5.275.02 MCC Standards of Acceptable Use

Primary Principles: Mohave Community College strives to promote a culture of openness, trust, integrity, and an environment wherein freedom of expression and scholarly inquiry are encouraged and supported. The intention of the Acceptable Use Standards are not to impose restrictions that are contrary to these values, which are the core of our academic and administrative community. Some computing resources dedicated to specific roles, including administrative systems and teaching systems containing information protected under the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), necessarily limit access in order to protect the privacy of MCC students, faculty, and staff.

Effective security is a team effort involving the participation and support of the entire Mohave Community College team, including its students, faculty, and staff. It is the responsibility of every computer user to know these guidelines, and to conduct activities accordingly.

Purpose: The standards set forth the responsible use of Mohave Community College information technology resources. Individuals and groups using MCC resources both on and off campus are responsible for complying with the security standards set forth, including securing passwords, identification numbers, and security codes and using them solely for their intended purposes. Individuals are solely responsible for their personal use of IT resources, including computer accounts and other resources under their control. These standards are in place to protect the MCC community and to ensure the smooth, secure operation of MCC's information technology systems.

Scope: The standards apply to all information technology resources, including but not limited to computer systems, data and databases, computer labs, smart devices including cell phones and tablets, e-mail boxes, data and voice networks, applications, software, files, and portable media. MCC provides the resources to support the academic, research, administrative, and instructional objectives of the college. The use of these resources are limited to college students, faculty, staff and other authorized users to accomplish tasks appropriate to the status of the individual.

General Acceptable Use Guidelines

The guidelines below are not intended to be comprehensive, but to define and explain the intent of this policy. Situations not specifically covered by this policy will inevitably arise and should be judged and interpreted in the spirit of this policy.

Generally Prohibited Conduct

1. Altering system hardware or software without authorization, including installation of unlicensed or unapproved software or hardware. "Freeware" and "Shareware" programs usually contain a provision denying use in professional environments without payment, so the installation of such programs violates this policy.
2. Disrupting or interfering with the delivery or administration of information technology assets, including network communications, e-mail, hardware, or software.
3. Attempting to access or accessing an account other than the account provided for your use.
4. Intercepting or reading electronic communications, including e-mail and chat messages not addressed or assigned to you.
5. Misrepresenting your identity in an e-mail, chat, or university owned social messaging platform.
6. Installing, copying distributing, or using digital content in violation of copyright and/or software agreements or applicable federal or state law. This includes the use of file sharing

software including but not limited to BitTorrent, uTorrent, Sharefile or other services that allow the illegal download or use of copyrighted media.
7. Interfering with others' use of share resources, including computers, lab space, or common technology areas.
8. Using college resources for commercial or profit-making purposes or to represent the positions or interests of groups unaffiliated or unassociated with the MCC community or the normal professional practices of students, faculty, and staff.
9. Ignoring or evading departmental or lab policies, procedures, and protocols.
10. Assisting unauthorized users' access to college IT resources.
11. Exposing sensitive or confidential information or disclosing information that you do not have the authority to disclose.
12. Using IT resources for illegal activities, including threats, harassment, copyright infringement, defamation, theft, identity theft, and unauthorized access.
13. Using IT resources to access gambling or gaming sites.
14. Failing to use good judgement with respect to personal use of IT resources. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

<u>Security and Proprietary Information</u>

1. All mobile and computing devices that connect to the network must be capable of minimum 128 bit encryption for network traffic.
2. System and user level passwords must comply with college standards (currently 8 characters, including an uppercase, lowercase, number, and a symbol). Failing to protect passwords or allowing others access to resources using your account is prohibited.
3. All computing devices must be secured with password protected screen savers with an automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.
4. Users should assume that attachments or unsolicited message may contain or do contain malware and viruses and avoid opening, executing, or downloading such attachments.
5. Employees posting to forums, social media, Usenet groups, or other communications platforms that use an MCC e-mail address must include a disclaimer stating that their posting does not represent the views of Mohave Community College unless such posting is part of their normal business duties.

<u>System and Network Access</u>

1. Accessing data, a server, or an account for any purpose other than conducting Mohave Community College business is prohibited.
2. Exporting software, technical information, encryption information, or information about the capabilities of information systems is prohibited.
3. Introduction of malicious programs, including viruses, worms, malware, adware, or similar programs is prohibited.
4. Port scanning, security scanning, and other types of network scanning is prohibited without the written permission of the information technology unit.

5. Disrupting network communication through the use of network sniffing, ping flood, packet spoofing, denial of service, forged routing information, e-mail spoofing, or otherwise misrepresenting network traffic is prohibited.
6. Providing information about, or lists of MCC students, faculty, or staff to outside parties unless it is part of your normal duties is prohibited.

E-mail and Electronic Communication

1. Use of MMC resources to access and use the internet requires good judgement on the part of the user. Users must realize that they represent the college and must, when stating an affiliation to the college, include verbiage indicating that the opinions expressed are their own and not necessarily those of Mohave Community College.
2. Sending unsolicited e-mail messages, including "spam" or "junk mail" or other advertising material to individuals who did not request it is prohibited.
3. The unauthorized use or forging of e-mail headers is prohibited.
4. Any form or harassment, including via e-mail, voice mail, and chat services whether through language, frequency, or size of messages is prohibited.
5. Solicitation of e-mail for any e-mail address other than your own is prohibited.
6. Forwarding chain letters, Ponzi or Pyramid scheme messages, or messages not related to college business is prohibited.
7. Use of MCC e-mail addresses for any purpose other than college business is prohibited.

Policy Compliance

The Information Technology department will verify compliance to these standards through various methods, including but not limited to business reports, internal and external audits, audit tools, and security related hardware and software tools.

The Information Technology team routinely monitors inbound, outbound, and internal network traffic for the purposes of compliance and network maintenance. Mohave Community College reserves the right to audit systems and network traffic to ensure compliance with the standards.

Exceptions to the Acceptable Use Standards must be approved by the Information Technology director in advance, and in writing.

Faculty or staff found to be in violation of the standards may be subject to disciplinary action as outlined in the Policy and Procedure Manual (Policy 5.155 Discipline).

Students found to be in violation of the standards may be subject to disciplinary action under the Student Code of Conduct Policies and Procedures.(PDF)