Administrative Regulation
Chapter 3 – General Institution

AR 3720 COMPUTER AND NETWORK USE

Purpose
The Santa Monica Community College District provides a wide array of technology resources to staff, students, and faculty. These resources are intended to advance the educational, scholarly, and service missions of the District. This document describes the general regulations covering the use of technology computing facilities which are under the direction of Santa Monica College Information Technology (IT) department and its staff.

Technology computing resources are a limited and finite resource that each and every user needs to respect. Every user is expected to use the technology resources in a manner which does not infringe upon use of those facilities by other people and which does not waste either "soft" resources (e.g., computer time) or "hard'' resources (e.g., paper, disk space, documentation materials). The guidelines discussed here are intended to insure that the security of the system is protected consistent with the user's right to privacy and fair share of available resources.

Users agree to read and abide by this regulation. The Vice President responsible for Information Technology or designee is responsible for providing interpretation, which will be modified periodically in light of experience gained and legal and administrative developments that occur.

System Security

1. The District will seek to maintain system security, but users should not assume that information in their accounts, or on District-owned or -administered computers they use, is private. Authorized District personnel may obtain access to computing and networking resources only as necessary to service the computing system, retrieve or modify District work, and to investigate suspected security violations of this policy, including unlawful activity. Files will be disclosed to third parties as required by law. Users will be notified of such access whenever possible.

    a. The District cannot and does not guarantee the confidentiality of electronic information. In addition to accidental and intentional breaches of security, the District may be compelled to disclose electronic information as required by law.

    b. As part of its necessary routine operations, the District occasionally gains access to network accounts and other computing services it makes directly or indirectly available to the campus community. Suspected security violations discovered during such routine operations will be reported to the Vice President responsible for Information Technology or designee and/or law enforcement officials. All other information accessed during such routine operations will be treated as confidential, except as otherwise required by this policy or law.

    c. Unless otherwise prohibited by law, and subject to legal requirements, the District and law enforcement personnel may access computers, network accounts, or any other electronic information or technology necessary to investigate suspected violations of this policy or unlawful activity.

    d. Users will relinquish access to computing and network resources upon permanent separation from the District.

e. The District and the IT staff will seek to maintain system security, but users should not assume that their accounts or the files or information they store on or their use of District-owned or –administered computers will remain private. Users should not assume their email messages are private communications, nor that their use of technology resources will not be monitored as part of the District's routine operations. As all electronic mail is a form of public record, users should have no expectation of privacy in their use of electronic mail, as the IT department may regularly choose to inspect, disclose, retain or dispose of electronic correspondence as part of the District's routine operations.

f. The IT department will make reasonable efforts to maintain the security of account names, numbers, passwords, directories and files. However, no computer system is completely secure. Even with all the safeguards taken by the District to control privacy and security, it may still be possible for some user to gain access to another user's accounts through actions or accidents beyond any reasonable control. As a result, each user must take full advantage of password and file protection security mechanisms provided by their computer and its operating system.

g. Users agree not to violate system security; maliciously interfere with system performance or another user's use of the system; or access network accounts, files, or passwords intentionally and without authorization.

2. Users may not intentionally send email or develop other electronic information inaccurately attributed to another person.

3. No computers or network accounts shall be used for unlawful purposes, or in violation of district policies or procedures.

Appropriate and Inappropriate Use

1. It is impossible to provide an exhaustive definition of inappropriate computer use, or a complete set of examples to cover every conceivable situation. Users who have questions about which computer uses are appropriate and which are not should inquire about their intended use by contacting the IT department.

