulnerability scan, and faculty or student, when explicitly authorized, utilizing tools in a controlled environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the user’s, unless this activity is a part of the user’s normal job functions

4.5 OBJECTIONABLE CONTENT

Unless authorized for instruction or research purposes, LMC strictly prohibits the use of institutional information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Political
- Racist
- Sexually-explicit
- Violent or promoting violence

4.6 HARDWARE AND SOFTWARE

The College strictly prohibits the use of any hardware or software that is not purchased, installed, configured, tracked, and managed by authorized College personnel. Users must not:

- Install, attach, or connect, or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institutional information system without the knowledge and permission of Information Technology;
- Download or install, or disable, remove, or uninstall, software of any kind, including patches of existing software, to any institutional information system without the knowledge and permission of the Information Technology; or

- Take LMC equipment off-site without prior authorization.

4.7 MESSAGING

The Institution provides a robust communication platform for users to fulfill its academic mission. Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism;
- Send unsolicited electronic messages, including “junk mail” or other advertising material to individuals who did not specifically request such material (spam);
- Falsify (“spoof”) the source or solicit electronic messages as any other individual’s digital identify (e.g. e-mail address, social handle), with the intent to disrupt, harass or to collect replies; or
- Create or forward chain letters or messages, including those that promote “pyramid” schemes of any type.

4.8 LIBRARY FILE AND PUBLIC ACCESS COMPUTERS

The library records for patrons of the LMC Libraries are protected by New York State Law, and are consistent with practices of the Code of Ethics of the American Library Association.

4.9 OTHER

In addition to the other parts of this policy, users must not:

- Use the Institution’s information systems for commercial use or personal gain.

5.0 ROLES AND RESPONSIBILITIES

LMC reserves the right to protect, repair, and maintain Campus computing equipment and network integrity. In accomplishing this goal, LMC IT personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by IT personnel about a user through routine maintenance of Campus computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of LMC’s computing resources.

6.0 ENFORCEMENT

Enforcement is the responsibility of the Information Security Committee. Users who violate this Policy may be denied access to the Institution's resources and may be subject to penalties and disciplinary action both within and outside of the Institution. The Institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Institution or other computing resources or to protect the Institution from liability.

Users are subject to disciplinary rules described in the Student Handbook, Employee Handbook, Faculty Handbook and other policies and procedures governing acceptable employee and student behavior.

7.0 EXCEPTIONS

Exceptions to the policy may be granted by the Director for Information Technology, or his or her designee. All exceptions must be reviewed annually.

7.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act
- NIST 800-53
- FIPS-199
- PCI DSS 3.1
- New York Civil Practice Law and Rules § 4509
- Code of Ethics of the American Library Association

8.0 RELATED POLICIES

- Le Moyne College Information Security Policy
- Le Moyne College Data Classification Policy, Procedure and Quick Reference Guide

9.0 RESPONSIBLE DEPARTMENT

Information & Technology Services (a.k.a. Information Technology)

10.0 POLICY AUTHORITY

This policy is issued by the Information Security Committee for Le Moyne College.

11.0 REVISION HISTORY

Version	Date	Author	Revisions
1.00	04-21-16	GreyCastle Security	Initial Draft
1.01	05-11-16	GreyCastle Security	Policy Updates
1.02	06-24-16	GreyCastle Security	Final Draft
1.03	01-01-2017	Le Moyne College	

12.0 APPROVALS

Executive	Information Security Officer
Name	Name
Title	Title
Date	Date
Signature	Signature