Acceptable Use Policy

Effective:
September 2, 2016

Purpose

Montreat College is committed to protecting its employees, partners, and itself from illegal or damaging actions by individuals, either knowingly or unknowingly. Access to computer equipment, systems, and networks owned or operated by Montreat College is a privilege that is granted by the college subject to certain rules, regulations, and restrictions. This access carries with it certain ethical responsibilities and obligations, and should reflect the academic honesty, discipline, and standards of conduct appropriate for our shared community of network and computer resources. Most importantly, each user of the college's technology resources is a representative of the college, in that a record of his or her user address – reflecting "montreat.edu"— is left at each site that is visited or emailed. Accordingly, each user is expected to behave in a manner that reflects our commitment to be a community under the Lordship of Jesus Christ.

The purpose of this policy is to outline the acceptable use of computer equipment at Montreat College. These rules are in place to protect the college and its faculty, staff, and students. Inappropriate use of technology exposes Montreat College to risks including virus attacks, compromise of network systems and services, and legal issues. Any person who has a question about this policy or is concerned about potential violation of this policy by him/herself or by another person, is encouraged to contact Campus Technology.

Scope

This policy applies to all individuals who are given access to computer equipment, systems, and networks owned or operated by Montreat College, including, but not limited to, the following (whether full-time or part-time): faculty, staff, and students. This policy applies to the use of information, electronic and computing devices, and network resources to conduct Montreat College business or interact with internal networks and business systems, whether owned or leased by Montreat College, the individual, or a third party.

Policy

By using the college's information technology resources, each user accepts the responsibility for his or her behavior and all activities on his or her user id and agrees as follows:

General Use and Ownership

- Users may only access files and data that they own, that are publicly available, or to which they have been given authorized access.

- Users may only use legal versions of copyrighted material in compliance with vendor license requirements and may not make or use illegal copies of copyrighted material, store such copies on college systems, or transmit them over college networks.
- Users must abide by a) all rules, regulations, policies, and procedures adopted by the college, b) all rules and regulations posted in computer labs and printer areas, and c) all instructions given by staff members.
- Users are responsible for promptly reporting the theft, loss, or unauthorized disclosure of Montreat College proprietary information.
- Users may access, use, or share Montreat College proprietary information only to the extent authorized and necessary to fulfill their assigned job duties.
- Users are responsible for exercising good judgment regarding the reasonableness of personal use of Internet/Intranet systems. If there is any uncertainty as to the reasonableness of personal use, users should consult with Campus Technology.
- For security and network maintenance purposes authorized individuals within Montreat College may monitor equipment, systems, and network traffic at any time.
- Montreat College reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

- System level and user level passwords must comply with the *Password Protection Policy*.
- Providing access to another individual, either deliberately or through failure to secure an account's access, is prohibited.
- All computing devices must be secured with a password-protected screensaver with an automatic activation of 15 minutes or less.
- Screens must be locked, or the user account signed out of the device when it is unattended.
- Postings by employees from a Montreat College email address to newsgroups should contain a disclaimer stating that "the opinions expressed are my own and not necessarily those of Montreat College," unless posting is in the course of normal job duties.
- Users must use extreme caution when opening email attachments received from unknown senders, as the attachments may contain malware.
- Montreat College proprietary information stored on electronic and computing devices – whether owned or leased by Montreat College, the employee, or a third party – remains the sole property of Montreat College. Users must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Policy*.

Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may have a need to disable network access of a host if that host is disrupting services).

Under no circumstances is a user authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing Montreat College-owned resources.

The lists below are by no means exhaustive, but rather attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited:

- Violations of the rights of any person or company 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” software or other software products that are not appropriately licensed for use by Montreat College.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Montreat College or the end user does not have an active license.
- Accessing data, a server, or an account for any purpose other than conducting Montreat College business, even if you have authorized access.
- Introduction of malicious programs onto the network or servers (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Revealing your account password to others or allowing the use of your account by others. This includes family and other household members.
- Using a Montreat College computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which you are not the intended recipient or logging into a server or account that you are not expressly authorized to access, unless these duties are within the scope of your regular duties. For purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Port scanning or security scanning.
- Executing any form of network monitoring which will intercept data not intended for your host, unless this activity is part of your normal job or duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the Montreat College network.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means, locally or via the internet/intranet.
- Providing information about or lists of Montreat College faculty, staff, administrators, or students to parties outside of Montreat College.
- Monopolizing systems, overloading networks with excessive data or non-work relate messages, or wasting computer time, connection time, disk space, printer paper, manuals, or other resources.
- Using computer programs or other means to decode passwords or access control information.
- Access or modification of network security logs.
- Using the college's systems for personal gain. For example, by selling access to your user id or password, or by performing work for profit in a manner not authorized by the college.
- Installing or operating computer games on college-owned machines for purposes other than academic instruction.
- Attempting or assisting in an attempt to a) penetrate system security, b) cause any part of the system to become impaired or inoperable, or c) gain unauthorized access or entry to computer facilities and/or computer-based data.

Email and Communication Activities

When using company resources to access and use the internet, users must realize they represent the college. Whenever employees state an affiliation to the college, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of Montreat College." Questions may be addressed to Campus Technology. The following activities are prohibited:

- Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or instant messenger, whether through language, frequency, or size of messages.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address other than that of the poster’s account with the intent to harass or collect replies.
- Creating or forwarding “chain letters”, “Ponzi”, or other “pyramid” schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of newsgroups or forums (newsgroup/forum spam).
- Using mail or message services intending to harass or intimidate another person, or to indiscriminately broadcast information of a frivolous nature.

Policy Compliance

The college considers any violation to be a serious offense. College officials reserve the right to access, examine, intercept, monitor, and copy the files and/or actual terminal sessions of any user, or to suspend a user’s access to the system, in connection with the investigation of any of the following: a) violations or suspected violations of security and/or policies, b) terminal interactions which may be contributing to poor computer performance, or c) computer malfunctions. In connection with such investigations, users whose files or terminal sessions are affected are deemed to have acknowledged the following: that they are not entitled to any expectation of privacy with regard to their files, data, or communications, and that appropriate college officials and criminal enforcement agencies may be notified of the violation and provided with information and materials relating to the investigation and/or violation.

Compliance Measurement

Campus Technology will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved by Campus Technology in advance.

Non-Compliance

The responses for violation of this policy will include, but are not limited to, the following:

- Notification: alerting a user to what appears to be an inadvertent violation of this policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.

- Loss of computer privileges: limitation or removal of computer privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer related material, equipment, hardware, software, data, and/or facilities, which reimbursement shall include, but not be limited to, the cost of additional time spent by college employees due to the violation.

In addition to the aforementioned, violators may be subject to disciplinary action – which may include suspension, expulsion, or termination – as may be prescribed by other rules, regulations, handbooks, procedures, or policies applicable to the violator. Furthermore, the violator may be subject to civil suits or ordinances, laws, statues, or regulations of the applicable local government, the State of North Carolina, or the United States of America.

Definitions of Terms

Sensitive Data: Data such as social security numbers, personal health information (PHI), personal identity information (PII), financial data, proprietary data, graded papers, etc. that must be handled with the utmost care, stored securely, and be protected to the greatest possible extent.

Contact Information

Campus Technology
Phone: 828-669-8012 Ext. 3663
Email: support@montreat.edu

Revision History

Initial Draft: 08/12/2016
Revised: 08/18/2016
Revised: 09/02/2016
Revised:09/07/2021