   Without limitation, the following examples shall be construed by all of the campus community as examples of inappropriate use of technology resources:

   - users shall not interfere with system performance or another user's use of the system
   - users shall not disclose their passwords or lend their account to any other individual, apart from IT staff
   - users shall not gain access to accounts, files, passwords or resources intentionally and without authorization of the account holder
   - users shall not use technology resources for non-District fundraising or commercial purposes.
   - users shall not use technology resources for any activities which violate state or federal laws. Computing resources may not be used to intimidate, threaten or harass individuals, or violate the college's policies concerning relationships between college constituencies. Such activities include, but are not limited to, using computing resources to store, print, or send obscene, slanderous, or threatening messages.

Users may use their computers and network accounts for non-District matters except as otherwise prohibited by this or other District policy or where such use unreasonably interferes with academic uses, job performance or system performance/operations. Such use is subject to the terms of this policy including, without limitation, terms regarding access to information on District computers and accounts.

a. Any and all information maintained on District-owned computers/network accounts, whether District-related or not, is accessible by the District. Other than to perform routine operations or as may be legally required, the District will not monitor accounts or access the information stored in computers/network accounts without the user's consent unless such action is necessary to enforce the board policy and this administrative regulation.

b. Employees are strongly encouraged to remove any "personal" information they may have stored on their computers/network accounts prior to ending their relationship with the District. The District may

destroy information left on computers/network accounts. Information will be retained if retention is in the District's best interest. If the District extends an individual's account access beyond the employment separation date, the account is not subject to this provision until the extension has ended.

Process for Suspension and Termination of Use

Users understand that violation of this regulation may result in suspension or termination of computer, network account and other access and, depending upon the circumstances, may result in disciplinary action. Violations will be processed through normal District channels. If the activity is also unlawful, it may result in criminal and/or civil prosecution.

1. **Emergency Suspensions**

   a. In the event of a perceived emergency or where other exigent circumstances demand immediate action, the Vice President responsible for Information Technology or designee may immediately suspend computing privileges and notice will be given to the user as soon as reasonably possible.

   b. The District may temporarily suspend a user's computing privileges for security or other administrative reasons. Computing privileges suspended pursuant to this provision will be restored as soon as the threat or concern has been addressed or within three business days, whichever is shorter. Accounts that are suspended for more than three days will be handled as outlined below, irrespective of whether disciplinary action has been initiated. Absent extenuating circumstances, no account may be suspended pursuant to this policy for more than 10 business days, unless the disciplinary process has been invoked.

2. **Non-Emergency Suspensions and Terminations**

   a. In non-emergency situations, the Vice President responsible for Information Technology or designee will provide the user with notice of the perceived problem and an opportunity to be heard before privileges are suspended.

   b. A suspension may be appealed in writing to the Vice President of Human Resources or designee within three business days of the effective date of the suspension. The Vice President of Human Resources or designee will provide a written decision to the Vice President responsible for Information Technology and the user within five business days of receipt of the appeal. The Vice President of Human Resources' or designee's decision will remain in effect pending final resolution of the disciplinary proceeding.

   c. Suspected violations by District employees will be reported to the employee's supervisor and handled through established channels for disciplinary action.

   d. Pending resolution of the disciplinary process, the Vice President responsible for Information Technology or designee may suspend District computing privileges if the alleged violation is reasonably perceived to constitute unlawful activity, pose a substantial risk to the integrity of campus computing or present an imminent threat to the safety or welfare of the campus or members of the college community.

   e. Sanctions for violations of this regulation will be imposed by the administrative official with final responsibility for resolution of the disciplinary process in use, following consultation with the Vice President responsible for Information Technology in the event that sanctions involve campus computing services. Sanctions with respect to campus computing services may include, but are not limited to, suspension or permanent revocation of computing privileges. The District reserves the right to seek restitution and/or indemnification from an employee for damages arising from violations of this regulation. In addition, the District and/or third parties may pursue criminal and/or civil prosecution for violations of law.

Personal Responsibility

1. As a representative of the District, users must accept personal responsibility for reporting any misuse of the network to relevant IT staff. This includes, but is not limited to, users who suspect that their District-provided computers or network accounts have been accessed without their permission. These users are expected to change their password as soon as it is reasonably possible to do so and to report the suspected activity to relevant IT staff.

2. Users are responsible for all use of computers and network accounts provided to them by the District, including backup of files on their District-provided computer and password maintenance.

    a. Responsible use includes using passwords that are not easily deduced by others. On a regular basis and in accordance with the current security practices of the computing industry, IT staff may require users to change their passwords.

    b. Voluntary unauthorized disclosure of a password may result in suspension, revocation and/or denial of computing privileges. Disclosure of passwords to Information Technology (IT) staff or other District system administrators is considered authorized disclosure.

    c. District-provided network accounts may only be used by the user to whom they are assigned unless otherwise authorized by the District. Access to computers and network accounts for maintenance/service purposes by persons responsible for systems and IT is considered authorized; users are not responsible for actions taken by these persons.

    d. Users who suspect that their District-provided computers or network accounts have been accessed without their permission are responsible for changing their passwords and are strongly encouraged to report the suspected activity to IT.

    e. Users are responsible for actions of others who use their network accounts with their permission.

    f. Users are responsible for logging off and for protecting their private account.

Users gain access to computer systems by being assigned an account on the college's computer network. Possession of an account may allow its owner to access various systems, databases, student records, websites and use peripheral devices such as printers. Each employee member is assigned an account for his/her use in their professional activities.

This regulation is governed by Article 27, Computer and Network Use, in the District/Faculty Collective Bargaining Agreement.

Also see BP/AR 3710 Securing of Copyright and AR 3750 Use of Copyrighted Material.

Computer Hardware and Software

1. Software may not be used on equipment controlled by the Santa Monica Community College District unless the software falls into one of the following categories:

   A. The software has been purchased by the District in sufficient quantities to account for one purchase for each machine on which the software is used and a written record of the purchase is available in district files.

   B. The software is covered by a licensing agreement with the software author, vendor, or developer, as applicable, and no tenets of the agreement have been violated by the user and a written copy of the agreement is available in district files.

   C. The software has been donated to the District and a written record of the donation or its acceptance is available in district files.

   D. The software has been developed or written by a District employee for use on District equipment and full credit has been given to the developer by other users.

   E. The software is in the public domain and documentation exists to substantiate its public domain status.

   F. The software is being reviewed or demonstrated as part of a purchasing or licensing decision and arrangements for such review or demonstration have been satisfactorily reached between the District and the appropriate vendor or representative.

2. Any software that is personal property of the user shall not be installed, used or maintained on computers owned by the District. The District is not accountable for unauthorized installation of personal software on District computers.

3. No person shall make, cause to be made, use, or cause to be used on the District's computer facilities an illegal copy of copyrighted or licensed software. An illegal copy is defined as any copy which violates the tenets of Public Law 96-517, Section 7(b) which amended Section 117 of Title 17 of the United States Code.

   According to this law, all copies are illegal unless they fall into one of the following categories:

   A. The copy is created as an essential step in the utilization of the computer program in conjunction with a machine and it is used in no other manner.

   B. The copy is for archival purposes only and all archival copies are destroyed when continued possession of the computer program ceases to be rightful.

Telecommunications

The Telecommunications department provides the voice and data communications infrastructure to campus through the delivery of cost-effective, state-of-the-art technology and services. The department also provides installation, repair and maintenance services for personal computers and related equipment.

Accessibility Standards for Electronic and Information Technology - Section 508

Electronic and information technologies (EIT) are a significant means by which Santa Monica Community College District provides information to students, faculty, staff and other constituents. The need to ensure accessibility to all members of the campus community becomes critical as more administrative services and learning environments are based on EIT. It is also a part of the district's ongoing commitment to establishing a barrier free learning community, or universal access, to all qualified individuals.

Individuals with disabilities are guaranteed access to educational institutions and systems of communication under the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990. Amendments to Section 508 of the Rehabilitation Act clarify accessibility requirements for EIT developed, procured, maintained, or used by federal agencies.

