# Mid-Atlantic Christian University
# Office of Information Technology Policy #1

SUBJECT: Acceptable Usage of Information Technology Resources

DATE: April 08 2013

REVISED: 02/11/2014; 02/27/2015; April 2020
NEXT SCHEDULED REVIEW: Yearly, February

APPROVED BY BOARD OF TRUSTEES: October 18, 2013

Policy for: All Authorized Users of Mid-Atlantic Christian Information Technology Resources
Procedure for: All Authored Users of Mid-Atlantic Christian Information Technology Resources
Authorized by: Vice President for Finance
Issued by: Board of Trustees

---

## I. Purpose

This policy is intended to protect the wide array of information technology resources ("Resources") as defined in this Policy provided by Mid-Atlantic Christian University ("University") and to provide guidelines for the use of those Resources.

## II. Policy

Mid-Atlantic Christian University imposes certain responsibilities on Authorized Users of Resources. Access to Resources is subject to University policies and procedures and federal, North Carolina, and all other applicable laws. Appropriate use is legal and ethical, coincides with the University mission, reflects academic honesty, reflects community standards, and shows restraint in the consumption of shared resources. Appropriate Use demonstrates respect for intellectual property; ownership of data; system security mechanisms; and individual rights to privacy and to freedom from intimidation, harassment, and unwarranted annoyance.

## III. Procedures

A. Understanding Resources and Appropriate Use
    a. Resources and Authorized Use
        i. Resources means the University's computing, network and, information technology Resources, including without limitation all data and information in electronic format or any hardware or software that makes

possible, in the broadest possible sense, the processing, transmission, storage or use of such information.

ii. The University may, in its sole and exclusive discretion, allocate, authorize use of, and control access to Resources in differential ways in order to achieve its overall mission. This policy does not prohibit use of tools and techniques by Office of Information Technology ("OIT") systems administration personnel, Authorized Users, or faculty for research or instructional purposes, as long as those activities do not interfere with appropriate use by others.

iii. Authorized Use of Resources is use that the University determines, in its sole and exclusive discretion, is consistent with the education, research, and mission of the University, consistent with effective departmental or divisional operations, and consistent with this policy.

iv. The University may control access to Resources in accordance with federal, North Carolina, all other applicable laws, and University policies and procedures limiting use to Authorized Users. Authorized Users may include:

1. Current faculty, staff, and students of the University
2. Anyone connecting to a public information service through the use of University Resources
3. Others whose access furthers the mission of the University, and whose usage does not interfere with general access to Resources, as determined by the University in its sole and exclusive discretion

**b. Individual Privileges**

The following individual privileges empower users to be productive members of the campus community. Privileges require acceptance of accompanying responsibilities.

i. Privacy - Technological methods must not be used to infringe upon privacy.

ii. Freedom from harassment and undesired information - All constituents have the right to be free from harassment as defined in this policy by or via usage of Resources

**c. Individual Responsibilities**

The University holds Authorized Users accountable for their actions as a condition of current and continued use of Resources.

i. Demonstrating common courtesy and respect for rights of others - Authorized Users must respect and value privacy rights, behave ethically, and comply with all legal restrictions regarding the use of information that is the property of others.
ii. Abiding by laws, policies, contracts, and licenses - Authorized Users must comply with all federal, North Carolina, and other applicable laws; all generally applicable University rules and policies; and all applicable contracts and licenses. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
iii. Compliance with copyright laws - Authorized Users may not copy, distribute, modify, or display another's work unless the copyright owner has given permission to do so; it is in the "public domain"; doing so would constitute "fair use"; or an "implied license" to do so was granted. Using Resources to download or share copyrighted material without the permission of the copyright owner may result in sanctions.
iv. Avoidance of harassment - No member of the community may use Resources to libel, slander, or harass any other person. Harassment includes, without limitation, the following:

