Policy Name:	Acceptable Use of Computer and Network Resources		
Associated Form(s):	Employee Affirmation Form	**Policy Number:**	2017-4
Reviewed:	Non-Academic Policy Advisory Review Council	**Approved:**	September 26, 2017
Approval Authority:	President Tim Hall	**Adopted:**	11/22/17
Responsible Executive(s):	Vice President for Operations and Facilities	**Revised:**	1) Mercy College Standards for Acceptable Use of College Computing and Network Resources (10/5/16) 2) Electronic Communications Policy (2007) 3) Email Access/Management of Systems Accounts (2005) 4) Communication Devices (2009)
Responsible Office(s):	Office of Information Technology	**Contact(s):**	Director of Information Technology

I. Policy Statement

Mercy College offers a diverse academic program, which prepares its students to become productive citizens. Mercy College's computer and network resources are used 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.

II. Applicability

This policy applies to all members of the College community and covers both internal and external use of computer and network resources, college computer and information technology hardware, software, data, access and other resources owned, operated, or contracted by Mercy, including but not limited to the following:

- Electronic mail (email)
- Voice mail, including the use of the Internet to transmit external e-mail
- Desktop and laptop computers
- Handheld devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets)
- Mainframes
- Minicomputers
- Servers
- Network facilities
- Databases
- Memory
- Memory sticks, and
- Associated peripherals and software, and the applications they support in addition to e-mail, such as cloud computing applications, and access to the internet.

III. Policy

A. General Use and Access

All Mercy College community members, including: students, staff, faculty 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.

Users granted an individual logon and password are responsible for all activity occurring under their ID and password. Users with passwords should not share them and are expected to change them regularly to maintain security. Passwords are used to maintain security, not to guarantee

privacy. The computers and computer accounts given to users are to assist them in the performance of their jobs.

The College will make reasonable efforts to maintain the integrity and effective operation of its computer system and network, but those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Users should not have an expectation of privacy in anything they create, store, send or received on the College computer system or network, even when using private e-mail account, such as Yahoo, AOL or G-Mail account.

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 prior notification and without the consent of the user. 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,
- 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.

B. Prohibited Uses

With the privileges of use comes responsibility. Users are expected to utilize our resources in an ethical and responsible manner, in congruence with a productive educational and work environment. The following uses of College computing and network resources are prohibited:

- Actions considered illegal under local, state and/or federal law
- Conducting private business, for profit or commercial purposes.

- Engaging in plagiarism, copyright infringement, sharing trade secrets, peer-to-peer file sharing, or violations of any and all other related laws and regulations.
- Copying licensed software off of, or on to, a College computer or network without authorization
- Behavior considered sexual harassment, threatening, harassing, bullying, stalking/cyber-stalking, or discriminatory, including but not limited to acts considered violations of Mercy's Equal Opportunity and Non-Discrimination Policy and Sexual Misconduct Policy.
- Making defamatory statements
- Tampering or damaging any equipment
- Disseminating malware
- Facilitating theft
- Facilitating identity theft or any other fraud, including but not limited to forging official documents or business records
- Impersonating another person for any reason
- Viewing, disseminating, or storing any pornographic or indecent images
- Allowing someone else to use your account, or using the account of another community member, for any purpose
- Hacking (or attempts to do so) of another system, database, user, etc.
- Bypassing or disabling (or attempts to do so) of the computer and/or network security, including but not limited to passwords, security software, and physical security devices, such as locks, cables and keypads.

The College has the right to immediately suspend or terminate any user's access to the College's computer and network resources and to take any other appropriate action in the event of a prohibited use.

C. Limitation of Use in Certain Circumstances

1. Reasonable use by employees

Reasonable use of the College's systems including but not limited to Internet, email, cell phones, tablets and other devices by faculty and staff for personal purposes such as communicating with a family member or friend, is permitted so long as such use does not interfere with the user's employment duties to the College, does not abuse the College's systems or pose a financial or other burden on the College, is legal and in good taste, and does not otherwise violate the terms or spirit of this Policy.

2. Unfair monopolization of resources

No community member shall perform acts that unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, playing video and other online games, chatting, and printing large quantities of documents or photos.

3. Use of campus-wide email

Because email communications tend to be more immediate and more informal than written communication, offices, departments and schools, as well as individuals should be cautious in sending group e-mails targeted to all faculty, staff and/or students. It is particularly important to avoid offensive, harassing, intimidating, threatening or defamatory statements in group e-mails. Group e-mails (or "reply to all" responses) addressed to all faculty, staff and/or students are only permitted when the subject matter of the message is sufficiently important to the targeted group that the message could appropriately be sent as formal memorandum, but because of some urgency the immediacy of an e-mail is required. Inappropriate group emails would include, but not be limited to, emails regarding personal matters, advertisements, political matters or messages with bulky attachments. Please refer to the College's marketing webpage regarding appropriate forms of messaging.

4. Provision of 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. All devices 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.

IV. Procedures for Violations of this Policy

All members of the College community have an obligation to use the College's computer and network resources consistent with this Policy. Training in appropriate use of any College technology resource is available through the Help Desk and is especially recommended for new users.

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;
- Required reimbursement of any costs, losses, damages or expenses incurred by the College or by others; and
- Disciplinary sanctions up to and including dismissal. Staff who violate this Policy are subject to discipline in accordance with the Employee Handbook, the Collective Bargaining Agreement, and any other disciplinary rules that the College may adopt. Faculty who violate this Policy are subject to discipline in accordance with the

Faculty Handbook, except in the case of adjunct faculty, who are subject to discipline in accordance with the adjunct faculty member's contract. Students who violate this Policy are subject to discipline in accordance with the Student Handbook and any other disciplinary rules or policy that the College may adopt.

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/ Management Representative