ADMINISTRATIVE PROCEDURE

AP 3720   Computer and Network Use

References: Education Code Section 70902; 17 U.S. Code Sections 101 et seq. Penal Code 502; Accreditation Standard III.C

Computer and Network Acceptable Use Agreement (AUA)

I.   Introduction

To comply with federal and state regulations, laws, and harassment mitigation policies, educational organizations are compelled to establish Internet safety guidelines otherwise known as Acceptable Use Agreements (AUAs) for the appropriate use of computer systems.

II.   Rights and Responsibilities

Use of computers, services, and networks owned by Monterey Peninsula College (MPC) is a privilege governed by certain regulations and restrictions as defined by the College as well as by all applicable federal, state and local laws.

The user agrees to abide by the regulations set forth in this AUA. This means that the user agrees to behave responsibly in accordance with the standards established by MPC and this document while using college systems and network resources.

III.   Right to Privacy

MPC supports each individual's right for personal communication; however, messages on computing resources are accessible to others through normal system administration activities and to the public through public records laws. Therefore MPC cannot guarantee privacy of electronic communication.

The system administrator reserves the right to monitor the usage of all network resources to ensure compliance with this policy, College policy, and federal, state and local laws. User files may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.

MPC users are expected to comply with copyright and intellectual property laws.

Users who become aware of any violation of this policy should notify the proper authorities.

IV.   Email

Email correspondence between employees of MPC to students or the community directly related to performing the duties and business of the College must take place using the official MPC.edu email address. Any official correspondence to a preferred or provided email address that is not a MPC domain email address will be considered a violation of this policy. MPC students should be directed to check MPC.edu email often for communication from the college and its employees. The MPC administration acknowledges there are exceptions to this policy such as when contacted by past students who no longer use college email or prospective students who have not yet received their student email address.

Student E-mail

An MPC e-mail address (username@mpc.edu) is provided to all students as an official means of communication. Students are responsible for all MPC communication sent to their MPC e-mail address.

It is expected that students check their e-mail account on a frequent and consistent basis. To ensure that students remain current with MPC-related communications, students are strongly encouraged:

To check their e-mail at least two times a week.

To respond to all official MPC communications as directed in each communication (e.g., responding in person, by surface mail, or by e-mail).

Do not assume an e-mail response is a satisfactory substitution when directed otherwise.

Students are subject to this policy during academic terms for which they are enrolled, during breaks between terms, and during MPC holidays and vacations.

Faculty members determine how they will use e-mail in their classes. Faculty may wish to include their e-mail expectations in the course syllabus. The distribution of mass communications is restricted to MPC departments and offices for MPC business. External requests for mass communications will not be honored.

MPC employs various measures to protect the security of its computing resources and users' accounts. However, users should be aware that MPC does not and cannot guarantee such security. Furthermore, individuals are advised to exercise caution when sending sensitive or FERPA-protected student information via e-mail. In addition, individuals are reminded that some MPC information is not appropriate for e-mail communication.

V. Enforcement

Violations of this policy will be reported to the appropriate administrator and, if warranted, the appropriate civil authorities. Non-compliance with this policy may also result in the loss of access to computer resources.

Students will be subject to the student discipline process as outlined in the college catalog.

Employees: Enforcement and discipline of this policy will be decided upon by HR and/or applicable union contract agreements.

VI. Acceptable Use Agreement

Conduct which is deemed non-acceptable use of MPC technology resources includes, but is not limited to, the following activities:

- Using a computer account without authorization.
- Sharing an account with other users is not authorized.
- Using the campus network to gain unauthorized access to any computer systems.
- Connecting unauthorized equipment to the campus network.
- Using a personally-owned wireless access point or wireless device acting as an access point on campus.
- Attempting to circumvent data protection schemes or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
- Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks, e.g., deleting programs or changing icon names.
- Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.
- Deliberately wasting/overloading computing resources
- Violating terms of applicable software licensing agreements or copyright laws.
- Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, movies, etc.
- Using College resources for commercial activity, such as creating products or services for sale.
- Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.
- Initiating or propagating electronic chain letters.
- Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."
- Forging the identity of a user or machine in an electronic communication.
- Transmitting, reproducing, or publicly displaying materials that are slanderous or defamatory in nature or that otherwise violate existing laws or MPC regulations.
- Attempting to monitor or tamper with another user's electronic communications.
- Reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
- Transmitting pornographic material.
- Software theft (pirating). Users will not install unapproved software on computers owned by MPC, including software that does not include a site license agreement via MPC Tech Services.
- Accessing MPC Ethernet (wired) network without written permission from MPC IT is strictly prohibited. Violations of this include:
  - Moving computers, printers or other devices from one data port to another.

- o Plugging any personal device into a data port.
- Network shared storage is for work related purposes only. Storing non-work related personal items, including photos, video clips and music is prohibited.

See Board Policy 3720