Sierra College
ADMINISTRATIVE PROCEDURE    AP 3720

Computer and Network Use

Date Adopted: 10/29/2002
Date Revised: 5/13/2016
Date Reviewed: 5/13/2016
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

The District Computer and Network systems are the sole property of the Sierra Joint Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

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. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes personal computers, workstations, mobile devices, mainframes, minicomputers, data network and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

- Conditions of Use: Individual units within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure but may provide additional detail, guidelines, or restrictions, and would need approval from the Chief Technology Officer (or designee).
• **Legal Process:** This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies will be subject to disciplinary action up to and including but not limited to loss of information resources privileges; disciplinary suspension or termination from employment or expulsion; or civil or criminal legal action.

• **Integrity of Information Resources:** Computer users must respect the integrity of computer-based information resources.

• **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. Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District will exercise this right only for legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

• **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 Programs:** Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

• **Unauthorized Use of Access Codes:** Users are prohibited from the unauthorized use of the access code of other users to gain access to computer or information resources and must not assist any other persons to gain unauthorized access.
• **Intellectual Property:** Users must comply with all software licenses, copyrights, other on-line information and all other state and federal laws governing intellectual property.

• **Unlawful Material:** Fraudulent, defamatory, harassing, embarrassing, indecent, profane, obscene, threatening, intimidating or other unlawful material that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information 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 Information 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 due to the possibility of unintended disclosure of communications.

• **Information Belonging to Others:** Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

• **Rights of Individuals:** Users must not release any individual’s (student, faculty, or staff) personal information to anyone without proper authorization.

• **User identification:** Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

• **Installation of software:** Users may not install software onto District computers or the network without first receiving authorization to do so from the designated IIT 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.

• **Copying:** Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law. The number of simultaneous users does not exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract.

• **Copyrights:** Computer users must respect copyrights and licenses to software and other on-line information. In addition to software, all other copyrighted information
(text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

- **Political, Personal, and Commercial Use:** The District is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

- **Political Use:** District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

- **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. Users also are reminded that the “.cc” and “.edu” domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within those domains.

- **Nondiscrimination:** All users have the right to be free from any conduct connected with the use of District network and computer resources which discriminates against any person on the basis of Board Policy 3410 & Administrative Procedure 3410 on nondiscrimination. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

- **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 and may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

- **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.

- **Modification or Removal of Equipment:** Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

- **Unauthorized Use:** Computer users must not interfere with others access and use of the District computers, intentionally develop or use programs which disrupt other
computer users, or which access private or restricted portions of the system, or which
damage the software or hardware components of the system. This includes but is not
limited to: the sending of chain letters or excessive messages, either locally or off-
campus; printing excess copies of documents, files, data, or programs; running
grossly inefficient programs when efficient alternatives are known by the user to be
available; using programs or utilities that interfere with other computer users, modify
normally protected or restricted portions of the system or user accounts, unauthorized
modification of system facilities, operating systems, or disk partitions; attempting to
crash or tie up a District computer or network; and damaging or vandalizing District
computing facilities, equipment, software or computer files.

- **Abuse of Computing Privileges:** Users of District information resources must not
access computers, computer software, computer data, or information, or networks
without proper authorization, or intentionally enable others to do so, regardless of
whether the computer, software, data, information, or network in question is owned
by the District. For example, abuse of the networks to which the District belongs or
the computers at other sites connected to those networks will be treated as an abuse of
District computing privileges.

- **Reporting Problems:** Any defects discovered in system accounting or system
security/password violation must be reported promptly to the IIT Helpdesk so that
steps can be taken to investigate and solve the problem.

- **Usage:** Computer users must respect the rights of other computer users. Attempts to
circumvent these mechanisms in order to gain unauthorized access to the system or to
another person’s information are a violation of District procedure and may violate
applicable law.

- **Possibility of Disclosure:** Users must be aware of the possibility of unintended
disclosure of communications.

- **Retrieval:** It is possible for information entered on or transmitted via computer and
communications systems to be retrieved, even if a user has deleted such information.

- **Public Records:** The California Public Records Act (Government Code Sections
6250 et seq.) includes computer transmissions in the definition of “public record” and
nonexempt communications made on the District network and computer must be
disclosed if requested by a member of the public.

- **Litigation:** Computer transmissions and electronically stored information may be
discernable in litigation.

- **Dissemination and User Acknowledgment:** All users shall be provided copies of these
procedures and be directed to familiarize themselves with them, as per the Computer
Use Ethics Account Request Form signed by any and all authorized District computer
users.
Potential Discipline: Violation of this policy may result in disciplinary action up to and including termination or expulsion.

See Board Policy 3720.