Policy Name:	Acceptable Use of Computer and Network Resources		
Associated Form(s):	Employee Affirmation Form	**Policy Number**:	2022-7
Reviewed:	Non-Academic Policy Review Committee	**Approved:**	May 13, 2022
Approval Authority:	President Timothy L. Hall	**Adopted:**	June 10, 2022
Responsible Executive(s):	Vice President for Operations and Facilities	**Revised:**	Acceptable Use Policy (November 2017)
Responsible Office(s):	Office of Information Technology	**Contact(s):**	Chief Information Officer Director Technical Services

CONTENTS

1.0 PURPOSE

Mercy College's computer and network resources are an important component to further the College's educational purposes and college business in support of Mercy's mission, which seeks to transform students' lives through higher education. Users of these resources have a responsibility to follow the guidelines set forth in this document, as well as all other related policies and procedures, not to abuse the privileges granted to them, and to respect the rights of others.

Mercy's technology infrastructure exists to support the College and administrative activities needed to fulfill the College's 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 each member of the College's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable Mercy 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 all employees and service providers with access to the College's computing resources and/or facilities. All Mercy College community members, including: students, staff, faculty, alumni, contractors, third party vendors and former full-time faculty who served at Mercy College for 10 years or more, are provided with a Mercy College identification card ("ID") and number, which grants certain accesses to College computer and network resources, depending on the community member and the particular need.

Computing resources include all Mercy owned, licensed or managed hardware and software, email domains and related Applications & Services (on-prem and Cloud Applications) and any use of the College's network via a physical, wireless connection or remote access, regardless of the ownership of the computer or device connected to the network (on-prem and Cloud).

This Policy applies to all members of the College community and covers both internal and external (on-prem and Cloud) use of computer and network resources, College computer and information technology hardware, software, data, access and other resources owned, operated, or contracted by Mercy.

3.0 PRIVACY AND ELECTRONIC MONITORING

Mercy will make every reasonable effort to respect a user's privacy. However, community members, including employees and students, do not have a right of privacy for communications transmitted or stored on the Mercy's resources. In addition, while the College does not routinely monitor or access its mail systems, to the extent permitted by law, the College reserves the right to access and disclose, and monitor when necessary, the contents of electronic communications made with or through the College's resources without the consent of the user. Further, any and all telephone conversations or transmissions, electronic mail or transmissions (as discussed above), or internet access or usage by a user by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems ("User Activity"), may be subject to monitoring at any and all times and by any lawful means.

Devices connected to the College's network or technology systems, or used pursuant to this Policy, may be monitored or intercepted to the extent such device is used for any User Activity. Such devices include the College provided devices and other devices (including personal devices) using the College's internet, servers, and networks. The College may do so for reasons including but not limited to:

- Investigating potential misconduct,
- Protecting health and safety,
- Protecting College resources,
- Preserving emails or other documents in connection with a litigation and/or pursuant to the College's Records Retention Policy
- Locating information required for College business,
- Handling matters when employees are out on extended leaves of absence,
- Responding to subpoenas and other legal obligations, and/or
- Fulfilling the College's obligations to third parties.

In addition, maintenance of the College's computing networks and systems may result in the contents of files and communications being seen by network, system, or other administrators.

Although users of the College's electronic communications resources have no right to privacy vis-à-vis the College, they must respect the legitimate privacy expectations of other users.

4.0 POLICY

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

Following the same standards of common sense, courtesy and civility that govern the use of other shared 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 Mercy's computing resources must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

Mercy explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the College's 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 Mercy.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music & videos, and any copyrighted software (utilizing any kind of Peer-to-Peer P2P software) for which the College 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 any user creates any liability on behalf of Mercy due to inappropriate use of the College's resources, the user agrees to indemnify and hold the College harmless, should it be necessary for Mercy to defend itself against the activities or actions of the user.

4.2 CONFIDENTIAL INFORMATION

Mercy has both an ethical and legal responsibility for protecting confidential information in accordance with its Confidential Information Policy. To that end, there are some general positions that the College has taken:

- Transmission of confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is prohibited.
- 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 employees and service providers will use approved workstations or devices to access College's data, systems, or networks. Non-college owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing confidential information on home computers is prohibited.
- All company portable workstations will be securely maintained when in the possession of employees. 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 secure areas.
- All confidential information stored on workstations and mobile devices must be encrypted & secured.
- All employees who use College-owned workstations will take all reasonable precautions to protect the confidentiality, integrity and availability of information contained on the workstation.
- College employees and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft and unauthorized use.
- College employees will activate their workstation locking software whenever they leave their workstation unattended or will log off from or lock their workstation when their shift is complete.

4.3 HARASSMENT

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

- Use College 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 the College's information systems, the user must report it, in writing, to his/her supervisor or any department head.

4.4 INCIDENT REPORTING

Mercy is committed to responding to security incidents involving personnel, College-owned information or College-owned information assets. As part of this Policy:

- The loss, theft or inappropriate use of College access credentials (e.g. passwords, key cards or security tokens), assets (e.g. laptop, cell phones), or other information must be reported to the IT Service Desk at helpdesk@mercy.edu.
- An College employees will not prevent another member from reporting a security incident.

4.5 MALICIOUS ACTIVITY

Mercy strictly prohibits the use of information systems for malicious activity against other users, the College's information systems themselves, or the information assets of other parties.

