

## AP 3720.1-3720.7 Electronic Communication Procedures

### Section 3720.1 Introduction

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. (See Appendix B for references).

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.

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.

### Section 3720.12 Purpose

The purposes of this Policy are to:

- Ensure that District *electronic communications resources* are used for purposes appropriate to the District's mission;
- Inform the District community about the applicability of laws and District policies to electronic communications;
- Ensure that electronic communications resources are used in compliance with those laws and District policies;
- Prevent disruptions to and misuse of District electronic communications resources, services, and activities; and
- Establish policy on privacy, confidentiality, and security in electronic communications.

### Section 3720.13 Scope

This Policy applies to:

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

**Section 3720.14 Definitions**

The terms used in this policy that are defined in Appendix A, Definitions, are printed in italics. Knowledge of these definitions is important to an understanding of these policies and procedures.

**SECTION 3720.2 ACCESSES AND USE OF ELECTRONIC COMMUNICATION RESOURCES****Section 3720.21 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*.

**Section 3720.22 Authorized Users**

**3720.221 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.

**3720.222 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 Section 3720.41, Intended Use, and subject to the responsibilities and limitations of these and other District policies.

**Section 3720.23 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.

### **SECTION 3720.3 PRIVACY AND CONFIDENTIALITY**

#### **Section 3720.31 Privacy**

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.

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.

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.

#### **Section 3720.32 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.

#### **Section 3720.33 Limitations**

Under certain circumstances as defined in Section 3720.6 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.

### **SECTION 3720.4 GUIDELINES FOR USE OF DISTRICT ELECTRONIC 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:

#### **Section 3720.41 Intended Use**

Electronic communications resources are provided by the District units to support the teaching, research, and public service missions of the College, and the administrative functions that support this mission.

#### **Section 3720.42 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.

#### **3720.43 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.

#### **3720.44 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.

**3720.45 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.

**3720.46 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.

**3720.47 Restrictions**

District electronic communications resources may not be used for:

- unlawful activities;
- commercial purposes not under the auspices of the District;
- personal financial except for incidental use directly related to one's responsibilities at the District;
- personal use inconsistent with Section 3720.42, Personal Use; or
- uses 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 (See Appendix B, References).

**3720.48 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.

When publishing web pages and transmitting broadcasts (i.e. voice, video, text) a user may not remain anonymous (the sender's name or electronic identification shall not be hidden).

**3720.49. 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;
- b. "spam", that is, exploit electronic communications systems and services for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications;
- c. send an extremely large message or send multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic communications systems and services;
- d. intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications services; or
- e. knowingly or negligently introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into District computers or networks.

### **SECTION 3720.5 INAPPROPRIATE USES OF DISTRICT ELECTRONIC COMMUNICATIONS RESOURCES: REPORTING AND CONSEQUENCES**

#### **Section 3720.51 Process for Investigating Inappropriate Use**

Computer *System Supervisor* may informally resolve unintentional or isolated minor violations of use policies or procedures through E-mail 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*, a System Supervisor may take immediate action as described in Section 3720.02.

#### **3720.511 Student Violations**

Suspected violation of this Policy or Procedures by a student shall be reported to the System Supervisor. He/she will determine if the student's conduct constitutes probable cause to initiate any disciplinary action and will then take any action deemed appropriate under the circumstances by following the appropriate sections of Board Policy 3231 - Student Conduct. If the System Supervisor determines that a violation has occurred, he/she may take immediate action to suspend the user's privileges for up to two (2) days. In the event a user's privileges are suspended, the System Supervisor 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 Dean of Educational Programs responsible for student discipline within one day of such action. Thereafter, the Dean may determine whether additional disciplinary action should be taken pursuant to established student discipline procedures as outlined in Board Policy 3231 - Student Conduct. The determination to suspend a student's user

privileges may be appealed pursuant to the appeal procedures set forth in Board Policy 3231 - Student Conduct.

### **3720.512 Faculty Violations**

Suspected violations of the Policy or Procedures by the district faculty shall be reported to the appropriate department chair, area supervisor or dean. He/she may: (1) contact the faculty member to attempt to resolve the matter informally, or (2) refer the matter to the area dean or Executive Vice President for investigation and potential disciplinary action following District Policy.

### **3720.513 Staff Violations**

Suspected violations by staff 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. If the Vice President determines that a violation has occurred, the System Supervisor may be directed to suspend or revoke the user's privilege. The appropriate Vice President may also direct the System Supervisor 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.

### **3720.514 Non-District User Violations**

Suspected violations of this Policy or Procedures by a non-district user shall be reported to the System Supervisor. The System Supervisor will determine if the non-district user's conduct constitutes a violation of the District Policy or Procedure. In the event of a violation, the System Supervisor will take appropriate 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 the District's Legal Affairs/Human Resources office and/or law enforcement authorities. 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.

## **Section 3720.52 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 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.

**Section 3720.53 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.

**3720.6 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:

- a. when required by and consistent with laws such as the California Public Records Act;
- b. when there is *probable cause* to believe that violations of law or of District policies listed in Appendix B;
- c. when there are compelling circumstances as defined in; or
- d. 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.

**3720.61 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. This authority may not be further delegated. Authorization shall be limited to action no broader than necessary to resolve the situation.

**3720.62 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.

**3720.63 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.

**3720.64 Compliance with Law**

Actions taken under Section 3720.6 shall be in full compliance with the law and other applicable District policies, including laws and policies listed in Appendix B, References. 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.

**3720.65 Recourse**

*Faculty and Staff:* District personnel grievance procedures shall be used as the process for review and appeal of actions taken under Section 3720.6 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.

*Students:* Board Policy 3235 – Student Grievance Policy, shall be used as the process for review and appeal of action taken under Section 3720.6.

**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 listed in Appendix B, 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 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 listed in Appendix B, 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 magnetic media (tapes, disks, diskettes, cassettes, etc.). Usually used to refer to computer programs.

**Staff:** Classified employee, administrator or other employee who is not faculty.

**System Supervisor:** Faculty or staff employed by the District whose responsibilities include system, site, or network administration and staff employed by departments whose duties include system, site, or network administration. System supervisors perform functions including, but not limited to, installing hardware and software managing a computer or network, and keeping a computer operational.

**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.

**APPENDIX B:**  
**FEDERAL STATE AND DISTRICT STATUTES REGULATIONS**  
**AND POLICIES REFERENCES**

The following is a partial list of Federal, State and District statutes, regulations and policies that pertain to the college's Computer Use Policy and Procedures. This list of references does not include all Federal, State, and District statutes, regulations and policies that pertain to this Policy.

**State of California Statutes**

State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)

State of California Education Code Section 67100 et seq.  
State of California Education Code 92000  
State of California Government Code, Section 11015.5  
State of California Penal Code, Section 502  
State of California Public Records Act (Government Code Section 6250 et seq.)

**Federal Statutes and Regulations**

American with Disabilities Act of 1990  
Communications Decency Act of 1996  
Copyright Act of 1976  
Digital Millennium Copyright Act of 1998  
Electronic Communications Privacy Act of 1986  
Electronic and Information Technology, Section 508  
Family Educational Rights and Privacy Act of 1974  
Federal Communications Commission Rules and Regulations  
Federal Copyright Act of 1976  
Privacy Act of 1974  
Telecommunications Act of 1934  
Telecommunications Act of 1996

**District Policies** (Note: Correct listing of relevant District Policies will be referenced in this Appendix)

Academic Freedom, *Policies for Faculty and Educational Administrators section 2520*  
Disciplinary Procedures, *Policies for Faculty and Educational Administrators, section 2500, Appendix F*  
Disciplinary Procedures, *Policies for Student Personnel, section 3231.3,*  
Discrimination, *Affirmative Action Program for Santa Barbara Community College District, Appendix A*  
Faculty Grievances, *Policies for Faculty and Educational Administrators, section 2500, Appendix F*  
Freedom of Expression, *Policies for Faculty and Educational Administrators section 2520*  
Intellectual Property, *Policies for Faculty and Educational Administrators, section 2410 (to be developed)*  
Microcomputer Software Copyright Policy, *section 2601 and 2602*  
Policy for Student Use of Computers and Network  
Rights to Privacy, *Policies for Faculty and Educational Administrators section 2520*  
Sexual Harassment, *Affirmative Action Program for Santa Barbara Community College District, Chpt. IX*  
Student Conduct, *Policies for Student Personnel, section 3231*  
Student Grievances, *Policies for Student Personnel, section 3235*  
Use of District Logo and Identity [no policy as yet]