

## **I. District Technology Access Agreement**

### **1. Introduction**

a. The District Computer and Network system are the sole property of Cuesta College. They may not be used by any person without proper authorization of the District. This policy refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and electronic communication facilities owned, leased, operated or contracted by the District.

b. The District encourages the use of electronic communications to share information and knowledge in support of the District's mission of education, student support, and public service and to conduct the District's business. To this end, the District supports and provides interactive electronic communications services and facilities for telecommunications, mail, publishing, and broadcasting. Recognizing the convergence of technologies based on voice, video, and data networks, this policy establishes an overall policy framework for electronic communications. This policy shall be interpreted and implemented in a manner consistent with other District Policies, and State and Federal laws.

c. While some electronic communications resources may be dedicated to specific research, teaching, or administrative tasks that would limit their use, freedom of expression must, in general, be protected. The District does not limit access to information due to its content when it meets the standards of legality and District policies. Consequently, the District's policy of freedom of expression applies to electronic communications. Coupled with freedom of expression are the personal obligations of each member of our community to use District resources responsibly, ethically, and in a manner which accords both with the law and the rights of others. The College depends upon a spirit of mutual respect and cooperation to create and maintain a community of responsible users.

d. In general, the District cannot and does not wish to be the arbiter of the contents of electronic communications. Neither can the District always protect users from receiving electronic communications they might find offensive.

### **2. Purpose**

a. The purpose of this Policy is to:

- 1) Ensure that District electronic communications resources are used for purposes appropriate to the District's mission;
- 2) Inform the District community about the applicability of laws and
- 3) District policies to electronic communications;

- 4) Ensure that electronic communications resources are used in compliance with those laws and District policies;
- 5) Prevent disruptions to and misuse of District electronic communications resources, services, and activities; and
- 6) Establish policy on privacy, confidentiality, and security in electronic communications.

### 3. Scope

#### a. This Policy applies to:

- 1) All electronic communications resources owned or managed by the District;
- 2) All electronic communications resources provided by the District through contracts and other agreements with the District;
- 3) All users and uses of District electronic communications resources; and
- 4) All District electronic communications in the possession of District employees or of other users of electronic communications resources provided by the District.

#### 4. Definitions. The terms used in this policy are defined in Appendix A.

## **II. Access and Use of Electronic Communication Resources**

1. Access. Access to and use of District electronic communications services or electronic communications resources, when provided, is accorded at the discretion of the District. This resource is subject to the normal conditions of use, including procedures for initiation and termination of access, established by this policy. In addition, access to and use of District electronic communications services or electronic communications resources may be wholly or partially restricted or rescinded by the District without prior notice and without the consent of the electronic communications user when required by and consistent with law, when there is probable cause that violations of law or District policies have taken place, when there are compelling circumstances, or under time-dependent, critical operational circumstances.

### 2. Authorized Users

a. District Users. District students, faculty, staff, and trustees are authorized to use District electronic communications resources and services for purposes in accordance with Section 3720.41, Intended Use, and subject to the responsibilities and limitations of these and other District policies.

b. Non-District Users. Persons and organizations that are not District Users (including those in program, contract, or license relationships with the District) may only access District electronic communications resources or services under programs

sponsored by the District in accordance with IV.1., Intended Use, and subject to the responsibilities and limitations of these and other District policies.

c. Responsibilities

By accessing the District's electronic communications resources, each user acknowledges and agrees to abide by the terms of this Policy and these Procedures. Violations may lead to revocation or suspension of the use of the District's electronic communications resources, employee or student discipline as applicable, and/or referral to outside agencies for prosecution in the event the user's actions constitute a violation of federal, state, or local laws.

### III. PRIVACY AND CONFIDENTIALITY

#### 1. Privacy

a. The District recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the District's legal and other obligations. The District respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations.

b. The District does not routinely inspect, monitor, or disclose electronic communications. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the District may deny access to its electronic communications services and may inspect, monitor, or disclose electronic communications under limited circumstances as described in these policies and procedures.

c. District contracts with outside vendors for electronic communications services shall explicitly reflect and be consistent with this Policy and other District policies related to privacy.

2. Confidentiality. Employees, students, and others are prohibited from seeking out, using, or disclosing personal information without authorization. Employees are required to take necessary precautions to protect the confidentiality of employee records, student records, and personal information encountered in the performance of their duties. Computer systems and networks provide mechanisms for the protection of private information from examination. These mechanisms are necessarily imperfect and any attempt to circumvent them or to gain unauthorized access to private information (including both stored computer files and messages transmitted over a network) will be treated as a violation of privacy and will be cause for disciplinary action.

3. Limitations. Under certain circumstances as defined in Section VI., the District may access electronic communications without an account holder's consent. Due to the open and decentralized design of the Internet and networked computer systems of the District, the District cannot protect individuals against 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 District electronic communications resources should know that the District cannot protect them from invasions of privacy.

**IV. GUIDELINES FOR USE OF DISTRICT ELECTONIC COMMUNICATIONS.** The District encourages the use of electronic communications resources and makes them widely available to the District community. Nonetheless, the use of electronic communications resources is limited by restrictions that apply to all District property and by constraints necessary for the reliable operation of electronic communications systems and services. The District reserves the right to deny access to its electronic communications resources when necessary to satisfy these restrictions and constraints. Use of District electronic communications resources is allowable subject to the following conditions:

1. **Intended Use.** Electronic communications resources are provided by the District units to support the instruction, research, and public service missions of the College, and the administrative functions that support this mission.
2. **Personal Use.** Users of a District electronic communications systems or service may use that facility or service for incidental personal purposes provided that such use does not:
  - a. Directly or indirectly interfere with the District's operation of electronic communications resources;
  - b. Interfere with the user's employment or other obligations to the District; or
  - c. Burden the District with incremental costs.

The District is not responsible for any loss or damage incurred by an individual as a result of personal use of District electronic communications resources.

3. **Accessibility to Individuals with Disabilities.** All electronic communications intended to accomplish the academic and administrative tasks of the District shall be accessible to authorized users with disabilities in compliance with law and District policies. Alternate accommodations shall conform to law and District policies and guidelines.
4. **Intellectual Property.** The contents of all electronic communications shall conform to laws and District policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. When the content and distribution of an electronic communication would exceed fair use as defined by the federal Copyright Act of 1976, users of District electronic communications resources shall secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.
5. **Representation.** Use of the District's name, logo and identity is regulated by District policy. Users of electronic communications resources must abide by District policies on the use of the District's identity. Users of electronic communications resources shall not

give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the District unless appropriately authorized to do so.

6. Endorsements. References or pointers to any non-District entity contained within District electronic communications shall not imply District endorsement of the products or services of that entity.

7. Restrictions. District electronic communications resources may not be used for:

- a. unlawful activities;
- b. commercial purposes not under the auspices of the District;
- c. personal use inconsistent with IV.2., Personal Use; or
- d. use that violate other District policies or guidelines.

The latter include, but are not limited to, policies and guidelines regarding intellectual property and sexual or other forms of harassment.

Users must not attempt to add, modify, or remove equipment, software or peripherals to the District Network (either wired or wireless) without proper authorization.

8. False Identity and Anonymity

Users of District electronic communications resources shall not, either directly or by implication, employ a false identity (the name or electronic identification of another). However, a supervisor may direct an employee to use the supervisor's proxy to transact District business for which the supervisor is responsible. In such cases, an employee's use of the supervisor's proxy does not constitute a false identity. A user of District electronic communications resources may use a pseudonym (an alternative name or electronic identification for oneself) for privacy or other reasons, so long as the pseudonym clearly does not constitute a false identity.

9. Interference. District electronic communications resources shall not be used for purposes that could reasonably be expected to directly or indirectly disrupt or degrade on any electronic communications resources, or unwarranted or unsolicited interference with others' use of electronic communications resources. Users of electronic communications services shall not:

- a. send or forward electronic mail chain letters or their equivalents in other services; "spam", that is, exploit electronic communications systems and services for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications;
- b. intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications services; or
- c. knowingly or negligently introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into District computers or networks.

## **V. INAPPROPRIATE USES OF DISTRICT ELECTRONIC COMMUNICATIONS RESOURCES: REPORTING AND CONSEQUENCES**

1. Process for Investigating Inappropriate Use. An appropriate District employee may informally resolve unintentional or isolated minor violations of use policies or procedures through Email or face-to-face discussion and education with the user or users concerned. If there is probable cause to believe that any user is engaging in activities that constitute an emergency circumstance, an appropriate District employee may take immediate action.

2. Student Violations. Suspected violation of this Policy or Procedures by a student shall be reported to the appropriate employee in charge of the facility. He/she will determine if the student's conduct can be dealt with informally or constitutes probable cause to initiate disciplinary action. The employee will then take any action deemed appropriate under the circumstances in accordance with the College Academic Honesty and Student Code of Conduct Policies or Board Policy 6200/R6200, available for reference in the College catalog or by requesting copies from Student Services or on the college web site. If the responsible employee determines that a violation has occurred, he/she may take immediate action to suspend the user's privileges by contacting the District Computer Services department. In the event a user's privileges are suspended, the District must provide the user with written notice of the suspension and provide a statement of reasons for the actions taken. Any suspension of user's privileges must be reported in writing to the Administrator responsible for student discipline within three business days of such action. Thereafter, the Administrator may determine whether additional disciplinary action should be taken pursuant to established student discipline procedures. The determination to suspend a student's user privileges may be appealed pursuant to the appeal procedures set forth in Academic Honesty and Student Code of Conduct Policies.

### **3. Employee Violations**

a. Suspected violations by an employee should be reported to the employee's immediate supervisor. He/she may: (1) contact the staff member to attempt to resolve the matter informally; or (2) refer the matter to the appropriate Vice President for investigation and potential disciplinary action following District Policy.

b. If the Vice President determines that a violation has occurred, the District Computer Services staff may be directed to suspend or revoke the user's privilege. The appropriate Vice President may also direct the District Computer Services staff to delete material found to be in violation of this Policy or Procedure. In the event user's privileges are suspended or revoked, the appropriate Vice President must provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the actions taken.

4. Non-District User Violations. Suspected violations of this Policy or Procedures by a non-district user shall be reported to an appropriate District Administrator. The Administrator will determine if the non-district user's conduct constitutes a violation of the District Policy or Procedure and can be resolved informally, or if additional action is

required. In the event that additional action is required, the Administrator will take actions to protect the District's resources and refer the matter to the appropriate District authority. Policy violations by non-district users may be referred to Human Resources office. Sanctions may include but are not limited to immediate revocation of user privileges, termination of contractual relationships, removal from campus and/or service area, restitution or civil or criminal prosecution.

5. **Disciplinary Action.** Violations of this policy may result in disciplinary action consistent with disciplinary policies and procedures for faculty, staff and students. Violations may also result in civil and/or criminal prosecution. 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.

6. **Local, Federal, or State Statutes.** Any offense which violates local, state or federal laws may result in the immediate loss of all District computing access and use and will be referred to appropriate District offices and/or law enforcement authorities.

## **VI. Access Without Consent**

Consent from a district user shall be obtained by the District prior to any inspection, monitoring, or disclosure of the contents of District electronic communications records in the holder's possession, except as provided for below. The District shall only permit the inspection, monitoring, or disclosure of electronic communications records without the consent of the holder of such records:

- When required by and consistent with laws such as the California Public Records Act;
- When there is probable cause to believe that violations of law or of District policies;
- When there are compelling circumstances or
- Under time-dependent, critical operational circumstances.

When under the circumstances described above, the contents of electronic communications must be inspected, monitored, or disclosed without the holder's consent, the following sections shall apply.

1. **Authorization.** Except in compelling circumstances, or under time-dependent, critical operational circumstances, or emergency circumstances as defined in Appendix A, Definitions, such actions must be authorized in advance and in writing by the College President or responsible Vice President. Authorization shall be limited to action no broader than necessary to resolve the situation.

2. **Emergency Circumstances.** In compelling, critical operational, or emergency circumstances, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section 3720.61.
3. **Notification.** In either case, the responsible authority or designee shall at the earliest possible opportunity that is lawful and consistent with other District policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.
4. **Compliance with Law.** Actions taken under Section VI., shall be in full compliance with the law and other applicable District policies. Advice of Counsel must be sought prior to any action involving electronic communications (a) stored on equipment not owned or housed by the District, or (b) whose content is protected under the federal Family Educational Rights and Privacy Act of 1974.
5. **Recourse**
  - a. **Faculty and Staff.** District personnel grievance procedures shall be used as the process for review and appeal of actions taken under Section VI., to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the District were in violation of this Policy.
  - b. **Students.** College Academic Honesty and Student Code of Conduct Policies, shall be the process for review and appeal of action taken under Section VI..

## **VII. Technology Access Agreements**

1. Employee Technology Access Agreement (See Attachment A - DRAFT)
2. Student Technology Access Agreement (See Attachment B - DRAFT)

## **Employee Technology Access Agreement – DRAFT 2007**

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. All employees are responsible for using technology and resources in an effective, efficient, ethical, and lawful manner.

### 1. Responsibilities:

- a. Read and follow the District Technology Access Agreement
- b. Maintain security of user name and password
- c. Log off student accessible computers when not in use, such as classrooms and labs
- d. Notify appropriate District employees if you observe or suspect violation of the District or Student Technology Access agreements

### 2. Prohibitions:

- a. Don't install or remove software (including plug-ins, shareware and freeware) or hardware on campus owned equipment without prior authorization from Vice President of Administrative Services.
- b. Removable media (i.e. CD, Thumb drive) should only be used to transfer data. Don't run applications from removable media
- c. 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.
- d. Personally owned computers and networked devices may never be connected to the Cuesta College network via a cable without authorization from the Vice President of Administrative Services. Personally owned computers and networked devices may be connected to the public wireless network (e.g. myCuesta).

3. Privacy. 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 of 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.

- a. 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.
- b. 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.

#### 4. Intellectual property

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

#### 5. Violations

- a. See V.3.(a)(b) of AP3720.

## **Student Technology Access Agreement - DRAFT**

Cuesta College provides broad access to its computing, communications and information resources. These resources support the delivery of the college's academic mission and accordingly, they must be used responsibly. These resources include the physical data communications network and all the computers, printers, scanners and other hardware which access the network, as well as all software, and access to the Internet.

This article is to communicate what other users, instructors, and the District expects of students when using College computer technology and facilities. In addition, the District Technology Access Agreement must be adhered to. Failure to conform to these stipulations can result in disciplinary action. Violations of regulations in the use of computer technology will be addressed in accordance with the inappropriate uses of District Electronic Communications Resources: Reporting and Consequences section of District Technology Access Agreement.

In addition to this policy, students are required to adhere to the posted usage policies of student labs or facilities they wish to use.

Cuesta College is not responsible for loss of data, time delay, system performance, software performance, or any other damages arising from the use of Cuesta computing resources. Every effort will be made to minimize the likelihood of this occurrence, but there is no guaranty.

1. Purpose. Computer technology and facilities are provided for the purpose of completing academic tasks. Students may use the technology and facilities to:
  - a. Complete course assignments;
  - b. Conduct academic research;
  - c. Communicate with faculty and students;
  - d. Pursue instructional activities;
  - e. Pursue student and campus life.
  
2. User Responsibilities. User responsibilities include, but are not limited to:
  - a. Do not use any of Cuesta's networks, including the myCuesta wireless network, to transfer confidential information unless protected by encryption, as others may be able to eavesdrop on your communications.
  - b. Behave in a responsible, ethical and legal manner and to respect the rights of other computer users.
  - c. Use your own designated ID, passwords/PIN, and accounts. Keep IDs, passwords/PIN, and account information confidential. It is recommended that you change their passwords/PIN periodically.  
Use software and electronic materials in accordance with copyright, trademark, and licensing agreements and restrictions.  
Accurately identify and represent yourself in electronic messages, files, and transactions.

- d. Save your data on removable storage media and not on the hard drive, of Cuesta provided equipment, unless instructed to do so by your instructor.
  - e. Comply with instructions from Cuesta designated personnel to discontinue activities deemed by Cuesta personnel to be inappropriate, or have negative impacts on computing or network resources.
  - f. In the case of a computer security situation, follow any necessary instructions from Cuesta designated personnel.
  - g. Your Cuesta student email account will be used for important communication by the college. It is your responsibility to read it on a regular basis.
3. Prohibitions. Prohibitions include, but are not limited to:
- a. Do not damage equipment, data, or software. Do not circumvent software protections, encryption or restrictions on applications and files, including but not limited to: introducing or using invasive, destructive, or eavesdropping programs such as viruses, worms, Trojan horses, spyware, keyloggers, sniffers, password crackers, and rootkits.
  - b. Do not make unauthorized use of accounts, access codes, passwords, or identification numbers.
  - c. Do not impede or disrupt the use of computer technology and electronic communications resources for others.
  - d. Do not engage in activities that use excessive network resources or that would reasonably lead to a denial of service;
  - e. Do not violate trademarks or the terms of applicable software licensing agreements. Do not violate copyright laws.
  - f. Do not access, use, or copy another user's account, ID number, password, electronic files, data, or e-mail. Do not allow such use by others.
  - g. Do not use District computer technology or electronic communications resources in any unlawful manner including making fraudulent, threatening, libelous, obscene, or harassing communication; or procuring or distributing obscene or pornographic material.
  - h. Do not generate or facilitate unsolicited commercial email ("spam").
  - i. Do not circumvent or attempt to circumvent local, network, or remote security measures for any reason. Do not make any attempt to cause a denial of service or to gain unauthorized access to any resource.
  - j. Do not alter, install, or attempt to alter or install software or hardware.

- k. Do not falsely identify and/or represent one's self in the use of computer technology and communications resources.
  - l. Do not connect equipment to the college network (wired or wireless) except where expressly designated and then, connect only single user computing equipment.
  - m. Do not use computer technology and/or communications resources for commercial use.
4. Privacy. See Privacy and Confidentiality section of District Technology Access Agreement
5. Enforcement
- a. See Inappropriate Uses of District Electronic Communications Resources: Reporting and Consequences section of District Technology Access Agreement.
  - b. By accessing Cuesta computing and electronic communication resources, you agree to be bound by these terms. A violation of these terms may result in administrative, civil, or criminal action.

## APPENDIX A: DEFINITION OF TERMS

**Compelling Circumstances:** Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of District policies, Policies Relating to Non-Consensual Access, or significant liability to the District or to members of the District community.

**Electronic Communications Resources:** Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

**Electronic Communications Systems or Services:** Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

**Emergency Circumstances:** Circumstances in which time is of the essence and there is a high probability that delaying action would almost certainly result in compelling circumstances.

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

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

**Probable Cause:** Reliable evidence indicating that violation of law or of District policies, Policies Relating to Non-Consensual Access, probably has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

**Proxy:** A specific e-mail procedure that allows one individual to grant another individual the ability to act on his/her behalf in using electronic mail.

**Server:** A computer that contains information shared by other computers on a network. and that can be used by one or more users.

**Software:** Programs, data, or information stored on media, usually used to refer to computer programs.

**Supervisor:** The employee's supervisor as defined in the District's organization chart.

**Time-dependent, Critical Operational Circumstances:** Circumstances in which failure to act could seriously hamper the ability of the District to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.

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