    1. Intentionally using Resources to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or others;
    2. Intentionally using Resources to sexually harass or discriminate against any individual;
    3. Intentionally using Resources to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;
    4. Intentionally using Resources to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease;
    5. Intentionally using Resources to disrupt or damage the academic, research, administrative, or related pursuits of another;
    6. Intentionally using Resources to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

v. Responsible use of Resources - Authorized Users are responsible for knowing what Resources are available, remembering that the members

of the community share them, and for refraining from all acts that corrupt, interfere, waste or prevent others from using these Resources, or from using Resources in ways that have been proscribed by the University and by federal, North Carolina, and all other applicable laws.

vi. Preserving information integrity - Authorized Users are responsible for awareness of the potential for and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to verify the integrity and completeness of information compiled or used. Unauthorized access to information contained in a user's Office of Information Technology (OIT)-maintained directory space is prohibited even if the files are readable and/or writable. Modifying files anywhere on an OIT-managed device or directory without consent of the file's owner is prohibited. This includes writing or modifying files that have file permissions set to allow modification or writing. This also includes creating new files, renaming, or deleting existing files in directories that may have directory permissions set to allow creation or modification of files.

vii. Use of Personally Owned Computing Devices ("PCOD") – The University does not condone the use of PCOD for University-related business.

At no time does the University accept liability for the maintenance, backup, or loss of data on a personal device.

It is the responsibility of the equipment owner to backup all software and data to other appropriate backup storage systems.

The University shall NOT be liable for the loss, theft, or damage of POCD. This includes, but is not limited to, when the device is being used for University business, on University time, or during University-related business travel.

The use of PCODs must not disrupt the use of Resources.

Users are responsible for ensuring that POCD meet the security standards of the University. For complete requirements for PCOD use at the University or on University-owned Resources, consult Office on Information Technology Policy FA-IT 02 Information Security.

**d. Network Drives and Storage of Data**

i. Each department is assigned a network drive. Departments and employees are expected to save all university-related files to appropriate network drives and maintain the structured integrity of each drive. Files

are not to be saved the root directly of each network drive. An appropriate folder should be made and, if needed, make a permission request through OIT. All permission and mapping requests should be made through OIT. Upon request, the “Staff” drive can be used as a repository for departments to interact. Request for interdepartmental drives should be made through OIT.

ii. All personal files should be saved to “H:” drives and not on local computers. If an "H:" drive is unavailable a request should be made through OIT.

**B. Access to Resources**

a. Access - An Authorized User must be specifically authorized to use particular Resources by the campus unit responsible for operating the Resources. Departmental managers and OIT systems administrators are authorized to inspect, use, or assign for use Resources in their area of responsibility.
b. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with others. No third-party access to any accounts with access to Resources is permitted without advance, written authorization. An Authorized User is responsible for any use of the individual account. Authorized Users may not run or otherwise configure software or hardware to intentionally allow access by unauthorized users.
c. Expectation of Privacy - University network users should have no expectation of privacy when transmitting information across the University network.
d. Use of privileged access - Special access to information or other special computing, network or information technology privileges or job responsibilities are to be used in performance of official duties only. Information obtained through special privileges is to be treated as confidential, except as otherwise provided in any University policy, procedure or ordinance, or as required or permitted by applicable law.
e. Termination of access - When an Authorized User ceases to be a member of the campus community through graduation, failure to enroll, change of guest status or termination of employment, or if an employee is assigned a new position and/or responsibilities within the University, access and authorization must be reviewed and the University reserves the right to terminate the account. An individual must not use facilities, accounts, access codes, privileges, or information without authorization appropriate to the new situation.
f. Attempts to circumvent security - Authorized Users are prohibited from attempting to circumvent or subvert any security measures or assigned account privileges. Authorized Users may not obtain unauthorized Resources, deprive another Authorized User of Resources, or gain unauthorized access to Resources by using knowledge of an unauthorized password or loophole in a computer security system.