The technical standards of Section 508 provide criteria specific to the following technologies:

Software Applications and Operating Systems (36 Code of Federal Regulations, Part 1194.21)
Web-based Intranet and Internet Information and Applications (36 Code of Federal Regulations, Part 1194.22)
Telecommunications Products (36 Code of Federal Regulations, Part 1194.23)
Video and Multimedia Products (36 Code of Federal Regulations, Part 1194.24)
Self-Contained, Closed Products (36 Code of Federal Regulations, Part 1194.25)
Desktop and Portable Computers (36 Code of Federal Regulations, Part 1194.26)
Functional Performance Criteria (36 Code of Federal Regulations, Part 1194.31)

Furthermore, California Government Code Section 11135 states the following:

1) In order to improve accessibility of existing technology, and therefore increase the successful employment of individuals with disabilities, particularly blind and visually impaired and deaf and hard-of-hearing persons, state governmental entities, in developing, procuring, maintaining, or using electronic or information technology, either indirectly or through the use of state funds by other entities, shall comply with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S. Code Section 794d), and regulations implementing that act as set forth in Part 1194 of Title 36 of the Code of Federal Regulations.

2) Any entity that contracts with a state or local entity subject to this section for the provision of electronic or information technology or for the provision of related services shall agree to respond to, and resolve any complaint regarding accessibility of its products or services that is brought to the attention of the entity.

As mandated by federal and state laws and the California Community Colleges Chancellor's Office it is necessary that Santa Monica Community College District comply with Section 508 Standards to ensure accessibility to EIT for individuals with disabilities. The Board directs the Superintendent/President or designee to enforce compliance with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S. Code Section 794d) and its implementing regulations set forth at Title 36 Code of Federal Regulations Part 1194.

Also see AR 6365 Contracts – Accessibility of Information Technology.

Responsible Use of Computer Resources

As a condition of using the District's computer resources, all student users (hereinafter "users") must sign the written "Acceptable Use Agreement" referred to in this Regulation. This agreement states that the user has read the Regulation and agrees to responsible usage of computer resources as defined in this Regulation. Also, any additional guidelines established by the administrators of each system shall be adhered to. Such guidelines will be periodically reviewed by the Information Services Committee and may become subject to Board approval as a District Regulation or procedure. Use of the District's computer resources in violation of this Regulation is prohibited, and can result in revocation of a user's access to the District's computer resources, student disciplinary action, consistent with established Board Policies, Administrative Regulations, applicable statutes and a referral for prosecution to other entities for violation of federal, state and/or local laws and regulations.

1. Definition of Terms

Administrative Officer: Employee of SMC with supervisory responsibility over a unit of the College which operates Information Resources.

Computer Account: The combination of a user number, user name, or user identification and a password that allows an individual access to a mainframe computer or some other shared computer or network.

Computer Resources: The sum total of all computers, workstations, mainframes, software, cabling, peripherals, networks, accounts, passwords, ID numbers, and data owned or leased by SMC.

Data Owner: The individual or department that can authorize access to information, data or software and that is responsible for the integrity and accuracy of that information, data, or software. The data owner can be the author of the information, data or software or can be the individual or department that has negotiated a license for SMC's use of the information, data or software.

Information Resources: In the context of this Regulation, this phrase refers to data or information and the software and hardware that makes that data or information available to users.

Mainframe Computers: "Central" computers capable of use by several people at once.

Network: A group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.

Normal Resource Limits: The amount of disk space, memory, printing, etc., allocated to your computer account by that computer's system administrator.

Peripherals: Special-purpose devices attached to a computer or computer network. For example, printers, scanners, plotters, etc.

Project Director: Person charged with administering a group of computer accounts and the computing resources used by the people using those computer accounts.

Server: A computer that contains information shared by other computers on a network.

Software: Programs, data, or information stored on magnetic media (tapes, disks, diskettes, cassettes, CDs, etc.) Usually used to refer to computer programs.

System Administrator: Staff employed by SMC whose responsibilities include system, site, or network administration and staff employed by SMC departments whose duties include system, site, or network administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If you have a computer on your desk, you may be acting, in whole or in part, as that computer's system administrator.

User: Any student who does not have system administrator responsibilities for a computer system or network but who makes use of that computer system or network. A user is still responsible for his/her use of the computer and for learning proper data management strategies.

2. Regulation Coverage

A. Privileges

1) Computers and networks provide access to resources as well as the ability to communicate with others worldwide. Access to SMC computing resources is a revocable privilege which requires that users act responsibly and in a manner consistent with the provisions of this Regulation. Individuals must respect the rights of other users, respect the integrity of the systems they are using, and observe all relevant laws and regulations.

2) Users do not own accounts on SMC computers, but rather are granted the use of such accounts. The District owns the account and grants individuals the privilege of using it.

3) All enrolled students may apply for user IDs to utilize e-mail and Internet and intranet services offered by the District. Such an application may be granted only if the applicant signs the Acceptable Use Agreement referred to herein. Users who have had their privileges revoked or suspended may not apply for a user ID during the term of such revocation or suspension.

4) SMC computers and networks are to be used for District-related research, instruction, learning, distribution of scholarly information, and administrative activities. Such uses shall be consistent with, and limited by the activities set forth in Section 2(B)(3) [Appropriate Use] of this Regulation. Users are required to use the District's computer resources, including hardware, software, networks, and computer accounts in accordance with this Regulation and in respect of the rights of other computer resource users. District computer resources are not available and shall not be used for purposes specified in section 2(C) of this Regulation [Inappropriate Use.]

5) Users shall not attempt to modify any system or network or attempt to crash or hack into District systems. They shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Nor shall users attempt to remove existing software or add their own personal software to District computers and systems unless properly authorized.

6) Users shall use only their own designated computer accounts. Users are required to keep all ID's, passwords, and account information confidential, and shall take reasonable precautions to prevent others from obtaining this information. It is recommended that users change their passwords periodically to prevent unauthorized use of their account. Accounts are not transferable, and users shall not allow others to use their own account. Users will be responsible for any use of their accounts by others to whom access has been given.
Users shall not use another individual's ID, password or account. Users shall respect the privacy and personal rights of others, and are prohibited from accessing or copying another user's e-mail, data, or other files without the prior express consent of that user. Users shall send e-mail only from their own personal e-mail addresses. Users are prohibited from concealing or misrepresenting their identity while using the District's computer resources.

7) Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions and applicable college regulations. Users are required to abide by all applicable copyright and trademark laws, and to abide by all licensing agreements and restrictions. Users shall not copy, transfer, or utilize any software or electronic materials in violation of such copyright, trademark and/or licensing agreements. The copying of software that has not been placed in the public domain and distributed as "freeware" is expressly prohibited by this Regulation. Users who access, copy, transfer and/or use "shareware" are expected to abide by the requirements of the shareware licensing agreement. No user may inspect, change, alter, copy or distribute proprietary data, programs, files, disks or software without proper authority.

8) The conventions of courtesy and etiquette which govern vocal and written communications shall extend to electronic communications as well. Fraudulent, harassing, threatening, or obscene messages (as those terms are defined in Section 2.5.2.1.1 of this Regulation) and/or other materials must not be transmitted through the District's computer resources.

9) Expected Privacy
The District's computer resources and all users' accounts are the property of the District. There is no right to privacy in the use of the computer resources or users' accounts, and the District reserves the right to monitor and access information on the system and in users' accounts for the purpose of determining whether a violation of this Regulation has occurred. The District will remove any information on the system that it determines to be in violation of this Regulation.