4.5.1 DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way enable disruption of Mercy'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.

4.5.2 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 server or account that the user is not expressly authorized to access;
- Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;
- Use the same password for Mercy accounts as for other non-Mercy access (for example, personal ISP account, social media, benefits, email, etc.);
- 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.
- Base passwords on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports teams, etc.).

4.5.3 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 Mercy, 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.

4.5.4 NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either Mercy 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 utilizing tools in a controller 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.
- Attach non-Mercy Network devices to the college network. Network snooping, capturing traffic or any sort of brute force network attempts. Including network switches, wireless routers and any other type of non-Mercy owned network or systems devices.

4.6 OBJECTIONABLE CONTENT

Mercy strictly prohibits the use of Collegeal 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

4.7 HARDWARE AND SOFTWARE

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

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any Collegeal information system without the knowledge and permission of Information Technology;
- Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any Collegeal information system without the knowledge and permission of the College;
- Use personal flash drives, or other USB based storage media, without prior approval from their manager; or
- Take Mercy equipment off-site without prior authorization.

4.8 MESSAGING

The College provides a robust communication platform for users to fulfill its 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);
- Solicit electronic messages for any other digital identifier (e.g. e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies; or
- Create or forward chain letters or messages, including those that promote "pyramid" schemes of any type.

4.9 REMOTE WORKING

When working remote, user must:

- Be given explicit approval from Manager pursuant to the College's Remote Work Policy.
- Safeguard and protect any College-owned or managed computing asset (e.g. laptops and cell phones) to prevent loss or theft.
- Not utilize personally-owned computing devices for Mercy work, including transferring Mercy information to personally-owned devices, unless approved by Manager.

- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Mercy's information processed, stored or transmitted on College-owned assets.
- Not create or store confidential or private information on local machines unless a current backup copy is available elsewhere.
- Not access or process confidential information in public places or over public, insecure networks.
- Only use Mercy approved methods for connecting to the College (e.g. VPN).

4.10 OTHER

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

- Stream video, music, or other multimedia content unless this content is required to perform the user's normal business functions;
- Use the College's information systems for commercial use or personal gain; or
- Use the College's information systems to play games or provide similar entertainment.

5.0 PROVISION OF MOBILE DEVICES OR USE OF PERSONAL MOBILE DEVICES

In order to meet the operational needs of the College, certain employees are issued a mobile device. Devices may be requested by emailing helpdesk@mercy.edu and providing a valid business reason. Based on department needs, you may be required to carry the device and respond outside of normal business hours. Alternatively, some employees may use their personal devices for College-related business. All devices (whether it be College-issued or personal devices used for College-business) will be configured with the current Mercy security standards set by the IT Department, which may include passcodes, encryption, biometrics, or other methods. International calling, purchasing and downloading apps, and frequent texting is not permitted unless required as part of your job.

6.0 ROLES AND RESPONSIBILITIES

Mercy reserves the right to protect, repair, and maintain the College's computing equipment and network integrity. In accomplishing this goal, Mercy 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 the College's computing equipment or network should remain confidential, unless the information pertains to activities that are not compliant with acceptable use of Mercy's computing resources.

7.0 ENFORCEMENT

Enforcement is the responsibility of the College's President or designee. Users who violate this Policy may be denied access to the Colleges resources and may be subject to penalties and disciplinary action both within and outside of Mercy. The College 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 the College or other computing resources or to protect Mercy from liability.

Users are subject to disciplinary rules described in the Employee Handbook, Student Handbook, Faculty Handbook, Collective Bargaining Agreement, and/or other policies and procedures governing acceptable behavior at the College.

All members of the College community have an obligation to use the College's computer and network resources consistent with this Policy.

Violation of this policy may subject members of the College community to the following sanctions:

- Criminal prosecution, in the event of a violation of any Federal, State or local law, or regulation;
- Loss of access to the College's computer and network resources, such as the Internet or email system;
- Seizure of College-owned equipment, such as computers, tablets, and cell phones;
- Personal devices connected to the College Network (non-Mercy owned assets like personal network devices/routers); causing harm to any College Systems & Services will be investigated and responded to in accordance with Mercy's Incident Response procedures.
- Required reimbursement of any costs, losses, damages or expenses incurred by the College or by others; and
- Disciplinary sanctions up to and including suspension or dismissal for employees, and suspension or expulsion for students.

8.0 EXCEPTIONS

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

9.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act

- Illinois Personal Information Protection Act (815 ILCS 530/)
- California Consumer Privacy Act (CCPA)
- NIST 800-171
- FIPS-199
- PCI DSS 3.1
- New York Civil Practice Law and Rules § 4509
- Code of Ethics of the American Library Association

EMPLOYEE AFFIRMATION FORM

Mercy College Policy on Acceptable Use of Computer and Network Resources

My signature below confirms that I have read the Policy on Acceptable Use of Computer and Network Resources. I further affirm that I understand the application of the Policy and will discuss with Human Resources and my supervisor any concerns or potential concerns as it relates to my work with the College and parties outside of the College.

Employee Name: _____

PLEASE PRINT

_____ **Date: _____/ _____/ ____**

Employee Signature

_____ **Date: _____/ _____/ ___**

Human Resources Representative