ADMINISTRATIVE REGULATION 4000.2

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

HUMAN RESOURCES

ELECTRONIC COMMUNICATIONS

This administrative regulation is intended to inform all users (employees, students and guests) of the South Orange County Community College District of the rules regarding use of the District's digital information network. The digital information network consists of District owned equipment such as computers, computer networks, electronic mail and voice mail systems, internet services, audio and video conferencing, and related electronic peripherals like cellular telephones, modems and facsimile machines.

The digital information network is owned by the District and is to be used for District-related activities only. If District employees, students or guests interface personally-owned equipment with the District network, they will be required to adhere to District policies and regulations.

I. PERMITTED USES OF THE DISTRICT'S DIGITAL INFORMATION NETWORK

Use of the digital information network is intended to enhance the availability of educational materials and opportunities for employees, students and guests. Therefore, students and faculty may only use the network for educational and work-related purposes. Guests in the Saddleback and Irvine Valley College Libraries may use the system on a limited basis with specific prior authorization from library staff and for educational and/or work related purposes only. Guests must present identification to library staff for authorization and guest usage must not preclude student use.

1. Guests and students are permitted access through open workstations provided by the District at multiple locations, including both campuses, and in classroom/laboratory environments.

    - An electronic verification (signature) to acknowledge this policy will be required at each log-in.

2. Employees are provided access through the above, or through assigned District-owned computers.

    - An electronic verification (signature) to acknowledge this policy will be required at each log-in.

3. Connection of privately owned computer equipment to campus wireless network is permitted.

- An electronic verification (signature) to acknowledge this policy will be required at each log-in.

4. Connection of privately owned computer equipment to the network by physical (cable) is permitted when authorized by an administrator of one of the technology organizations at the colleges or the District to ensure compatibility of equipment.

    - Such authorizations will be in written form issued by a systems administrator indicating the person(s) is/are authorized to use personal equipment, and other relevant network information assigned to the equipment in order to enable use on the network.

II. USER RESPONSIBILITIES

Users shall not access information contained in restricted data bases, files, and information banks, without permission from authorized District staff.

Personal passwords/account codes will be created and issued to users to protect employees and students. Users agree to represent themselves according to their true and accurate identities in all electronic messages, files, and transactions. These passwords/account codes shall not be shared with others, nor shall employees or students use another party's password/account code except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords and account codes protects employees and students from wrongful accusation of misuse of electronic resources. If a communication is authored out of a password-protected system, the presumption will be that the owner of the password authored it

Users have no right to privacy in any material on the network and/or e-mail system. The District reserves the right to monitor network and e-mail use for any business reason, including for the purpose of determining whether a violation of Board policy, administrative regulation, or law has occurred, and reserves the right to remove any materials or information found to be in violation of Board policy, administrative regulation, or law. In addition, the District must perform necessary maintenance of the digital information network which may also require access to information in user files, or files in the system which contains personal data.

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11

III. PROHIBITED USES

Use of the digital information network is a privilege and not a right of any employee, or student member, and that privilege may be modified or revoked at any time by the District for violation of District policy or administrative regulations, or any violation of law.

The Vice Chancellor of Technology and Learning Services, applicable Academic Administrator, or designee shall take action with regard to any activity by users which is inconsistent with the permitted uses under this regulation and/or board policy. Prohibited uses which will result in revocation of user privileges and may result in additional action being taken by the District as necessary and appropriate include, but are not limited to, the following:

1. Communicating any information concerning any password, user account, personal identification number or confidential information protected by law without the permission of its owner or the controlling authority of the computer facility to which it belongs.

2. Forgery of messages and/or alteration of system and/or user data used to identify the sender of messages.

3. Using District communication systems to solicit or conduct non-work related business.

4. Fundraising of any kind, except fundraising by faculty or staff that is work related.

5. Retrieving, viewing, or disseminating any material in violation of any federal or state regulation or District policy. This can include, but is not limited to, improper use of copyrighted material and improper use of passwords or access codes.

6. Damage, theft, or alteration of system hardware or software.

7. Disconnecting or otherwise tampering with District owned computers or network equipment and connections.

8. Connecting privately owned computers or other network capable devices to the network without appropriate authorization as specified from the system administrator.

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11

9. Using any device to monitor, discover, or otherwise ascertain (i.e. "sniffing" or "hacking") information regarding network operations not intended for public knowledge or consumption.

10. Placement of unlawful information, computer viruses, or harmful programs on~~,~~ or through the computer system.

11. Entry into restricted information on systems or network files in violation of password/account code restrictions.

12. Interfering with the rights of others to use the District's systems.

13. Displaying images or audio that is obscene, sexually harassing or otherwise violates the District rules prohibiting harassment.

14. Violating any laws, including but not limited to copyright laws or laws regarding obscenity, or participating in the commission or furtherance of any crime or unlawful activity.

15. Unsolicited email, social networking, streaming audio, streaming video, or multi-player games impose a substantial burden on the system, and are not allowed, with the exception of those services that serve educational or work-related purposes.

16. For Students - Use of the network in furtherance of any violation of the Student Code of Conduct.

17. For Employees - Use of the network in furtherance of any violation of applicable District policies or administrative regulations.

18. Employees or students may not use copyrighted materials without the permission of the copyright holder. The connections represented by the Internet allow users to access a wide variety of media. Even though it is possible to download most of these materials, users shall not create or maintain archived copies of these materials unless the materials are in the public domain, e.g., freeware, shareware, etc.

IV. INCIDENTAL PERSONAL USE

Users of a district electronic communications system may use the system for incidental personal purposes for short periods of time, usually consisting of a few minutes per day, provided that such use does not:

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11

a) directly or indirectly interfere with the District's operation of electronic communications resources;

b) interfere with the user's employment or other obligations of the District;

c) burden the District with incremental costs; or

d) violate any of the specific uses described in Paragraph III.

The District is not responsible for any loss or damage incurred by an individual as a result of personal use of District electronic communications resources.

V. ENFORCING THIS REGULATION

Due to the open and decentralized design of the Internet and the digital information network, the District cannot protect individuals against receipt of material that may be offensive to them. Likewise, individuals who use email, or those who disclose private information about themselves on the Internet or across the digital information network, should know that the District cannot protect them from invasions of privacy by third parties or other users.

The Vice President of Student Services will determine violations by students, the Vice Chancellor of Technology and Learning Services will determine violations by District employees, the Director of Information Technology will determine violations by College employees, and the Dean of Library and Learning Resources will determine violations by guests. These administrators may with the approval of the Chancellor name designees who will perform these functions.

District employees and other users may informally resolve unintentional or isolated minor violations of use policies.

1. Student Violations - Individuals may report a suspected violation of this regulation or board policy by a student to the supervisor of the library/laboratory. In turn, the library/laboratory supervisor will contact the Vice President of Student Services or appropriate designee (the "Administrator"). The Administrator shall determine whether a violation of this regulation or of board policy has occurred. If the Administrator determines that a violation has occurred, the Administrator may take action to suspend or revoke the use's privileges as set forth in Section V(C) (4) of this Regulation (see below).

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11

Thereafter, the Administrator may also submit the matter to the appropriate District department for a determination of whether additional action should be taken. Possible sanctions include the deletion of materials found to be in violation of this regulation or of board policy, loss of user privileges, student discipline, and other sanctions available within the judicial processes.

2. Employee Violations - Individuals may report a suspected violation of this regulation or board policy by District employees to their supervisor. In turn, the supervisor will notify the appropriate Academic Administrator (Vice Chancellor of Technology and Learning Services) for district employees, Director of Information Technology for college employees or their designee (the "Administrator"). The Administrator shall then determine whether a violation of this regulation or board policy has occurred. If the Administrator determines that a violation has occurred, the Administrator may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the Administrator will provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the action taken. The Administrator may also submit the matter to the appropriate academic or classified staff supervisor or administrator for a determination of whether disciplinary action should be taken pursuant to established District collective bargaining agreements, District policies, administrative regulations, and/or other applicable laws, rules, or procedures.

3. Guest Violations - Individuals may report a suspected violation of this regulation or board policy by a guest to the supervisor of the library/laboratory. In turn, the library/laboratory supervisor will notify the Dean of Library and Learning Resources or designee (the "Administrator"). The Administrator shall then determine whether a violation of this regulation or of board policy has occurred. If the Administrator determines that a violation has occurred, the Administrator may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the Administrator will provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the action taken. If requested by the user, the Administrator will meet with the user within five business days. The Administrator may also submit the matter to the College President for a determination of whether additional action should be taken. Possible sanctions include the deletion of the materials found to be in violation of this regulation or board policy, loss of user privileges, and other sanctions available within the judicial processes.

4. Appeals – Students may appeal imposition of discipline for violation of this policy under the procedures set forth in Administrative Regulation 5401 for student discipline generally. Students may appeal revocation of privileges with

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11

regard to the system pursuant to the procedures set forth in subsection V(C)(5) below. Employees may appeal imposition of discipline and revocation of any privileges pursuant to the procedures under the District's personnel policies and any applicable collective bargaining agreements.

5. Revocation for Students – Repeated violation of this policy by a student will results in revocation of the student's access to the electronic communications network for a period not exceeding six months, in addition to any other discipline. Students will be provided three (3) days notice of a decision to revoke privileges. The Administrator will prepare the notice, which will include a statement of the reasons for revocation, of why the action is necessary to enforce the administrative Regulation or other rules or laws, and of the student's rights under this section. A student may appeal the decision by submitting a request in writing to the Dean of Student Services within five (5) days of notice of intent to revoke, and this action will temporarily suspend the proposed revocation. The petition will be reviewed by the Dean of Students Services of a designee who will conduct a conference if requested by the students and will issue a final decision within five (5) days of receipt of the petition, at which point privileges may be revoked. Following the conference, the student may within five (5) days demand a hearing challenging the revocation.
The hearing and any appeal from it will be conducted by the Disciplinary Panel pursuant to Administrative Regulation 5401. Part V, but subject to the time limits set forth here. The Notice provided in Part A.A will be provided as soon as practicable. The hearing will commence within three (3) days of the student's demand or a longer period of up to fifteen (15) days later if the student requests. The panel conducting the hearing on behalf of the College will reach a final decision within three (3) days after the conclusion of the hearing. The panel will issue a written decision explaining the evidence and the basis for its decision. Following exercise of any appeal rights pursuant to Administrative Regulation 5401, Part V, and the decision will be final. The student should contact the District within five (5) days thereafter if he or she intends to request judicial review.

The student may waive the preliminary conference and proceed directly to a Disciplinary Hearing by providing notice to the Dean of Student Services.

The administration may immediately revoke a student's access to the electronic communications network in compelling circumstances, including to prevent the commission of illegal acts, to prevent harm to person or property, to prevent loss of significant evidence, or if the student continues willfully to refuse to abide by the District's policy. The student may challenge immediate revocation pursuant to the foregoing procedures.

Adopted: 9-16-97
Revised: 8-30-99
Revised: 5-19-03
Revised: 4-28-08
Revised: 5-23-11