g. Denial of service and other harmful activities - Deliberate attempts to degrade the performance of Resources, or to deprive Authorized Users use of or access to Resources, is prohibited. Harmful activities that are prohibited include without limitation: creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to Resources.
h. Academic dishonesty - Use of Resources in accordance with the high ethical standards of the University community is required. Academic dishonesty is a violation of those standards (Academic Affairs Policy AA-48 Academic Honesty).
i. Use of copyrighted information and materials - The University does not condone unauthorized copying of copyrighted material. Authorized Users are expected to adhere to the rights granted to copyright owners under Section 106 of the Copyright Act (Title 17.) The Digital Millennium Copyright Act establishes the liability for infringement of copyright laws by users of computing resources at institutions of higher education. More information can be found at the official University copyright information site: copyright.macuniversity.edu. Additional information can also be found at http://www.copyright.gov/ and http://www.copyright.gov/help/faq/
j. Use of licensed software - No software may be installed, copied, or used on Resources except as permitted by the owner of the software and the approval of OIT. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly followed. (OIT Policy F-IT 04 – Software Regulations)
k. E-mail - By opening and using an e-mail account, Authorized Users agree and consent that the University may access the account for administrative and all other purposes permitted or required by law and/or the University's policies, procedures and ordinances, which may require the University or its e-mail provider to access and disclose to the University any information stored within the account. The University does not centrally retain or archive e-mail sent, processed or received by the University e-mail system. E-mail may be retained, stored or archived by external providers of e-mail services. Email is considered an official method for communication at Mid-Atlantic Christian University. Official email communications are intended to meet the academic and administrative needs of the University. The University has the right to expect that such communications will be received and read in a timely fashion. To enable this process, the University ensures that all Authorized users can be accessed through a standardized, University-issued email account. For more information, see OIT Policy #7 Email.
l. Web sites, blogs, political campaigning, and other public information uses -The use of Resources in political campaigns or for commercial purposes is prohibited unless authorized by the President of the University.
m. Game playing, web surfing and other recreational activities - Limited recreational game playing, web surfing, or other recreational activity that is not part of an

authorized and assigned research or instructional activity is tolerated (within the parameters of each department's or division's rules). Resources are not to be used for excessive recreation, as determined by the University in its sole and exclusive discretion, outside residential and recreational areas. Individuals engaged in recreational activities while occupying a seat in a public computing facility must give up that seat when others who need to use the facility for academic or research purposes are waiting.

n. Unrelated business - Resources may not be used in connection with compensated outside work, business unrelated to the University, or for the benefit of organizations not related to the University except in connection with scholarly pursuits (such as faculty publishing activities or work for professional societies) or other activities authorized by the President of the University. This and any other incidental use must not interfere with other users' access to Resources and must not be excessive.
o. Prurient interest - Use of Resources must not violate any federal, North Carolina, or any other applicable laws. The use of Resources should adhere to the University's standards of conduct and overall mission. For more information, review § 7 (Rights and Responsibilities) of the University Staff Handbook
p. Issues of Safety and well-being - The University may suspend an individual's access to and use of Resources for reasons relating to his/her physical or emotional safety and well-being, or for reasons relating to the safety and well-being of others, or the safety and well-being of University property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action.
q. Investigative contact - If contacted by a representative from an external organization (FBI, Homeland Security, police department, etc.) or a representative from an internal investigating body conducting an investigation of an alleged violation involving Resources, inform the Office of the President immediately.
r. Reporting security and abuse incidents - Report any discovered unauthorized access attempts or other improper usage of Resources to OIT (itsupport@macuniversity.edu)

## C. Monitoring and Inspection of Logs and Files

a. The University seeks to maintain a secure computing system, but cannot and does not guarantee security or confidentiality. In addition to accidental and intentional breaches of security, the University may be compelled to disclose electronic information as required by law.
b. As part of necessary routine operations, OIT occasionally gains access to Resources. Suspected policy violations discovered during such routine operations will be reported as noted in the Procedures and Sanctions section. All other information accessed during such routine operations will be treated as

confidential, except as otherwise provided in any University policy, procedure or ordinance or as required or permitted by applicable law.

c. When the University has a good faith belief of suspected violations of this policy or unlawful activity, it may access Resources necessary to investigate such suspected violations.
d. The University may access Resources and/or accounts for any other reason as permitted or required by law.
e. If required by law or this policy, the Authorized User will be notified that his/her Resources have been accessed.
f. Using Resources for unauthorized monitoring is prohibited.

**D. Reporting of Violations**

a. Student Violations - Reports of violations are forwarded to the Vice President for Student Services.
b. Employee/staff Violations - Reports of violations are forwarded the appropriate vice president. OIT will first seek to educate those found to be in violation of this policy.
c. Faculty Violations – Faculty violations are forwarded to the Vice -President for Academic Affairs.
d. Violations by other Authorized Users - Reports of violations will be forwarded to the appropriate University official.

**E. Sanctions**

a. Imposition of Sanctions - The University may, in its sole and exclusive discretion, impose sanctions and/or disciplinary action for violations of this policy including without limitation the sanctions described in this policy.
b. Sanctions - In all cases of an actual or suspected violation of this policy, access to Resources will be suspended until final resolution as noted below.
c. Subsequent and/or major violations - Subsequent and/or major violations, as determined by a representative of OIT in his or her sole and exclusive discretion, will be forwarded to Office of the President.
d. Range of Disciplinary Sanctions - Persons in violation of this policy are subject to the full range of sanctions, including without limitation the loss of access privileges to Resources, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined by federal, North Carolina, and all other applicable laws; the University will carry out its responsibility to report such violations to the appropriate authorities.

## IV. Published: Policy Website

## V. Reason for Revision

## VI. Appendices

| Definitions | |
|---|---|
| Authorized Use | Authorized Use of Resources is use that the University determines, in its sole and exclusive discretion, is consistent with the education, research, and mission of the University, consistent with effective departmental or divisional operations, and consistent with this policy. |
| Authorized Users | Authorized Users may include:<br>• Current faculty, staff, and students of the University<br>• Anyone connecting to a public information service through the use of University Resources<br>• Others whose access furthers the mission of the University, and whose usage does not interfere with general access to Resources, as determined by the University in its sole and exclusive discretion |
| Confidential Data | Confidential data refers to sensitive information related to University business, personally identifiable information, or other information that is not intended for outside disclosure. Confidential data includes, but is not limited to, social security numbers, credit card information, driver's licenses, banking information, protected health information (as defined by HIPAA), student disciplinary records, employee personnel files, judiciary committee proceedings, and protected student information (as defined by FERPA.) |
| Personally Owned Computing Device | Devices used by Authorized Users that are not owned by the University. |
| Resources | Resources - Resources means the University's computing, network and, information technology Resources, including without limitation all data and information in electronic format or any hardware or software that makes possible, in the broadest possible sense, the processing, transmission, storage or use of such information. |

| Relevant Policies and Documents |
|---|
| Academic Affairs Policy AA-48 – Academic Honesty |
| Office of Information Policy F-IT 02- Information Security |
| Office of Information Policy F-IT 04 – Software Regulations |
| Office of Information Policy F-IT 07 – Email |

**Relevant Legislation**

| | |
|---|---|
| **United States Code, Title 18, Section 1030 et seq,** *Computer Fraud and Abuse Act* | Imposes sanctions for, among other acts, knowingly accessing a computer without authorization or in excess of authorized access, knowingly causing damage to protected computers, or trafficking in password information. |
| **United States Code, Title 18, Section 2510 et seq.,** *Electronic Communications Privacy Act*, | Imposes sanctions for, among other acts, interception of wire, oral or electronic communications. |
| **United States Code, Title 18, Sections 2701 et seq.,** *Stored Wire and Electronic* | Imposes sanctions for, among other acts, intentionally accessing without authorization, a facility through which electronic communication service is provided, or intentionally exceeding authorization to access a facility, thereby obtaining, and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage. |
| **United States Code, Title 47, Section 223 (H)(1) et seq.,** *Communications Act of 1934 (as amended)* | Imposes sanctions for, among other acts, use of any device or software that can be used to originate telecommunications or other types of communications that are transmitted in whole or in part by the internet, without disclosing the sender's identity, and with intent to annoy, abuse, threaten, or harass any person who receives the communications. |
| *North Carolina Identity Theft Protection Act of 2005* | Enacted in 2005, the North Carolina Identity Theft Protection Act of 2005 affords certain protections to individuals and requires that businesses within North Carolina take reasonable steps to protect the information of its information. Additionally, this act requires that the University notify affected users of security breaches. |