

## Appendix A

### Monterey Peninsula College Institutional Technology Committee

#### Internet/Network Use Policy

**1. Introduction:**

Monterey Peninsula College (MPC) owns and operates a variety of computer systems for use by its faculty, student, and staff. MPC encourages the use of its computer systems for education, academic development, public service, and other educational purposes. When using MPC's computer systems, all users are required to abide by the rules of this Policy and use the system in an ethical and lawful manner.

**2. Policy Requisite:**

All users of MPC's computing systems must read, understand, and comply with the terms outlined in this Policy, as well as any additional guidelines established by the administrator of the system. *By using any of these systems, users agree that they will comply with these policies.* Users understand and agree that MPC's role in managing these systems is only as an information carrier and that they will never consider transmission through these systems as an endorsement of said transmission by MPC.

**2. Related Legislation, Policies & Regulations:**

Federal Computer Fraud and Abuse Act 1986 (US) 18 USC 1030

State Penal Code Sections: 1191-1209.5; 13848-13848.7; 186-186.8; 639-653.1; 422; and 484-502.9

MPC Electronic Mail Policy

**4. Rights:**

These computer systems, facilities, and accounts are owned and operated by MPC. MPC reserves all rights, including termination of service without notice, to the computing resources that it owns and operates. These procedures shall not be construed as a waiver of any rights of MPC, nor shall they conflict with applicable law.

**5. Authorized Use:**

Access and privileges on MPC's computing systems are assigned and managed by the administrator of the specific system. Eligible individuals may become authorized users of the system and be granted appropriate access and privileges by following the approval steps prescribed for that system. All access to MPC's computer resources, including issuing of

passwords, must be approved by an authorized MPC agent. Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others without written permission from the system's administrator. The authorized user is responsible for the proper use of the system, including any password protection.

## **6. Permissible Use:**

Electronic communications facilities (such as e-mail) are for college-related activities only. Further, users are responsible for maintaining the following:

- 6.1 An environment in which access to all of MPC's computing resources are equitably shared between users. The system administrator will set minimum guidelines within which users must conduct their activities.
- 6.2 An environment conducive to learning:
  - 6.2.1 Many of the MPC computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that MPC does not assume responsibility for the contents of any of these outside networks.
  - 6.2.2 The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through MPC's systems.
  - 6.2.3 The user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through specific individual networks.
  - 6.2.4 The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origin, the person who performed the transmission will be solely accountable for the message, not MPC, which is acting solely as the information carrier.
- 6.3 Any user who finds a possible security lapse on any system is obligated to report it to the system administrator. The system must not be used until the system administrator has investigated the problem.

Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of

computing resources for which proper authorization has not been given.

## 7. **Prohibited Uses:**

Use of any and all of MPC's computer systems for any of the following purposes is strictly prohibited. Liability for violations of prohibited uses shall remain solely and exclusively with the user. By using MPC's computer systems, the user further agrees to indemnify MPC for any liability incurred by MPC for misuse of the user.

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these privileges. Such suspected violations will be confidentially reported to the appropriate system administrator.

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of computer use privileges, dismissal from the college, and legal action. Violations of some of the above policies may constitute criminal offenses.

The user agrees never to use the system to perform an illegal or malicious act as set forth in this section. Any attempt to increase the level of access to which the user is authorized or any attempt to deprive other authorized users of resources or access to any MPC computer system shall be regarded as malicious and may be treated as an illegal act.

### 7.1 Copyright Infringement:

Computer software protected by copyright cannot be copied from, into, or by using campus computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

### 7.2 Defamation--Libel/Slander:

Creation or transmission of any false statement that tends to cause injury to one's reputation is strictly prohibited. Any user creating or transmitting defamatory statements shall have sole liability for any damages resulting from such defamatory statement. Users will also be subject to MPC's disciplinary procedures set forth in this policy. The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately

misleading (except for those outside services which may conceal identities as part of the service).

7.3 **Obscene Material:**

Creating, transmitting, uploading, or downloading obscene materials is a strictly prohibited use of MPC computer systems. "Obscene matter" means matter, taken as a whole, the predominant appeal of which to the average person, applying contemporary statewide standards, is to prurient interest, meaning a shameful or morbid interest in nudity, sex, or excretion; and is matter which, taken as a whole, goes substantially beyond customary limits of candor in description or representation of such matters; and is matter which taken as a whole lacks significant literary, artistic, political, educational, or scientific value. Any user violating this provision may be subject to applicable criminal and civil penalties. Civil liability shall be solely and exclusively with the user.

7.4 **Commercial Use:**

Commercial use of MPC computer systems is prohibited.

**8. Accounts:**

An account assigned to an individual must not be used by others without written permission of the system administrator. The individual is responsible for the proper use of the account, including password protection.

**9. Confidentiality:**

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. MPC reserves the right to access all information stored in MPC computers. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to ensure the privacy of the user's files. However, if policy violations are discovered, they will be reported immediately to the appropriate system administrator.

The system has the ability to read mail: individual accounts and the system administrator account. All reasonable attempts have been made to ensure the privacy of accounts and electronic mail; this is no guarantee that accounts or electronic mail is private.

**10. System Performance:**

No one should deliberately attempt to degrade the performance of the computer system or to deprive authorized personnel of resources or access to any college computer system.

**11. Unauthorized Access:**

Loopholes in computer security systems or knowledge of a special password shall not be used to damage the computer system, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

**12. Additional Guidelines:**

MPC retains the right to revoke, amend, or change the provisions of this Policy. The system administrator will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowing connect time and disk space, handling of e-mail mail that can not be retrieved, assigning responsibility for account approval and other items related to administering the system.

*Approved by the Monterey Peninsula College Governing Board  
December 15, 1999*