Users must understand the weak privacy afforded by electronic data storage and electronic mail in general, and apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including e-mail, that is transmitted over the District's computer resources and/or the Internet is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information which is intended to be confidential should not be sent through the District's computer resources.

In addition, users should be aware that the District may access information contained on its computer resources under numerous circumstances, including, but not limited to, the following

a) Under the California Public Records Act (CPRA), electronic files are treated in the same way as paper files. Public documents are subject to inspection through CPRA. In responding to a request for information under the CPRA, the District may access and provide such data without the knowledge or consent of the user.
b) The District will cooperate appropriately, upon the advice of District Legal Counsel, with any local, state or federal officials investigating an alleged crime committed by an individual affiliated with a District computer resource, and may release information to such officials without the knowledge or consent of the user.
c) The contents of electronic messages may be viewed by a system administrator in the course of routine maintenance, or as needed for District administrative purposes, including investigation of possible violations of this Regulation.
d) In addition, electronic mail systems store messages in files (e.g. the file containing a user's inbound mail.) These files are copied to tape in the course of system backups. The contents of these files and the copies on system backup tapes are subject to disclosure as stated in the preceding paragraphs.

10) Receipt of Offensive Material

Due to the open and decentralized design of the Internet and networked computer systems of the District, the District cannot protect individuals against the receipt of material that may be offensive to them. Those who use the District's computer resources are warned that they may receive materials that are offensive to them. Likewise, individuals who use e-mail or those who disclose private information about themselves on the Internet or on District computer resources should know that the District cannot protect them from invasions of privacy

B. Ethical Standards

Supporting the District's stated mission to "promote creativity, collaboration and the free exchange of ideas in an open, caring community of learners" (SMC Mission Statement), the District's networked computing facilities and systems offer powerful tools for open learning and exchange of ideas. However, with power comes responsibility and ethical obligation. If this electronic medium of exchange is to function well and support "an open, caring community of learners," its users need to agree to and abide by ethical standards of online behavior that assure all users fair, equitable, effective and efficient access and use. Such ethical standards include but are not limited to:

1) Honesty:

a) Users agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.
b) While using college computing facilities and systems, users agree to behave within the standards described in the college's Code of Academic Conduct, especially those standards describing academic honesty and campus safety. These standards regarding plagiarism or collusion on assignments apply to course work completed with computers just as they do to other types of course work.

2) Respect:

a) Legal and ethical limitations on the use of District computer resources.
In using the District's computer resources, users must communicate in the same manner as is expected in the classroom or on campus. The distance provided by electronic communications does not create a forum in which there are no ethical or legal limitations. Users shall not use District computer resources in any unlawful manner, including, but not limited to, attempting to defraud another, threatening physical harm to another, procuring or distributing obscene material in any form, or unlawfully harassing another.

While the District recognizes and respects users' rights to freedom of speech, such rights are not absolute. Speech which is fraudulent, libelous, obscene, harassing, or threatening is not permitted under state or federal law. Users are expressly prohibited from using the District's computer resources to engage in such conduct. Users violating this section will be subject to revocation of their user accounts, and will be further subject to student/staff disciplinary action, and, in appropriate circumstances, a referral for prosecution for the violation of criminal laws.

For purposes of this Regulation, the terms fraud and libel are given their legal meaning as developed by the courts of this State and of the United States. "Obscenity" means words, images, or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value. "Threatening" means communications which result in an individual being fearful of imminent bodily harm and/or emotional/mental disruption of his/her daily life. "Harassing" means to engage in a knowing and willful course of conduct directed at another which seriously alarms, annoys or harasses another, and which serves no legitimate purpose. In addition, "Harassment" shall also mean to subject another to unwelcome sexual advances, requests for sexual favors, and other verbal, visual or physical conduct of a sexual nature as set forth in California Education Code Section 212.5.

- For the privacy, integrity and ownership of others' electronic files, documents and materials.

- For the access rights of others.

- For the rights of others to an educational environment free of any form of harassment.

b) For the integrity and content of college electronic documents, records or identification issued or posted online by faculty, staff or administrators.

c) For the rights of others over the integrity of their intellectual property and to the fruits of their intellectual labor.

d) For the access and security procedures and systems established to ensure the security, integrity and operational functionality of the college computing facilities and systems for the entire college community.

3) Appropriate Uses of College Computer Resources

The college's computing facilities and network systems exist to support the instructional, cultural, research, professional and administrative activities of the college community. In general, the same guidelines that apply to the use of all college facilities apply to the use of college computing resources. All users are required to behave in a responsible, ethical and legal manner as defined by this Regulation and other existing college regulations and guidelines. The following sections broadly define appropriate and inappropriate use.

a) Appropriate use

Activities deemed to be appropriate uses of Santa Monica College computing resources include but are not necessarily limited to:

b) Educational Use

Carrying out SMC course assignments and activities requiring access to and use of campus computing facilities and systems, including:

- Authorized access to and use of computer programs licensed by SMC available on stand-alone and networked computing stations.
- Authorized access to lab and campus networks to perform and complete required course work for SMC courses in which the user is currently enrolled.
- User access to authorized SMC student e-mail accounts.
- Independent study and research.
- Users agree to follow acceptable use regulations established by individual computing labs and network systems and to obey directives issued by authorized District personnel supervising such labs and systems.

C. Inappropriate Use

Use of District's computer resources for purposes other than those identified in section 3.1 is not permitted. Users are specifically prohibited from using the District's computer resources in any manner identified in this section, as identified in the following subsections. Users who violate this section of the Regulation by engaging in inappropriate use of the District's computer resources shall be subject to the revocation or suspension of user privileges, student disciplinary procedures, and may be subject to criminal or civil sanctions if permitted by law. Inappropriate uses of Santa Monica College computing resources which violate this Regulation include, but are not limited to:

a) Destruction or damage to equipment, software, or data belonging to the college or others

b) Disruption or unauthorized use of accounts, access codes, or identification numbers

c) Use of District computer resources to harass others, as defined in section 2.4.2.1.1 of this Regulation.

d) Use of District computer resources in ways which intentionally or unintentionally impede the computing activities of others are prohibited. Such activities include, but are not limited to, disrupting another's use of computer resources by game-playing; sending an excessive number of messages or e-mail; making or printing excessive copies of documents, files, data, or programs; or introducing computer viruses of any type onto the District's computer resources.

e) Use of the District's computer resources which violates copyrights, trademarks and/or software license agreements

f) Use of the District's computer resources to violate another's privacy, including, but not limited to, accessing or using another user's account, id number, password, electronic files, data or e-mail.

g) Use of the District's computer resources in an effort to violate the District's rules of Student Conduct/Academic Honesty Regulation including, but not limited to, the following types of conduct:
   - Copying a computer file that contains another student's assignment and submitting it as your own work.
   - Copying a computer file that contains another student's assignment and using it as model for your own assignment.
   - Working together on an assignment, sharing the computer files or programs involved, and then submitting individual copies of the assignment as your own individual work.
   - Knowingly allowing another student to copy or use one of your computer files and to submit that file, or a modification thereof, as his or her individual work.
   - Specific examples of inappropriate use of computing resources include but are not limited to:
   - Impersonation of any person or communication under a false or unauthorized name
   - Transmission of any unsolicited advertising, promotional materials or other forms of solicitation
   - Using District resources for commercial purposes or personal financial gain
   - Using District computer resources in any unlawful manner including, but not limited to, attempting to defraud another, threatening physical harm to another, procuring or distributing obscene material in any form, or unlawfully harassing another
   - Inappropriate mass mailing (“spamming” or “mail bombing”)
   - Tampering, or attempting to tamper with any software protection, encryption or restriction placed on computer applications or files.
   - Knowingly or carelessly introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into District computers or networks
   - Attempting to circumvent local or network system security measures
   - Altering or attempting to alter system software or hardware configurations on either network systems or local computing devices.
   - Installing unauthorized software programs on District local computing devices or network systems and/or using such programs.

- Ignoring or disobeying regulations and procedures established for specific computer labs or network systems.
- Copying system files, utilities and applications that expressly belong to the District.

3. Inappropriate Uses of District Computer Resources: Reporting and Consequences

A. Investigating Violations

If District staff or system administrators have information that a violation of this Regulation or any other misuse of computing resources has occurred, and if that information points to the computing activities or the computer files of a student, they have the obligation to pursue any or all of the following steps to protect the user community.

1) Take action to protect the system(s), user jobs, and user files from damage. SMC reserves the right to immediately suspend a user's privilege of access to SMC's computer resources if SMC has any reason to believe that the user has committed a violation of this Regulation.
2) Notify the alleged abuser's supervisor, project director, instructor, academic advisor or administrative officer, as appropriate, of the investigation.
3) Refer the matter for processing through the appropriate District's student disciplinary process if the user's actions are deemed to be in violation of standards of conduct for students.
4) Suspend or restrict the alleged abuser's computing privileges during the investigation and administrative processing.
5) Inspect the alleged abuser's files, diskettes, and/or tapes.
6) Minor infractions of this Regulation or those that appear accidental in nature are typically handled internally by the Director of Network Services in an informal manner by electronic mail or in-person discussions. More serious infractions are handled via the procedures outlined above.
7) Infractions such as harassment, or repeated minor infractions as described in this Regulation may result in the temporary or permanent loss of access privileges, notification of a student's academic advisor and/or Student Conduct Office.
8) More serious infractions, such as unauthorized use of another user's ID and/or account, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of the District's regulations, or repeated violations of minor infractions may result in the temporary or permanent loss of access privileges, and referral for discipline under applicable existing student disciplinary processes.
9) Offenses which are in violation of local, state or federal laws will result in the immediate loss of computing privileges, student discipline, and will be reported to the appropriate law enforcement authorities.

Abuse of computing privileges is subject to disciplinary action as well as loss of computing privileges. An abuser of the District's computing resources may also be liable for civil or criminal prosecution. It should be understood that nothing in this Regulation precludes enforcement under the laws and regulations of the State of California, any municipality or county therein, and/or the United States of America.

4. Procedure for Suspension and/or Revocation of Computer Use Privileges

A. Student Violations

Individuals may report a suspected violation of this Regulation by a student to the College Disciplinarian. The College Disciplinarian shall then determine whether a violation of this Regulation has occurred. If the College Disciplinarian determines that a violation has occurred, he/she may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the College Disciplinarian must provide the user with written notice of the suspension or revocation, and provide a statement of the reasons for the action(s) taken. College Disciplinarian's determination to suspend or revoke a student's user privileges may be appealed pursuant to the appeal procedures set forth in the Student Code of Conduct. Thereafter, the College Disciplinarian may also submit the matter to the Office of Student Affairs for a determination of whether additional action should be taken pursuant to established District student discipline procedures as outlined in the Student Code of Conduct. Possible sanctions include the deletion of materials found to be in violation of this Regulation, loss of computer resource privileges, student expulsion, and other sanctions available within the judicial processes.

References:

Government Code Section 3543.1 subdivision (b);
Penal Code Section 502;
Cal. Const., Art. 1 Section 1;
15 U.S. Code Sections 6801 et seq.;
17 U.S. Code Sections 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

Approved: No Date (for AR 2513 and AR 2514); December 11, 2001 (for AR 4435); March 2004 (for AR 2512); and November 6, 2009 (for AR 2515)
Updated: November 2018; June 2024 (references only)

(Replaces former SMC AR 2512, AR 2513, AR 2514, AR 2515, and 4435)