SAN BERNARDINO COMMUNITY COLLEGE DISTRICT (REVISED)
ADMINISTRATIVE REGULATION **3720**

COMPUTER AND NETWORK USE

Purpose: The San Bernardino Community College District ("District") owns and operates a variety of computer and communication systems, including voicemail, electronic mail (e-mail), telephone, and access to the Internet, which are provided for the use of District faculty, administrators, staff, and students in support of the programs of the Colleges and District. Here after, this system and all of its component parts shall be referred to as the "District Network." This network establishes a communications platform that often substitutes for in-person meetings regarding District business.

The *Computer and Network Use: Rights and Responsibilities* Policy ("the Policy") applies to all members of the District community using the District Network including faculty, administrators, staff, students, independent contractors, and authorized guests. The Policy covers use of computer equipment and communication systems at any District facility in computer labs, classrooms, offices, libraries and the use of the District servers and networks from any location. If any provision of this policy is found to be legally invalid it shall not affect other provisions of the policy as long as they can be effective without the invalid provision.

Ownership Rights

The Policy is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, and all hardware and software components within it, is the sole property of the District which sets the terms and conditions of its use consistent with the law. Except as provided in Board Policy or collective bargaining agreements pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the District Network.

Privacy Interests

The District recognizes the privacy interests of faculty and staff and their rights to freedom of speech, participatory governance, and academic freedom as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users anticipate. In addition, the District Network can be subject to authorized and unauthorized access by both internal and external users.

For these reasons there are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the District Network is not to be relied upon as confidential or private. Nonetheless, the District seeks to afford email communications privacy protections comparable to those it traditionally affords paper mail and telephone communications.

District Rights

System administrators may access user files or suspend services they manage without notice: 1) to protect the integrity of computer systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; or 4) when it is reasonable to believe that violations of law or District policy or procedures have occurred. For example, system administrators, following organizational guidelines, may access or examine individual files or accounts based on suspicion that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board policy. Such data or information may also be used as grounds for appropriate personnel action.

User Rights

While the District monitors electronic usage as part of its normal network operating procedures, the District does not routinely inspect or monitor users' computer hardware or files, email, and/or telephone message system, nor disclose information created or stored in such media without the user's consent. The District shall

attempt to notify users before accessing computer hardware and files or prior to suspending service. In the event that the District acts without user consent, under its District Rights specified above, the District shall do so with the least perusal of contents and the least action necessary to resolve the immediate situation. When the District accesses files without user consent, it shall notify the user as soon as possible of its access and provide the reason for its action.

User Responsibilities

The Board recognizes that computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources and observe all relevant law, regulations, and contractual obligations.

For District employees the intended uses of the District Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional activities. Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities provided that such use is within reason and provided that such usage is ordinarily on an employee's own time, is occasional, and does not interfere with or burden the District's operation.

"Unauthorized uses" include prohibited uses and any other use for a prohibited purpose, including illegal activities, messages which may constitute discrimination or harassment under state or federal law, or anything that interferes with the intended use. These types of prohibited uses and purposes are further defined in Administrative Regulation 3720.

All users of the District Network must read, understand, and comply with this Administrative Regulation, and any additional guidelines established by the District. Such guidelines will be reviewed by the District and may become subject to Board approval as a District policy or procedure. By using any part of the District Network, users agree that they will comply with this Policy.

Copies of this Policy can be found in the policies section of the College Catalogues, Schedule of Classes, Student Handbooks, Faculty Handbooks, New Classified Employee Handbook, and the Handbook for New Administrators. Copies of this Policy are also available in the District Human Resources Office, the Office of the Presidents (Crafton Hills College and San Bernardino Valley College), the Office of the Vice-Presidents of Instruction, Student Services, and Administrative Services (Crafton Hills College and San Bernardino Valley College), and on the District's Web site at http://www.sbccd.org.

