

**Administrative Procedure**  
Chapter 3 – General Institution

## **AP 3720 Technology Acceptable 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 subdivision (b);
- 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 San Mateo County 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, mainframes, minicomputers, 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 or expulsion; 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. Computer users may not attempt to gain access to another computer user's SMCCD technology or to attempt access by using another User's login name or password.

**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.

**Commercial Usage** - Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below).

**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 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 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 the San Mateo County Community College District network and computer resources which discriminates against any person on the basis of categories delineated in BP 3410 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.

### **DISCLOSURE**

**No Expectation of Privacy** - The District reserves the right to monitor all use of the District network and computer to assure compliance with these policies. 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.

**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 7920.7931et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network or computers must be disclosed if requested by a member of the public.

**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. We will also deliver a copy of this electronically via email & knowBe4 platform.

Users receiving a copy electronically will have an acknowledgment and waiver included in this procedure stating that they have read and understand this procedure and will comply with it. This acknowledgment and waiver shall be in the form as follows:

### **Technology Acceptable Use Policy**

I acknowledge that I have received and read a copy of the Acceptable Use Policy. I understand the guidelines outlined and agree to comply with the Computer and Network Usage Procedures for the duration of my employment or enrollment.

I am aware that any violations of these procedures may result in disciplinary action, including but not limited to revocation of my network access and potential legal consequences under applicable State or Federal law.

**[A dedicated URL (smccd.edu/cnupform) will be required to post the form and provide a link.]**

### **Title IV Information Security Compliance**

- 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.

### **Access to District Email**

Human Resources or Managers with the rank of Dean or higher are permitted to direct Information Technology Services to disable a subordinate's email account.

Managers with the rank of Vice President or higher are permitted to access a subordinate's email account provided, however, that Information Technology Services is able to confirm the authority to access an account consistent with Board Policy 2.34 "Computer and Network Use."

All employees who are in good standing at the time of their last active day of employment shall have the right to:

- a) retain use of their "smccd.edu" email address until 5pm of the last day of employment;
- b) ITS will disable the account & reset the password for the sole purpose of sending out an out of office reply message with updated contact information.

Employees who are not in good standing shall have their access to the "smccd.edu" email address disabled immediately following their last active day of employment.

Employees who have been discovered to be engaged in malicious behavior or determined to be a threat to the security of the resources maintained by Information Technology Services may have the "smccd.edu" email disabled immediately with no advance notification.

Any disputes concerning the application of this Administrative Procedure shall be resolved by the Vice Chancellor, Human Resources and Employee Relations.

*Also see BP 3720 Computer and Network Use, BP/AP 3725 Information and Communications Technology Accessibility & Acceptable Use, and AP 6365 Contracts – Accessibility of Information Technology.*

---

**Approved:**10/14

Revised:

*(Replaces former SMCCCD AP 2.35.1)*