

<b>COMPUTER TECHNOLOGY AND COMMUNICATIONS RESOURCES USE – FACULTY AND STAFF</b>	<b>2755</b>
---	-------------

It is the policy of the San Luis Obispo County Community College District to maintain access to local, national and international sources of information, to provide an atmosphere that encourages access to knowledge and sharing of information, and to maintain an intellectual environment in which students, staff and faculty may create and collaborate with colleagues at any institution, without fear that the products of their intellectual efforts will be misrepresented, tampered with, destroyed and/or stolen.

The District provides computer technology and communications resources, which are to be used for education, research, academic development, administrative functions, and public service in support of District programs. Faculty and staff are responsible for using technology and resources in an effective, efficient, ethical, and lawful manner.

<b>COMPUTER TECHNOLOGY AND COMMUNICATIONS RESOURCES USE – FACULTY AND STAFF</b>	<b>R2755</b>
---	--------------

This regulation provides for the implementation of Board Policy 2755, Computer Technology and Communications Resources Use - Faculty, Staff, including defining acceptable and prohibited uses. The Vice President, Administrative Services is the administrative officer with responsibility for administering District computer technology and communications resources.

A. Privileges

1. Access to the District's computer technology and communications resources, is a revocable privilege. Individuals may become authorized users of District computer technology and communications resources and may be issued passwords only with the approval of the Vice President, Administrative Services.
2. Individuals may become users of District computer technology and communications resources in accordance with Intellectual Property Rights Board Policy.

A. User Responsibilities

User responsibilities include, but are not limited to:

1. Using only their own designated ID, passwords, and accounts, and keeping IDs, passwords, and account information confidential. It is recommended that users change their passwords periodically.
2. Using software and electronic materials, including shareware, in accordance with copyright, trademark, and licensing agreements and restrictions.
3. Accurately identifying and representing themselves in electronic messages, files, and transactions.

A. Prohibitions

Prohibited uses include, but are not limited to:

1. Damaging equipment, data, software, software protection, encryption or restriction on applications and files; including, introducing invasive or destructive programs (such as viruses, worms, and Trojan Horses).
2. Disrupting or unauthorized use of accounts, access codes, passwords, or identification numbers.
3. Impeding or disrupting the use of computer technology and communications resources by game playing, sending an excessive or unreasonable number of messages, sending messages of unreasonable size (with large attachments); making or printing excessive copies of documents, files, data, or programs.
4. Violating copyrights, trademarks, and/or license agreements.
5. Accessing, using or copying another user's account, ID number, password, electronic files, data, or e-mail without prior authorization; or allowing such use by others.
6. Using District computer technology and communications resources in any unlawful manner including fraudulent, threatening, libelous, obscene, or harassing communications; procuring, or distributing obscene or pornographic material.
7. Circumventing or attempting to circumvent local, network, or remote security measures.
8. Altering or attempting to alter system software.
9. Altering or attempting to alter system hardware without Computer Services approval.
10. Modifying or attempting to crash or hack into computer technology or communications resources.
11. Accessing or attempting to access restricted portions of any operating system or security software unless authorized to do so.
12. Installing or removing software unless authorized to do so.
13. Using computer technology and/or communications resources for private commercial or other personal purposes.
14. Copying software that has not been placed in the public domain and distributed as freeware; inspecting, changing, altering, copying, or distributing proprietary data programs, files, disks, or software without authorization.
15. Falsely identifying and/or representing one's self in the use of computer technology and communications resources.

A. No Expectation of Privacy

1. Users have no expectation of privacy in the use of District computer technology and communications resources. The District reserves the right to access, review and copy, and

disclose any information entered or retained in computer technology and communications resources. The District may delete material, after the user has received reasonable notification of the intent to do so, or after the District has made serious, multiple, attempts to notify.

The District shall exercise this right only for legitimate District purposes including, but not limited to, ensuring the integrity and security of computer technology and communications resources and compliance with use regulations. The District will not engage in routine or random monitoring of these communications.

2. Disclaimer: The District encourages the use of computer resources for development of intellectual property, however, cannot assume the responsibility for distinguishing staff intellectual property from any other data files. Therefore, the district cannot guarantee the safety and security of staff intellectual property stored on the District's computer resources.

It is the District's recommendation that anyone developing intellectual property store that property offsite via electronic data storage medium.

3. During an investigation, the District has unedited, unobstructed access to any and all accounts. Information entered on or transmitted via computer and communications systems may be subject to subpoena or discovery in litigation.
4. The District acknowledges that because of the nature of the relationship between the District and the recognized employee unions on personnel disputes and bargaining matters, those unions will have a reasonable expectation of privacy in their e-mail communications involving such matters pursuant to the Privacy Act of 1986, 18U.S.C. Section 2510 et seq.

A. Manager Responsibilities

Manager responsibilities include, but are not limited to:

1. Posting the following notice in an easily visible place in an assigned area of direct supervision:

**NOTICE:**

Pursuant to the Electronic and Communications Privacy Act of 1986, 18 U.S.C. Section 2510 et seq., notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications.

Do not use this system for any communications for which the sender intends only the sender and the intended recipient to read.

All communications entered into this system are readable by the operator(s) of the system whether or not they are intended recipients of the communications.

By use of this system, employees agree to hold harmless the District and operators of the system against any and all claims arising out of said use no matter the cause or fault.

1. Informing users of computer technology and communications resources of this Board Policy 2755, Computer Technology and Communications Resources Use – Faculty and Staff, and its regulation, and providing copies to users on request.

2. Developing, distributing and enforcing any additional guidelines or procedures necessary to implement Board Policy 2755, Computer Technology and Communications Resources Use – Faculty and Staff within an area of responsibility.
3. Investigating reported or observed misuse of computer technology and communications resources in accordance with the procedures set forth in H. Investigating Violations, (below) and taking appropriate action.
4. Providing training as deemed necessary to users of computer technology and communications resources in an area of responsibility.

A. Violations Defined

Violations include, but are not limited to, breach of any of the provisions of Board Policy 2755, Computer Technology and Communications Resources Use – Faculty and Staff its regulations R2755, Computer Technology and Communications Resources Use - Faculty and Staff, and guidelines or procedures applicable to a specific area.

B. Reporting Violations

Supervisors and managers who have information that harassment or unlawful acts have occurred through the misuse of computer technology and/or communications resources have the responsibility to report the alleged violation to the appropriate administrator

C. Investigating Violations

1. If a supervisor/manager has information that misuse of computer technology or communications resources has occurred, the supervisor/manager has the obligation to pursue any or all of the following:
  - a. Protecting the system(s), user jobs, and user files from damage.
  - b. Notifying the appropriate Vice President of the alleged abuse.
  - c. Suspending or restricting the alleged abuser's computing privileges during the investigation and administrative processing.
  - d. Inspecting the alleged abuser's files, diskettes, and/or any other record.
  - e. Handling violations that appear to be accidental in an informal, (electronic mail, telephone, or in-person discussions) manner.
  - f. Offenses that are in violation of local, state, or federal laws will be reported to the campus police office which will conduct an investigation to determine if criminal charges should be pursued through the appropriate criminal justice agency (reference Penal Code 503).

A. Sanctions

Misuse of computer technology and communications resources may result in suspension or revocation of use privileges, disciplinary action, civil liability, and/or criminal prosecution as appropriate.

Suspension or revocation of use privileges, and/or disciplinary action may be appealed using established procedures applicable to the employee.

Nothing in this policy precludes enforcement under the laws and regulations of the state of California, any municipality or county therein, and/or the United States of America.

B. Additional Guidelines

System administrators will establish guidelines for specific computer systems and networks to cover allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval, and other items related to administering the system.

C. Definition of Terms

1. **Computer Account:** the combination of a user number, user name, or user ID and a password that allows an individual access to a mainframe computer or other shared computer or network.
2. **Computer Technology and Communications Resources:** the sum total of all computers, workstations, mainframes, software, internet access, telephone, voice mail, cabling, peripherals, networks, accounts, passwords, ID numbers, and data owned or leased by the District.
3. **Data Owner:** the individual or department that can authorize access to information, data, or software and that is responsible for its integrity and accuracy. 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 the District's use of the information, data, or software.
4. **Information Resources:** data or information and the software and hardware that makes that data or information available to users.
5. **Network:** a group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.
6. **Peripherals:** special-purpose devices attached to a computer or computer network such as, printers, scanners, and plotters.
7. **Software:** programs, data, or information stored on magnetic media (for example tapes, disks, diskettes, cassettes, CD-ROMs, etc.). Usually used to refer to computer programs.
8. **System administrator:** staff whose responsibilities include District system, site, or network administration, and staff whose duties include departmental 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.
9. **User:** someone who uses a computer system or network. A user is responsible for learning and implementing proper data management strategies in using computer technology and communications resources.

Users include District officers, employees, and independent contractors authorized to use District computer technology and communications resources.