MPC
MONTEREY PENINSULA
COLLEGE

ADMINISTRATIVE PROCEDURES

Chapter 3 General Institution 3720

AP 3720 Computer and Network Use

This procedure applies to all Monterey Peninsula Community College District employees and students and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone, or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching, or other purposes.

Conditions of Use

The District Computer and Network systems are the sole property of Monterey Peninsula Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work-related purposes only. Computer users must respect the rights of other computer users. Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines, or restrictions.

Legal and Disciplinary Process

This procedure exists within the framework of the District Board Policy and state and federal laws. Violations of this procedure will be reported to the appropriate administrator and if warranted, the appropriate civil authorities. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including, but not limited to, loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action. Enforcement and discipline of this procedure will be decided upon by Human Resources and/or applicable union contract agreements. Students will be subject to the student discipline process as outlined in the college catalog.

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other on-line information.

A. **Copying**: Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

B. **Copyrights**: In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

C. **Number of Simultaneous Users**: The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department unless otherwise stipulated in the purchase contract.

Integrity of Information Resources
Computer users must respect the integrity of computer-based information resources.

A. **Modification or Removal of Equipment**: Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

B. **Unauthorized Use**: Computer users must not interfere with others' access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software, or computer files.

C. **Unauthorized Programs**: Computer users must not intentionally develop, install, or use unauthorized programs or programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

D. **Unauthorized Equipment and Access Points**: Computer users are prohibited from connecting unauthorized equipment to the campus network. Accessing the District ethernet Network to install a personally-owned wireless access point or wireless device acting as an access point on campus is also prohibited.

Unauthorized Access & Reporting Problems
Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

A. **Abuse of Computing Privileges**: Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges. Additional violations include, but are not limited to:
    - Moving computers, printers, or other devices from one data port to another.
    - Plugging any personal device into a data port.

B. **Password Protection**: A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

C. **Reporting Problems**: Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

Usage

A. **Unlawful Messages**: Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening or other messages that violate applicable federal, state, or other law or District policy, or which constitute the unauthorized release of confidential information.

B. **Commercial Usage**: Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations, or promotions (see "Commercial Use" below). Some public discussion groups have been designated for selling items and may be used appropriately, according to the stated purpose of the group(s).

C. **Information Belonging to Others**: Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users.

D. Rights of Individuals: Users must not release any individual's personal information to anyone without proper authorization.

E. User Identification:

- Network accounts are based on users' legal names. District employee name changes must be approved by Human Resources.
- Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.
- Forging the identity of a user or machine in an electronic communication is prohibited.

F. Network Storage: Network shared storage is for work-related purposes only. Storing non-work-related personal items, including photos, video clips, and music is prohibited.

G. Actions that Interfere with Normal Operations: Users must not knowingly or carelessly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks. Examples of such actions include, but are not limited to, deleting programs or changing icon names.

H. Political, Personal, and Commercial Use: The District is a non-profit, tax-exempt organization and as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property, and similar matters.

- **Political Use**: District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.
- **Personal Use**: District information resources should not be used for personal activities not related to District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.
- **Commercial Use**: District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

Email: Official District Communication

A. District email is intended for official District business; therefore email correspondence related to District business must be conducted by MPC employees using the official MPC.edu email provided by the District. Faculty and staff are prohibited from setting District email to automatically forward to any other email address.

B. The distribution of mass communications known as "All User emails" is restricted to select MPC departments and offices for District business. External requests for mass communications will not be honored.

C. Monitoring or tampering with—or attempting to monitor or tamper with—another user's electronic communications is prohibited.

D. Faculty members determine how they will use email communications in their classes within the parameters described in this procedure. Faculty members may wish to include their expectations regarding email communications with students in the course syllabus.

E. Students are provided with an MPC.edu email address as an official means of communication.

- To ensure that students remain current with District communications, students are strongly encouraged to regularly monitor their MPC email. It is suggested that students:
  - Check their email at least two times a week.
  - Respond to all official District communications as directed (for example, responding in person, by mail, or by email).

Nondiscrimination

All users have the right to be free from any conduct connected with the use of Monterey Peninsula Community College District network and computer resources which discriminates against any person on the basis of the categories listed in Board Policy 3410 - Nondiscrimination. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure

A. No Expectation of Privacy: The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system. It is the practice of Information Services (IS) to respect the confidential nature of user files. Any IS employee must have permission from the appropriate administrator and/or Human Resources Department prior to investigating use of the District network and computers or modifying access to individual user accounts. The District shall not inspect, monitor, or disclose use of District network and

computers without the holder's consent, except (1) when is required by and consistent with the law; (2) when there is a substantiated reason to believe that violations of law or provisions herein have taken place and the holder or user is the subject of suspicion; or (3) under time-dependent emergency circumstances or critical compelling circumstances.

B. Possibility of Disclosure: Users must be aware of the possibility of unintended disclosure of communications.

C. Retrieval: It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

D. Public Records: The *California Public Records Act* (*Government Code Sections 6250 et seq.*) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network or computers must be disclosed if requested by a member of the public.

E. Litigation: Computer transmissions and electronically stored information may be discoverable in litigation.

F. Law Enforcement: 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.

G. Security: The District employs various measures to protect the security of its computing resources and users' accounts. However, the District does not and cannot guarantee such security. Therefore, individuals are advised to exercise caution when sending sensitive or FERPA-protected student information via email. In addition, individuals are reminded that some District information is not appropriate for email communication.

Dissemination and User Acknowledgment

All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

A "pop-up" screen addressing the email portions of these procedures shall be installed on all email systems. The "pop-up" screen shall appear prior to accessing the email network. Users shall sign and date the acknowledgment and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. This acknowledgment and waiver shall be in the form as follows:

MPC
MONTEREY PENINSULA
COLLEGE

ADMINISTRATIVE PROCEDURES

Computer and Network Use Agreement
I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated _____, and recognize and understand the guidelines. I agree to abide by the standards set in the Procedures for the duration of my employment or enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of state or federal law.

See Board Policy 3720 - Computer and Network Use

See also Board Policy 2716 - Political Activity, Board Policy 2717 - Personal Use of Public Resources, Board Policy 3410 - Nondiscrimination, Board Policy and Administrative Procedure 7370 - Political Activity, and Administrative Procedure 7371 - Personal Use of Public Resources

References: *15 U.S. Code Sections 6801 et seq.;*
17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1 subdivision (b);
16 Code of Federal Regulations Parts 314.1 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45;
Accreditation Standard III.C

Approved: April 28, 2020
Revised and Approved: May 11, 2021