MercyCollege of Ohio

2221 Madison Avenue
Toledo, OH 43604
mercycollege.edu
888.80.MERCY

SUPERSEDES: 09/08/2015	**SECTION:** Academic and Student Affairs
POLICY AND PROCEDURE MANUAL MERCY COLLEGE OF OHIO, TOLEDO, OHIO Signature on file Signature: Dr. Susan Wajert, President	**CODE NO.** 515
	SUBJECT: Information Technology Student Acceptable Use
	DATE ORIGINATED: 09/08/2015
	DATE BOARD COMMITTEE APPROVED: N/A
	DATE BOARD APPROVED: 09/12/2023
	DATE OF NEXT REVIEW: 2026 April 1-30

Information Technology Student Acceptable Use Policy

PURPOSE:

To outline the use of Mercy College of Ohio's ("the College") computer resources accessed by students for educational and research purposes. The intention is to keep restrictions on individual use to a minimum. It is essential that users observe reasonable standards of behavior regarding the use of the computing facilities and services. The College reserves the right to access all information on the College's computers, equipment, and network without prior notice.

POLICY:

I. Students who are, as part of their study and/or work (paid, volunteer, or contract), required to or involved with use of the College's computers ("users") must agree to abide by the standards of this policy to use these resources, which prohibits the following:
   - A. Any attempt to modify or damage computer equipment;
   - B. Tampering of computer and/or network resources or engaging in any activity to interfere with normal operations of computers, network, and facilities;
   - C. Improper use of computer equipment including, but not limited to:
     1. Connecting personal or unapproved equipment to any college-owned computer or to the network;
     2. Installing personal software, including non-academic games, on college-owned computer;
     3. Installing college software on equipment that is personally owned;
     4. Recreational game playing;
     5. Knowingly using any system to produce system failure or degrade performance (e.g., creating or propagating viruses, overloading network with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass posting of any types).
   - D. Using an ID belonging to another individual or sharing user IDs and passwords with other users or any other person;
   - E. Making unauthorized copies of licensed software and illegally using copyrighted software and materials;
   - F. Using computer resources for private purposes including for-profit endeavors or illegal purposes and in a manner inconsistent with the College's license agreements;
   - G. Unauthorized reading, use of, or deletion of private files or email belonging to another user. This includes accessing or intentionally destroying college software;
   - H. Engaging in the unauthorized duplication, alteration or destruction of data, programs, or

software;

I. Communicating any credit card number or other financial account number, or any social security number with/without the permission of the owner;
J. Circumventing or subverting any system or network security measures;
K. Posting of obscene materials; this activity is unlawful and users are specifically cautioned against linking to sites that contain such materials, even if the site has other useful content;
L. Engaging in activity that is illegal under any local, state, federal, or international law;
M. Use of College email should adhere to the same standards of conduct as any other form of mail. The use of distasteful, inflammatory, harassing, or otherwise unacceptable comments is prohibited. The College may engage in monitoring of email messages or other electronic files created by students, faculty, and staff. Users are asked to delete unnecessary emails on a regular basis.

II. Students that are as part of their study and/or work, (paid, volunteer, or contract), required to or involved with use of the College's computers will attest to their understanding of this policy at orientation.

III. Each user is responsible for any misuse of the Information System perpetrated using the user's account or network access. Therefore, the user must take steps to ensure that others do not gain unauthorized access to Information Systems through the user's account. Users are responsible for constructing and using strong passwords. It is never appropriate to print, store online, or give personal passwords to others. Should tech support require the sharing of an individual's password, it is the user's responsibility to ensure the password is changed upon completion of support services. This requirement also includes the sharing of passwords with supervisors and managers.

IV. Users are responsible for taking reasonable precautions to ensure that they do not introduce viruses into the network.

A. Users must scan files and downloads for viruses and other destructive programs before storing or installing them on a workstation or other computer system. This includes laptops and home machines that access the network remotely. Users are required to protect any personal computer that connects to the network with an anti-virus software package. The anti-virus software operated on College-supplied workstations is configured for automatic updates to the software and virus definitions on a weekly basis, e-mail scanning, automated disk scanning, and on access scanning where possible. Interruption or overriding any of these settings is strictly prohibited without prior authorization from Information System management or staff.
B. Users should never open attachments or follow links provided in email messages from senders that are not recognized. Extreme caution should be used when opening attachments or following links that originate from outside the College, even from known senders. Links and attachments can be used to perform various malicious functions on workstations (e.g., install viruses, key loggers, remote access software, etc.).

C. Any suspicious email should be reported immediately via the "Report Phishing" option (or current reporting protocol) in webmail. Users should immediately contact the Bon Secours Mercy Health Service Desk at 1-833-691-4357 if they accidentally click on a link that is suspected as being malicious or if the user provided login credentials to an unknown source.

V. There is no expectation of privacy in the Mercy College e-mail system, computer equipment, network, or other informational technology resources. The following actions are specifically NOT allowed on the Mercy College e-mail system:

- Knowingly sending or forwarding any type of malicious code such as Viruses, Worms, Trojan Horses, etc.

- Sending numerous copies of the same or substantially similar messages or sending very large messages or files to a recipient with the intent to disrupt a server or account. The propagation of chain letters is similarly prohibited, whether the recipient wishes to receive such mailings. The College is not responsible for the forwarding of e-mail sent to any account that has been suspended or terminated. Such e-mail will be returned to sender, ignored, or deleted.

REFERENCING FORMS:

Form 515-A Information Technology Student Acceptable Use Attestation

---

Board Approved: 09/12/2023
Revised: September 2023 *(Revised policy to add best practices for security and suspicious items)*
Board Approved: 06/12/2018
Board Committee Approved: 05/22/2018
Revised: February 2018 (*Revised policy to focus on student users, updated referencing forms)*
New Policy Full Board Approved: 09/08/2015
New Policy Board Committee Approved: 08/25/2015

Information Technology Student Acceptable Use Attestation

Form 515-A

I agree to abide by Mercy College of Ohio's Information Technology Student Acceptable Use policy. In doing so, I agree to observe reasonable standards of behavior regarding the use of the computing facilities and services provided at, and by, the College. I understand that the College reserves the right to access all information on the College's computers, equipment, and network without prior notice.

In agreeing to abide by the Information Technology Student Acceptable Use policy, I understand that failure to adhere to the guidelines set forth in this policy can result in disciplinary action up to and including dismissal from the College.

_____	_____
Student Name (please print)	Student ID#
_____	_____
Student Signature	Date

Office: Student Affairs
Date: 11/30/18

2221 Madison Avenue, Toledo, Ohio 43604 1.888.80.MERCY mercycollege.edu