AP 3720 Computer and Network Use

References:

15 U.S. Code Sections 6801 et seq.;
17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1
Section 1; Government Code Section 3543.1(b);
16 Code of Federal Regulations Part 314.1 et seq;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45
Education Code Section 70902

The District Computer and Network systems are the sole property of *the Santa Clarita Community College District*. The Computer and Network systems are for District instructional and work-related purposes only. Any person without proper authorization of the District may not use these resources.

This procedure applies to all District students, faculty, staff, administrators, and to others granted use of District information resources (referred to hereafter as users). 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, mainframes, minicomputers, and associated peripherals, websites and electronic mail, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

Conditions of Use
Information Technology may define additional conditions of use for District information resources. These statements must be consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Legal Process
This procedure exists within the framework of other District Board Policies and state and federal laws. However, this procedure is not intended to restrict the academic freedom of the faculty as stated in other District Board policies. A user of District information resources who is found to have violated any of these procedures will be subject to loss of information resources privileges and possible disciplinary action as described in Board Policy 7360 (Academic Employees), 7365 (Classified Employees), 5530 (Student), and their associated Administrative Procedures and/or civil or criminal legal action.

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.

- **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 proceedings.

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.

- **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 appropriate system administrator 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 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.

U**sage**

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.

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

- **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, and 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 unless anonymous communications are expressly permitted or solicited in writing or through the provision of an anonymous response option.

- **Accurate Information** – Users shall not knowingly post on the District's Web server or distribute by any other electronic means information that the user knows to be inaccurate or in violation of other Board policies or District procedures.

- **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.

- **Personal Use** - District information resources should not be used for personal activities not related to appropriate District functions, except in a purely incidental manner.

- **Commercial Use** - District information resources should not be used for commercial purposes. Users also are reminded that the domains registered by the District on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within those domains.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of *the Santa Clarita Community College District* network and computer resources which discriminates against any person in accordance with the District's Board Policy and Administrative Procedure on Non-Discrimination (BP/AP 3410) 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 policy, District procedure state law, or federal law regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

Disclosure and Compliance

No Expectation of Privacy - Users should be aware that although the District does not routinely inspect or monitor User's assigned electronic resources, Users have no expectation of privacy in the use of the District's network and computer resources apart from the conditions expressed in this procedure or provided by law. The District reserves the right to maintain and monitor District network and computer resources to ensure integrity, performance, security, and compliance with this procedure. When there is a "reasonable suspicion" of a violation of the law, Board Policy, or Administrative Procedures, the District may access a User's electronic resources without consent for legitimate, legal District investigations or other purposes. Access shall be limited in scope to meet a specific objective and conducted only by those with knowledge of the technical, responsible, legal, and ethical implications of gathering User information for the intended purpose. The District shall not access cameras and/or microphones embedded or connected to District-issued equipment without the permission of the User.

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 discoverable in litigation.

Notification - When practical, the District will attempt to notify or gain consent from Users if their District resources are intended to be accessed. Users should not expect notification when performing maintenance or updates whereby a User's electronic files are not reviewed for their content, during a confidential investigation, when notification is not permissible during litigation, or if the user is not the primary subject of a Public Records Act request.

Title IV Information Security Compliance

The District shall develop 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 entity's information security program.

- Identification of reasonably foreseeable internal and external risks to the 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 entity'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 entity identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

- Oversee service 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 entity's service providers by contract to implement and maintain such safeguards.

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

Dissemination and User Acknowledgment
All users shall be provided copies of these procedures and be directed to familiarize themselves with them. All users will be asked to sign or electronically accept the following statement acknowledging their responsibilities under Board Policy 3720.

I understand that I have been granted access to the District's Information Technology resources and may have access to confidential information. I agree to abide by the standards set forth in this procedure and I am aware that violations of the Board Policy on Computer and Network Usage (Board Policy 3720) may subject me to disciplinary action.

Furthermore, all faculty, staff and administrative users of the District information system will be presented with the following statement when logging into the system:

CONFIDENTIALITY STATEMENT

State and federal law protect the confidentiality of student, employee, and application records.I understand that all records accessed are confidential and subject to all policies and state or federal laws.

I agree that I will not access any information unless authorized to do so.

I agree that I will maintain the confidentiality of information in compliance with college policies and state and federal laws, both during and after employment.

I understand that if I fail to abide by these conditions, I may be subject to formal disciplinary action up to and including, loss of information resource privileges, disciplinary suspension or termination from employment, and/or civil or criminal legal action.

I understand that by proceeding into the College of the Canyons College software system, I agree to comply with this statement.

Revised 12/02, 5/03, 11/14, 5/15

Reviewed: 06/24/15
Reviewed and Endorsed by CPC: 12-1-20
Next Review Date: 2026