Monroe Community College
STATE UNIVERSITY OF NEW YORK

7.1 MCC Acceptable Use of College Technology Policy (Revised Draft)

If you need assistance accessing this document, please email complianceandaudit@monroecc.edu or call (585) 292-2182.

Category: Technology

Name of Responsible Office: Technology Services

Title of Responsible Executive: CFO / Vice President, Administrative Services

Date Established: 1998

Date Last Approved: March 7, 2016

~~Summary~~Policy Statement

The purpose of the Acceptable Use Policy is to clearly communicate the responsibility each member of the college community has to protect the information assets and to establish minimum expectations for meeting the requirements.

Following the same standards of common sense, courtesy and civility that govern the use of other shared resources, acceptable use of information technology resources generally respects all individuals' right to be free from intimidation, harassment, and unwarranted annoyance.

Monroe Community College's technology resources exist to support the academic and administrative activities needed to fulfill the college's mission. Access to these resources is a privilege that should be exercised responsibly, ethically, and lawfully.

~~MCC computer facilities and systems are intended for appropriate college-related work.~~ MCC computer systems are ~~a public~~ college resources and users should have no expectations of privacy while using them ~~resources~~. Computer systems will be monitored for software and activities not approved by the college.

All MCC data ~~stored on college resources is~~are property of the college, but that does not give any individual permission to access, change, copy, delete, distribute and/or read electronic data ~~of~~such as ~~individual~~anyone else's email or personal file storage without the permission of the owner. ~~Shared data locations are meant for collaborative work and as such changes to files are permitted but limited to the rights afforded by the network administrators.~~ Exceptions to this policy will be allowed for troubleshooting technical problems and for college-authorized investigations of potential violations by the appropriate college personnel.

Acceptable use standards require everyone to take prudent and reasonable steps to prevent unauthorized access to systems and data. Access authorization relies on a user-ID and password for each user. The user-ID forms the basis for credentials which are designed to establish ownership and responsibility for computing resources and use. Each individual should use their own user account to access MCC systems. Acceptable use respects these identification and security mechanisms.

Using a personal device does not absolve the user from the responsibility to protect college data. Any college data on non-college-owned devices must be protected with controls equivalent to those on college-managed devices. Monroe Community College reserves the right to block unsafe devices from connecting to the network and systems. This may require users to register their device and accept terms which allow technical assessments before the device is permitted to connect. Automated device inspection utilities would block devices that do not meet security standards. Examples include outdated hardware

and / or software versions, detection of malware, lack of antivirus protection, lack of a device lock-screen passcode, lack of encryption, or other security vulnerabilities.

Activities related to the Monroe Community College mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the college's operation is prohibited.

Monroe Community College reserves the right to immediately take any action it deems necessary, including but not limited to disconnection and quarantine of devices and/or suspension of user accounts or services, to maintain the stability, security and operational effectiveness of computing and network resources.

~~Policy~~

~~*Policy Statement*~~*Prohibited Activities*

College information technology resources may not be used in any manner prohibited by state and federal laws or disallowed by licenses, contracts or policy. This section, while not all-inclusive, lists examples of misuse that would constitute a violation of this policy.

Individuals using MCC's computing technology, facilities, or equipment are NOT permitted to:

- Copy, download, change, distribute or modify any computer programs in part or whole from a website, textbook or another individual without the written consent or permission of the owner. This may be considered plagiarism and/or a violation of copyright and patent laws.
- Install non-college-related software or downloads on college-provided computers, without the permission of Technology Services.
- Use MCC facilities and systems for the purpose of advertising or running an organization or business not affiliated with the College or for personal gain.
- Send, view and/or print lewd or pornographic materials for non-academic purposes.
- Reveal their password to anyone including employees, or let another person use their MCC account. Likewise, users should not use anyone else's credentials for any college systems or services. Each user is responsible for what is done with their MCC account.
- Share codes or approve multi-factor authentication (MFA) prompts unless they are for their own login.
- Use passwords that are weak or can be easily guessed. Users are responsible for establishing unique passwords that comply with MCC password standards including length and complexity requirements. Users must protect their passwords from disclosure and should not record or store them insecurely.
- ~~Users are responsible for what is done with their MCC account.~~Use personal accounts to conduct college business.
- Use MCC accounts, credentials or devices for non-college / personal purposes.
- Use the same password for MCC and non-MCC or personal accounts. ~~Users are responsible for what is done with their MCC account.~~
- ~~All data stored on college resources is property of the college, but that does not give any individual permission to access, change, copy, delete, distribute and/or read electronic data of individual email or personal file storage without the permission of the owner. Shared data locations are meant for collaborative work and as such changes to files are permitted but limited to the rights afforded by the network administrators. Exceptions to this policy will be allowed for the investigation of potential abuses of college resources by the appropriate college personnel.~~

- Engage in intentional malicious activity designed to harm systems, computers and networks. Such activity includes but is not limited to: hacking systems; disabling or crashing systems; network sniffing; sending viruses, malware or mass e-mail; creating unnecessary or multiple jobs and processes.
- Take MCC computing equipment off-site without prior authorization through either the Administrative Services Employee Portable Computer Program for laptops or from Technology Services for other computing equipment or peripherals, such as Desktop Computers, monitors, webcams, etc.
- Fail to follow college data handling requirements for confidential information. Examples include but are not limited to:
    - Accessing or processing restricted college information over public insecure networks. Instead, use an approved secure connection method such as VPN (virtual private network).
    - Storing restricted college information on non-college computers or removable media (phones, tablets, USB drives, etc.), which is prohibited. Any portable device storing confidential college information must be encrypted, and must be securely transported and stored when not in use. Laptops issued by the college to MCC employees are encrypted.
    - Storing, transmitting or sharing restricted college data using solutions not securely managed by MCC. Restricted data should not be stored or shared using non-MCC-provided methods or tools, such as peer to peer sharing, Google Docs, Dropbox, etc. Sharing restricted data should be done only on secure collaboration tools such as Microsoft Teams or M Drive folders with controlled access limited by "need to know/least privilege" principles.
    - Transmitting restricted college information by email (even internally on secure MCC email), especially to distribution lists.
- Bypass ~~accounting or~~ security mechanisms, circumvent data-protection or system consistency schemes, force unauthorized access, or ~~uncover~~ attempt to exploit security loopholes.
- Leave a computer or device unattended without locking the screen to prevent unauthorized access to college systems or information. Any device used to access college systems or data must have lock screen enabled.
- Install, attach, connect, remove or disconnect computing or network hardware to college information systems without approval from Technology Services
- Send harassing, obscene, libelous, or threatening messages.
- Aid or abet another person in violating any part of this Policy, or prevent anyone from reporting an incident.
- Violate any other state, local or federal laws or regulations pertaining to cyber security.

~~*Background*~~*Enforcement*

This policy is intended to comply with and augment all local, state, and federal laws. Individuals who violate any part of the policy will be subject to college disciplinary action (in accordance with all applicable collective bargaining agreements), criminal prosecution, or civil action as determined by college and legal authorities. Use of MCC computer systems is a privilege that may be revoked during the investigation of an alleged violation, or a finding of violation of this policy.

Incident Reporting

In order to detect and respond promptly to security incidents and limit the harm to the college, users have a responsibility to immediately report to the MCC Technology Support Help Desk the loss, theft, inappropriate use, suspicious activity and/or other signs of compromised systems, data, access credentials, security tokens, or devices.

Applicability

This policy applies to all members of the College community with access to the College network, systems and data ~~resources~~, including but not limited to ~~affiliated organizations,~~ employees, students, alumni, trustees, volunteers, vendors, affiliated organizations, and visitors.

~~*Definitions*~~

~~**Users** – Any person who has an MCC Network Account and is permitted to use network resources~~

Exceptions

Exceptions to the policy may be granted by the Chief Information Officer, or by their designee. All exceptions must be reviewed annually.

Responsibility

Associate Vice President, Technology Services / CIO

~~Director, Communications and Network Services/CISO~~

Contact Information

Technology Services

Related Information

Technology Policies that cover systems, access, data, and related issues.

- 7.2 Password Policy
- 7.3 Information Technology Security Policy
- 7.4 Data Classification Policy
- 4.4 Cyber Security Awareness and Education Policy
    - 4.4P Cyber Security Awareness and Education Procedure

~~The MCC Acceptable Use of Technology Policy is a revision of 6.1 Code of Conduct for Users of College Computer Systems.~~