Abuse of computing, networking or information resources contained in or part of the District Network may result in the loss of computing privileges. Additionally, abuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable District or college policies, procedures, or collective bargaining agreements. Complaints alleging abuse of the District Network will be directed to those responsible for taking appropriate disciplinary action. Illegal reproduction of material protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment. Examples of behaviors constituting abuse which violate District Board Policy 3720 include, but are not limited to, the following activities:

System abuse

- Using a computer account that one is not authorized to use.
- Obtaining a password for a computer account that one is not authorized to have.
- Using the District Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly 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.
- Knowingly or carelessly allowing someone else to use your account who engages in any misuse in violation of Board Policy 3720 or of this Administrative Regulation.
- Forging e-mail messages.
- Attempting to circumvent data protection schemes or uncover or exploit security loopholes.
- Masking the identity of an account or machine.
- Deliberately wasting computing resources.
- Downloading, displaying, uploading, or transmitting obscenity or pornography, as legally defined.
- Attempting without District authorization to monitor or tamper with another user's electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal under California Computer Crime Laws.
- Personal use which is excessive or interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the Network.

Harassment

- Using the telephone, e-mail or voice mail to harass or threaten others.
- Knowingly downloading, displaying, or transmitting by use of the District Network, communications, pictures, drawings, or depictions that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious, or political belief.
- Knowingly downloading, displaying, or transmitting by use of the District Network sexually explicit images, messages, pictures, or cartoons when done to harass or for the purposes of harassment.
- Knowingly downloading, displaying, or transmitting by use of the District Network sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.
- Posting on electronic bulletin boards material that violates existing laws or the colleges' Codes of Conduct.
- Using the District Network to publish false or defamatory information about another person.

Commercial use

- Using the District Network for any commercial activity, without written authorization from the District. "Commercial activity" means for financial remuneration or designed to lead to financial remuneration.

Copyright

- Violating terms of applicable software licensing agreements or copyright laws.
- Publishing copyrighted material without the consent of the owner on District Web sites in violation of copyright laws.

Exceptions
Activities by technical staff, as authorized by appropriate District or college officials, to take action for security, enforcement, technical support, troubleshooting, or performance testing purposes will not be considered abuse of the Network**.**

Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities and will take no disciplinary action provided that such use is within reason and provided that such usage is ordinarily on an employee's own time; is occasional and does not interfere with or burden the District's operation. Likewise, the District will not purposefully surveil or punish reasonable use of the network for union business-related communication between employees and their unions.

Complaints
A user who asserts that the District or District personnel have violated this policy shall file a complaint with his or her immediate supervisor with a copy to the Vice Chancellor of Human Resources, and a copy to the employee's bargaining unit. The supervisor shall notify the supervisor of the alleged violator to discuss the complaint. The supervisor of the complainant shall initiate an investigation if necessary and determine an appropriate remedy/resolution in consultation with the Vice Chancellor of Human Resources. In cases where the supervisor is part of the complaint, the complaint shall be filed with the next level of supervision for investigation and resolution and/or remedy. The complainant shall be informed in writing 1) of the initiation of the investigation, and 2) of its outcome as appropriate, with copies to the Vice Chancellor of Human Resources and the employee's bargaining unit. Complainants dissatisfied with the resolution/remedy have full recourse to relevant contractual protections and/or legal action.

Enforcement of the Policy
The Board directs the Chancellor or designee to enforce all existing federal and state laws and District and college policies, including not only those laws and regulations that are specific to computers and networks but also those that apply generally to personal conduct. Violations of this Policy will be dealt with in the same manner as violations of other District policies or standards of behavior and may result in disciplinary action, subject to applicable due process requirements.

Users who believe this policy has been misinterpreted or misapplied may file a complaint in accordance with the Complaint Procedures found in *Administrative Regulation 3720*.

Students who do not observe the requirements of this Policy may be in violation of the Student Code of Conduct and subject to student discipline.

This Policy and Administrative Regulation 3720 shall be distributed to all new and existing employees. Nothing in this policy should be construed to interfere with First Amendment rights or with the academic freedom of faculty as outlined in Board Policy 4030.

Reference:
Education Code: §70902
Adopted: 07/12//01
Amended: