Technology Resources Acceptable Use
TEC 2.0

Office of Information Technology

Policy Type: Administrative
Applies to: Faculty, staff, student employees, students, and volunteers

POLICY DATES

Issued: 6/01/1995
Revised:
Edited: 5/23/2018
Reviewed:

It is the policy of the Office of Information Technology of the University of Mount Union that the technological resources are intended to be used primarily for educational purposes, communications and to carry out the legitimate business of the University. Appropriate use of the resources includes instruction, independent study and research, and the official work of the offices and recognized student organizations. The privilege of using computer and network resources extended by the University to specific individuals and organizations is not transferable.

Table of Contents

Definitions

Term	Definition

Policy Details

Mount Union makes available technological resources that may be used by University students, faculty and staff. These resources may include administrative software applications, file and print services, VPN, wireless access, network resources, e-mail, library resources, ID card system, multi-media resources, desktop applications and computer resources.

These resources are intended to be used primarily for educational purposes, communications, and to carry out the legitimate business of the University. Appropriate use of the resources includes instruction, independent study and research, and the official work of the offices and recognized student organizations. The privilege of using computer and network resources extended by the University to specific individuals and organizations is not transferable.

The responsible, considerate and ethical behavior expected by Mount Union in all aspects of the community extends to cover the use of campus computer and network resources and the use of networks throughout the world to which Mount Union provides computer access. The University's guidelines for appropriate use are not meant to be an exhaustive list of what may or may not be done with the University's computer or network resources.

Those who make use of the network and computing resources must conform at all times to the policies contained herein, as well as the regulations and guidelines of the University as specified in the Student Handbook and the various employee handbooks. These policies exist to safeguard the security and functionality of the campus network and all components therein

The Technology Resource Acceptable Use Policy is comprised of several components described below including unacceptable use, Technology User Code of Conduct, Network Use Policy, E-mail Policy, Hardware & Software Support Policy and Data Security. For faculty and staff members of the University should also familiarize themselves with the Information Security Policy, Environmental Print Policy and Loaner Equipment Policy as these additional polices may pertain to them.

Applies to: Faculty, staff, student employees, students, and volunteers

PROCEDURE

Issued: 6/01/1995
Revised:
Edited: 5/23/2018
Reviewed:

Unacceptable use of the University's computer and network resources are described below:

I. Misuse of Service
   a. Any action that renders facilities unusable to those who rely on them or that interferes with another's use of facilities constitutes misuse. Examples are failure to respect the priorities posted at a public machine, overuse of resources, damage to software or hardware, sending repeated unwanted electronic mail, neglect or damage of software or hardware, and failure to report known problems.

II. Breach of Security
   a. Any attempt to circumvent the protection that Mount Union has in place to prevent unauthorized access or any action that reduces the security of the University's computer and network resources is unacceptable use. Examples are attempts to misappropriate passwords, attempts to gain unauthorized access or sharing your password with others and violating federal, state and local laws related to privacy.

III. Illegal Use
   a. Any use of computer or network resources in the commission of an illegal act is unacceptable. Examples are violation of licensing agreements, attempting to break into a computer or sending harassing or threatening electronic mail. There are federal, state and local laws that govern certain aspects of computer and telecommunications use. All laws pertaining to tangible documents or instruments apply equally to electronic files. This includes student records. Members of the University community are expected to respect these laws. Any use, even if not specifically prohibited, which falls within these broad categories should be considered inappropriate. If you are unsure of the propriety of an action, contact the Office of Information Technology (IT) for clarification.
   b. Much like laws that govern print and recorded media, U.S. Copyright law protects copyright owners from unauthorized reproduction, adaptation or distribution of digital media. While users in educational settings enjoy limited permission to use copyrighted works under the "fair use" provisions of the copyright law, students and faculty who are engaged in developing web pages and other electronic media are advised to read further what the law allows under these circumstances. A very useful text Commonsense Copyright: A guide for Educators and Librarians by R. S. Talab is available in our Library
   c. Some points include:
      i. Excerpts must be brief and confined to a campus network
      ii. Faculty may keep copies of student work for a maximum of two years as examples of exemplary work.
      iii. Students may show multimedia projects developed in University classes for interview and potential employment as long as they have followed fair uses practices.

IV. Peer-to-Peer File Sharing
   a. Peer-to-peer file sharing is prohibited. The Office of Information Technology monitors traffic patterns in order to guarantee acceptable network performance for all users. If IT becomes aware of policy violations or illegal activities in the course of investigating network congestion or problem determination, IT will further investigate by inspecting content stored or shared on its network.
   b. A minimum response to violators of copyright laws, as well as those impeding network performances, will be a warning to cease and desist. In certain circumstances, including those involving repeat offenders, violators will have their access blocked and be turned over to the

University judicial process. If contacted by the RIAA (The Recording Industry Association of America), DMCA (Digital Millennium Copyright Act) or by the courts and asked to identify those who are sharing or downloading based on IP addresses, Mount Union will comply with the law.

c. Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject a student, faculty or staff member to civil and criminal liabilities. Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act 9Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement. Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work Infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. Willful copyright Infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information visit the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq

V. Systematic Monitoring and Access and Disclosure without Consent

a. Mount Union is not obligated to monitor the content of e-mail or file space. The Office of Information Technology, however, maintains the rights to monitor, trace, intercept, or block any network traffic for security or management purposes. Mount Union will, as a courtesy, normally try to inform users prior to any inspection, monitoring or disclosure of e-mail or electronic files, except when such notification would be detrimental to an investigation of possible violation of law or University policy. Users are required to comply with University requests for access to and copies of e-mail records and electronic files when access or disclosure is required or allowed by applicable law or policy, regardless whether such records reside on a computer housed or owned by the University. Failure to comply with such requests can lead to disciplinary or legal action pursuant to applicable law or policy, including, but not limited to, appropriate University personnel policies or Codes of conduct.

b. In summary, Mount Union shall only permit the individual monitoring, inspection or disclosure of electronic mail, electronic files or network traffic:

i. When prior consent has been obtained in writing from the employee and/or student. Consent is given when an individual signs her/his contract or registration. Any employee or student who refuses consent may be denied access to the Internet and electronic mail;
ii. When required by and consistent with law;
iii. When there is probable cause or substantiated reason to believe that violations of law or of Mount Union or state policies have taken place;
iv. When it is for a valid business purpose and there are compelling circumstances; and/or
v. Under time-dependent, critical operational circumstances.

