Sierra College
ADMINISTRATIVE PROCEDURE AP 3720

Computer and Network Use

Date Adopted:	10/29/2002
Date Revised:	12/12/2025
Date Reviewed:	12/12/2025
References	Government Code Section 3543.1(b); Penal Code Section 502; Cal. Const., Art. 1 Section 1; 15 U.S. Code Sections 6801 et seq.; 17 U.S. Code Section 101 et seq.; 16 Code of Federal Regulations Parts 314.1 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

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.

This procedure applies to all District students, faculty, and staff and to others granted use of District information resources. 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.

- *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; removal, suspension or expulsion of students; or civil or criminal legal action as determined appropriate by the District.

- *Copyrights and Licenses*: Computer users must respect copyrights and licenses to software and other on-line information.

- *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.

- *Number of Simultaneous Users:* The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

- *Copyrights:* 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.

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

- *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.

- *Connection to Other Computer* S*ystems:* 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.

- *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.

- *Unauthorized Use*: Computer users must not interfere with others access and use of the District computers. 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; 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.

- *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 action liability.

- *Unauthorized Access:* Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

- *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.

- *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 must be reported promptly to the Information Technology Services (ITS) Service Desk at servicedesk@sierracollege.edu or (916) 660-7777 so that steps can be taken to investigate and solve the problem.

- *Password Protection:* A computer user who has been authorized to use a password-protected account may be subject to discipline, as well as 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.

- *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.

- *Unlawful Messages:* Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

- *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.

- *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.

- *Commercial Usage:* Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use below). Some public discussion groups have been designated for selling items and may be used appropriately, according to the stated purpose of the group.

- *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.

- *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 District policies and federal, state, or other applicable laws.

- *Personal Use:* District information resources should not be used for personal activities not related to District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time.

- *Commercial Use:* District information resources should not be used for commercial purposes. Users are also 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 the Sierra Joint Community College District network and computer resources which discriminates against any person on the basis of Board Policy 3410 and 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.

- *No Expectation of Privacy:* The District reserves the right to monitor all use of the District network and computers to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of District network and computer resources including in the content of their communications using such 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.

- *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 7920.000 et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network or computer must be disclosed if requested by a member of the public. This includes emails and other communications using District information resources.

- *Litigation*: Computer transmissions and electronically stored information may be discoverable 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.

Title IV Information Security Compliance

The District shall develop, implement and maintain an information security program in compliance with the Gramm-Leach-Bliley Act which will include:

- A designated employee or employees to coordinate the District's information security program.

- Identification of reasonably foreseeable internal and external risks to security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

  At a minimum, such a risk assessment should include consideration of risks in each relevant area of the District's operations, including:
  1) Employee training and management;
  2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
  3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

- Design and implementation of information safeguards to control the risks the District identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of safeguards' key controls, systems, and procedures.

- Oversee services providers, by:
  1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
  2) Requiring the District's service providers by contract to implement and maintain such safeguards.

- Evaluate and adjust the District's information security program in light of the results of the testing and monitoring required; any material changes to the District's operations or business arrangements; or any other circumstances that the District knows or has reason to know may have a material impact on the District's information security program.

See Board Policy 3720.