

SIERRA COLLEGE

ADMINISTRATIVE PROCEDURE No. AP 3720

Computer and Network Use

Date Adopted: 10/29/2002

Date Revised: 5/7/2007

Date Reviewed: 5/7/2007

References: 17 United States Code Section 101 et seq.; Cal. Const., Art. 1 Section 1; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45; Government Code Section 3543.1(b); Penal Code Section 502

Sierra Joint Community College District (“the District”) respects the individual privacy rights of its users. However, users cannot expect privacy rights to extend to work-related conduct or the use of college-owned equipment or supplies.

The term “users,” as used in this policy, refers to all employees, students, and, with the District’s permission, independent contractors and other persons or entities accessing or using the District’s computer and telecommunication resources and services.

- *District’s Right to Access Information:* Although users have individual access codes to voice mail, e-mail and computer network systems, these systems are accessible at all times by the College and may be subject to periodic inspections by the College for College/business purposes.
- *Systems Use Restricted to College Business:* Users are expected to use the telephone system, e-mail, voice mail, and computer network systems primarily for College or District business and not for personal purposes. Personal purposes include, but are not limited to, soliciting for commercial ventures, religious or political causes, outside organizations, or other similar non-job-related purposes.
- *Disruptive or Offensive Practices:* Users are prohibited from using the District’s information systems in any way that may be disruptive or offensive to others, including, but not limited to, the intentional transmission of sexually explicit messages, graphics, cartoons, ethnic or racial slurs, or anything that

may be construed as harassment or disparagement of others. This is consistent with the District's non-discrimination policy.

- *Unauthorized Use of Access Codes:* Users are prohibited from the unauthorized use of the access code of other users to gain access to computer resources and voice mail messages.
- *Intellectual Property:* Users must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property.
- *Unlawful Material:* Fraudulent, harassing, embarrassing, indecent, profane, obscene, intimidating or other unlawful material may not be sent by e-mail or other forms of electronic communication or displayed on or stored in the District's computers. Users encountering or receiving such material should immediately report the incident to their supervisor, instructor or other administrator.
- *View of E-mail by Others:* Users should use the same care in drafting e-mail and other electronic documents as they would for any other written communication. Anything created on the computer may, and likely will, be viewed by others.
- *Installation of software:* Users may not install software onto District computers or the network without first receiving authorization to do so from the system manager or designee, or for the purposes of conducting Sierra College business within the framework of one's job description.
- *Altering/Copying/Reading Files:* Users should not alter or copy a file belonging to another user without first obtaining permission from the owner of the file. The ability to read, alter or copy a file belonging to another user does not imply permission to read, alter, or copy that file.
- *Commercial/Personal Use:* The computer and telecommunication resources and services of the District may not be used for the transmission or storage of commercial, political, or personal advertisements, solicitations and promotions, destructive programs (viruses and/or self-replicating code), or political material, or any other unauthorized use.
- *Passwords:* Users are responsible for safeguarding their passwords for the system. Individual passwords should not be given to others. Users are responsible for all transactions made using their passwords.
- *Connection to Other Computer Systems:* A user's ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

Potential Discipline: Violation of this policy may result in disciplinary action up to and including termination or expulsion.

See Board Policy 3720.