VI. Remedial Action and Sanctions for Violations of Technology Policies

a. Final technical authority for the Mount Union computer network rests with the Office of Information Technology, who may issue training notices, alerts, or warnings for any minor or inadvertent misuse of service or breach of security. Any illegal activity will be reported immediately to the appropriate University official. Final disciplinary authority for misconduct or misuse by members of the Mount Union community rests with the appropriate authorities outlined in the Student Handbook and the various employee handbooks.

b. Access to Mount Union's e-mail, network and Internet services are a privilege that may be wholly or partially restricted by the University without prior notice and without the consent of the user. This may occur when there is probable cause or a substantiated reason to believe that violations of policy or law have taken place or in exceptional cases when required to meet time-dependent, critical operational needs. Any employee or student who abuses the privilege of University facilitated access to the Internet and e-mail may be subject to disciplinary action up to and including termination or expulsion. If necessary, the University also reserves the right to advise appropriate legal officials of any violations and institute legal proceedings against violators of this policy. Any policy violations should be reported to Helpdesk@mountunion.edu. Acts of retaliation

for reporting instances of misuse are prohibited, both by the University and under state and federal law. Reports of misuse cannot be made anonymously, due to the ability of the system to track the originator of any electronic communications.

Technology User Code of Conduct

I. The following Code of Conduct is intended to instruct technology users in acceptable behavior regarding their use of Mount Union technological resources. This document is not intended to be exhaustive if all possible behaviors that may be deemed inappropriate. Users are expected to adhere to all policies set forth by the University regarding the use of technology resources. Failure to follow the expectations set forth in this Code of Conduct or any other policy of the University regarding use of technology may result in sanctions against the user, including, but not limited to, loss of access to technology resources and/or disciplinary action.
   a. Users are responsible for how their accounts are used; therefore, every effort must be made to protect against unauthorized access to accounts. Users must have a password which will protect their accounts from unauthorized use and which will not be guessed easily. If a user discovers that someone has made unauthorized use of her/his account, she/he should change the password and report the intrusion to the Office of Information Technology. Users are required to change their password every 90 days.
   b. Users may not intentionally seek information about, browse or obtain copies of or modify files or passwords belonging to other people, whether at Mount Union or elsewhere, unless specifically authorized to do so by those individuals. Also, users may not attempt to intercept, capture, alter or interfere in any way with information on campus or global network paths
   c. Users must not attempt to decrypt or translate encrypted material or obtain system privileges to which they are not entitled. Attempts to do any of the above will be considered serious violations
   d. If users encounter or observe a gap in system or network security, they must report the gap to the Office of Information Technology. Users must refrain from exploiting any such gaps in security.
   e. Users must refrain from any action that interferes with the supervisory or accounting functions of the system or that is likely to have such effects.
   f. Users must be sensitive to the public nature of shared facilities, and take care not to display sounds or messages that could create an atmosphere of discomfort or harassment for others.
   g. Users must avoid tying up computing resources for game playing or other trivial applications, sending frivolous or excessive mail or messages locally or over an affiliated network or printing excessive copies of documents, files, images or data. Users should be sensitive to special needs for software and services available in only one Page | 4 Last Update: May 2016 location and cede place to those whose work requires the special items.
   h. Users may not prevent others from using shared resources by running unattended processes or placing signs on devices to “reserve” them without authorization.
   i. Users may not copy, cross-assemble or reverse-compile any software or data that the University has obtained under a contract or license that prohibits such actions. If it is unclear if it is permissible to take such actions, users should assume that they may not do so.
   j. Software may not be copied or used illegally. Website materials must be cited appropriately and permission obtained for the publishing, performing or distribution of copyrighted material.
   k. Messages, sentiments and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. Users are free to publish their opinions, but they must be clearly and accurately identified as coming from the particular user or, if a user is acting as the authorized agent of a group recognized by the University, as coming from the group she/he is authorized to represent. Attempts to alter the “From” line or other attribution of origin in electronic mail, messages or postings will be considered violations of University policies.
   l. Users may not take any action that damages Mount Union technology resources in any way, including technology found in classrooms, public computing labs, departmental labs, residence halls and University houses, or any other campus location.
   m. Users may not establish any computer to function as a server without the knowledge and approval of the Office of Information Technology.

Applies to: Faculty, staff, student employees, students, and volunteers

n. Users are required to utilize anti-virus software on their computers. Anti-virus software must be updated regularly.
o. Users may not deploy any network electronic equipment or install wireless access points without express permission from the Information Technology Department.
p. Users who utilize the Mount Union e-mail system are required to comply with state and federal law, University policies, and normal standards of professional and personal courtesy and conduct.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	Provides and maintains the campus's information technology resources.

Resources

Contacts

Position	Office	Telephone	E-mail/URL
Director of IT	Office of Information Technology	330-823-2854	IT@mountunion.edu

History

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.
Issued: 6/01/1995

Revised:

Edited: 5/23/18

Reviewed: