Administration

Administrative Rules and Procedures

2311 Computer Use

The computing facilities of the Chabot-Las Positas Community College District are provided for the use of students, faculty, and staff in support of the programs of the Colleges and District. In order to facilitate proper and responsible use of computers, the following administrative rules and procedures are established for all users. Instructors, managers, departments, or colleges may elect to impose additional requirements or restrictions.

Beyond the consequences listed herein, rule violations may have consequences determined by District Board policy and applicable law.

1. **Proper Use**

   a. Board Policy 2311 specifies that the computer systems of the District are provided solely for the following purposes:

      1) use by authorized employees and agents of the Chabot-Las Positas Community College District for District business;

      2) use by authorized employees of the Chabot-Las Positas Community College District for professional activities related to the employee's job function, or

      3) use by registered students or authorized employees of the Chabot-Las Positas Community College District for instructional activities; or

      4) public access to approved District or College information resources via the public telephone and data networks.

   b. Use of District computer resources for personal or recreational purposes is prohibited. Prohibited activities include, but are not limited to, the following examples:

      - storing personal recipes
      - balancing your personal checkbook

- preparing a homeowner's association newsletter
- playing any sort of computer games unless the games are a specific component of an instructional activity or assignment.

c. Use of District computer resources for personal gain, profit, or commercial purposes is prohibited. Prohibited activities include, but are not limited to, the following examples:

- consulting for profit
- typing services for profit
- maintaining commercial business records
- developing software for sale, except as permitted in Board Policy pertaining to intellectual property rights
- any activity which is not District business or a professional activity related to the employee's job function.

d. Use of District computer resources for unauthorized activities is prohibited. Unauthorized activities include, but shall not be limited to, the following examples:

- use of passwords or accounts of another user
- attempts to capture or "crack" passwords
- attempts to break encryption protocols
- attempts to use loopholes in computer security or special passwords to gain access to systems, obtain extra resources, or make unauthorized use of systems
- destruction or unauthorized alteration of data belonging to the District or to another user
- creation or communication of "viruses", "worms", or "Trojan horses"
- acts that restrict access to the system or damage the system
- acts that deliberately misrepresent the identity of the source of a message
- acts that harass, threaten, or defame other persons
- acts that violate any law

2. **Copyrights and Licenses**

a. The District acquires a substantial portion of its computer software from vendors under license agreements which restrict the use of the software to specific computer systems and which require the District to limit the use and copying of the software. Board Policy 2311 requires compliance with the terms of these licenses and with copyright law.

Use of District computer resources in violation of copyright restrictions or software license terms is prohibited under Board Policy 2311. Prohibited activities include, but shall not be limited to, the following examples:

- copying District-licensed software in violation of the license terms or copyright law
- installing software on District computers in violation of the license terms or copyright law
- "giving" District software to students or colleagues

b. Each major organization shall be responsible for implementation of this policy: For computer software used on College computers, the College Presidents shall be responsible for establishing implementation procedures. For computer software used on District-organizational unit computers, the Chief Management Information Officer shall be responsible for establishing implementation procedures.

3. **System Access**

a. **Administrative Systems**. The District's administrative systems are operated by MIS. Access to these systems requires MIS approval of a written request prepared by the employee's supervisor or manager. In addition, other administrative review is sometimes required. For example, the Controller will review the need for Finance System access. Usually, requests will be approved for staff who have specific

administrative responsibilities requiring system access. Administrative responsibilities that require system access include, but are not limited to, the following examples:

- management or overseeing of department or area budgets
- management of financial records of special projects or grants
- data entry of information pertaining to students, personnel, or finance records
- student information inquiry by counselors or A&R staff

Administrative system users shall access only those system accounts authorized by MIS. All other access to administrative systems is prohibited.

Administrative system users may not, under any circumstances, transfer or confer their system access privileges to another individual or permit use of their assigned system accounts by another individual. Users will be held responsible for all administrative system transactions conducted under their login passwords.

Administrative system users will be granted access privileges only if they agree in writing to adhere to the rules and procedures presented in this section. System access privileges may be revoked without notice in response to violations of these rules and procedures or in response to legitimate requests from the employee's supervisor or manager.

b. **Instructional Systems**. The District's instructional systems are owned and operated by the Colleges. (The sole exception is the instructional Sequent computer, which is operated by MIS.) Access and privileges for these systems are assigned by the systems administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed by the College for that system.

4. **Passwords**

   a. Passwords are the keys to system security, and they provide the most important defense against unauthorized use of District systems. Each system user is responsible to

      - follow certain rules when creating passwords
      - select passwords that are secure
      - change login passwords periodically
      - keep passwords secret

      Users shall fulfill these responsibilities in conformity with established CLPCCD Password Guidelines.

   b. Users of a terminal or PC that is logged in to an administrative system must not leave it unattended. Users will be held responsible for all system transactions conducted under their login passwords.

5. **Ownership**

   a. The District's computer systems, including hardware, software, and all computerized information and data are owned by the District or are licensed from vendors under license agreements. Except as provided in Board Policy pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to the information they contain, even if the employee or student entered the information into these systems. Employees may use this information only as directed in the legitimate business of the Colleges and District and only as prescribed by Board Policy 5511.

6. **Electronic Mail Privacy**

   a. Under Board Policy 2311, the District's electronic mail system and messages are owned by the District and provided for legitimate business use by its employees.

b. The District's E-mail system uses encrypted messages and is relatively secure. It is contrary to MIS department policy for MIS staff to snoop or routinely examine the contents of employee E-mail, and most E-mail messages will enjoy private status.

Nevertheless, E-mail messages are not guaranteed to be private or confidential, and the District accepts no responsibility for consequences that might arise from disclosure of an E-mail message. Please remember that control over a message is lost once it is sent, and future events may have unanticipated results:

- The recipient of the message might forward it to others on the system.
- The recipient of the message might print it and hand it to another reader or might even post it on the wall.
- The message might accidentally be sent to an unintended recipient, especially when using named Groups for the "TO" address.
- In unusual circumstances, MIS staff might need to examine mail in order to resolve a system problem.
- Conceivably, one or more messages might be subpoenaed in a legal proceeding, and then MIS would be required to provide the subpoenaed material.

The bottom line: E-mail is not guaranteed to be private or confidential. MIS encourages users to draft E-mail messages thoughtfully, assuming they might be viewed by unanticipated readers. It's best to treat them as any other written document.

7. **Etiquette**

Users are expected to use the system in a manner that reflects respect for other users.

a. It is a violation of system etiquette to transmit material which is offensive, harassing, or needlessly affects the work of other users.

b. Please carefully consider the appropriateness of any E-mail message being sent to EVERYONE; notification of the arrival of such a message will interrupt every user on the system and consume a portion of their system resources. Such messages are sometimes perceived as the electronic equivalent of "junk mail".

c. Mail messages composed in all capitals are difficult to read and are often perceived as the electronic equivalent of "SHOUTING". Please use such messages sparingly.

8. **Nondiscrimination**

a. All users have the right to be free from any conduct associated with the use of District computer systems which discriminates against any person on the basis of race, color, national origin, gender, or disability. Users of District systems shall refrain from such discriminatory acts.

b. Discriminatory conduct includes, but is not limited to, written or graphic conduct that satisfies both of the following conditions: (a) harasses, denigrates, or shows hostility to or aversion toward an individual or group based on race, color, national origin, gender, or disability, and (b) has the purpose or effect of creating a hostile, intimidating, or offensive educational environment.

1) "Harassing conduct" includes, but is not limited to, epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts, that relate to race, color, national origin, gender, or disability. This includes acts that purport to be "jokes" or "pranks" but that are hostile or demeaning.

2) A "hostile educational environment" is established when harassing conduct is sufficiently severe, pervasive, or persistent so as to interfere with or limit the ability of an individual to participate in or benefit from District computing systems.

c. Any user who believes he or she has be subject to conduct associated with the use of District computer systems which discriminates on the basis of race, color, national origin, gender, or disability may report the incident to the College or District Affirmative Action / Harassment Officer.

9. **Management Rights and Responsibilities**

a. **Administrative Systems** Managers shall make written requests for employees' access to the District's administrative systems. In addition, to maintain system security, managers shall notify MIS in writing immediately when system access is no longer required or authorized for an employee.

Managers shall be responsible to provide general supervision of departmental employees' adherence to the rules and procedures presented herein, and managers shall have the right to impose additional departmental rules or procedures. In the event of conflict, the rules and procedures presented herein shall take precedence over departmental rules and procedures.

b. **Instructional Systems** Managers responsible for instructional computing facilities shall be responsible to provide general supervision of staff and students' adherence to the rules and procedures presented herein, and managers shall have the right to impose additional departmental rules or procedures. Under the general direction of College management, the systems administrators of the College instructional systems may develop more detailed guidelines, as needed, concerning administration and daily operation of these systems. In the event of conflict, the rules and procedures presented herein shall take precedence over departmental rules and procedures.

10. **MIS Staff Rights and Responsibilities**

a. In the normal course of systems administration, the MIS staff occasionally may need to examine files, electronic mail, and printer output in order to gather sufficient information to diagnose and correct system problems or perform technical maintenance. In the course of this work, the staff reserves the right to inspect, copy, remove, or otherwise alter any data, file, or system resources which may adversely affect the system without notice to the user. In addition, the MIS staff reserves the right to restrict system access of any user who violates the rules/procedures presented in this section.

b. Although MIS staff have the right to examine any system files, they also have a responsibility to maintain users' privacy to the maximum extent possible.

11. **User Rights and Responsibilities**

a. As described herein, users of District systems have the right to

- use District systems as authorized
- own information stored on District systems solely as provided in Board policy pertaining to intellectual property rights
- be free of routine intrusions on privacy
- be free of discrimination in use of District systems.

b. As described herein, users of District systems have the responsibility to:

- use the systems in compliance with the rules and procedures presented in this section
- make proper use of District systems
- comply with copyright law
- access systems only as authorized
- keep passwords secret and maintain password security

- use the system with proper etiquette and respect for other users
- refrain from acts that are discriminatory, defamatory, harassing, or illegal
- agree that the District is not responsible for the content of external networks and for actions by individual users of the systems in violation of these rules.

12. **Agreement and Disclaimers**

By using District computer systems, users agree to the following conditions:

a. Users agree that they understand and will comply with the rules and procedures presented in this section.

b. The District disclaims responsibility for actions by individual users in violation of these rules and procedures, and users accept this disclaimer. Any user who harasses others or makes defamatory or derogatory remarks or misrepresents the identity of the source of a message is in violation of the rules and procedures of this section and shall bear sole and full responsibility for these actions. Users agree that the District or College's role in managing the computer systems used is solely as an information carrier, and that they will never consider transmission though the system as an endorsement of said transmission by the District or College.

c. The District disclaims responsibility for the content of external networks, and users accept this disclaimer. Many of the District's computing systems provide access to outside networks which furnish electronic mail, information services, bulletin boards, news groups, conferences, etc. Users are advised that the District does not assume responsibility for the content of any of these outside networks.