



## PASADENA AREA COMMUNITY COLLEGE DISTRICT POLICY

**Title: Privacy, Security and Acceptable Use of Electronic Resources**

**Policy No. 5350**

**Legal Authority:** California Education Code Section 70902

**Page 1 of 4**

---

**It is the policy of the Pasadena Area Community College District that there be privacy, security, and acceptable use of its electronic resources, as follows:**

1. As a part of the physical and social learning infrastructures, Pasadena City College (PCC) acquires, develops, and maintains computers, voice communications, world wide web computer systems, and networks. These computer and voice resources are intended for college-related purposes, including direct and indirect support of the college's instruction, research, and service missions; of college administrative functions; of student and campus life activities; and of the free exchange of ideas among members of the college community and between the college community and the wider local, national, and world communities.
2. The rights of academic freedom and freedom of expression apply to the use of these college computing and voice transmission resources. In that regard, PCC respects the privacy of the communications of its employees and students while they are engaged in acceptable use of these resources. The college does not however guarantee that these communications are completely private.
3. The use of college computing and voice transmissions resources, like the use of any other college-provided resource and like any other college-related activity, is subject to the normal requirements of legal and ethical behavior within the college community. Thus, acceptable use of these electronic resources does not extend to whatever is technologically possible. Although some limitations are built into communications systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the communication or network and whether or not they can be circumvented.

**PASADENA AREA COMMUNITY COLLEGE DISTRICT  
PROCEDURES  
For Policy No. 5350**

**Title: Privacy, Security and Acceptable Use of Electronic Resources**

**Procedure No. 5350.10**

**Page 2 of 4**

1. Applicability

- a. These procedures apply to all users of computers, voice communications, world wide web computer systems, and networks, hereinafter referred to as systems and to all uses of those systems, whether on campus or from remote locations. Additional procedures may apply to specific computers, computer systems, voice mail, or networks provided or operated by specific units of the college. Consult the operators or managers of the specific computer, computer system, or network in which you are interested for further information.

2. Acceptable Use

All users of college systems must:

- a. Comply with all federal, California, and other applicable law; all generally applicable college rules and policies; and all applicable contracts and licenses. Examples of such laws, rules, policies, contracts, and licenses include the laws concerned with libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, and California Penal Code Section 502, which prohibit "hacking," "cracking," and similar activities; the college's code of student conduct; the college's sexual harassment policy; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- b. Use only those computing and voice transmission resources that they are authorized to use and use them only in the manner and to the extent authorized. Ability to access computing and voice mail resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons or groups other than those to whom they have been assigned by the college.
- c. Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding.
- d. Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users. Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of college computing and voice transmission resources, the college may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all the relevant circumstances.
- e. Recognize that these resources are not provided for personal commercial purposes or for personal financial or other gain. Personal use of college "systems" is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other college responsibilities, and is otherwise in compliance with this procedure. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

- f. Refrain from stating or implying that they speak on behalf of the college. Affiliation with the college does not, by itself, imply authorization to speak on behalf of the college. The use of disclaimers is encouraged when appropriate.
  - g. Refrain from using college logos without authorization to do so. Users are directed to refer to the college policies regarding the uses of the college logo.
3. Enforcement
- a. Users who violate this procedure may be denied access to college computing and voice transmission resources and may be subject to other penalties and disciplinary action, both within and outside the college. Violations will normally be handled through the college disciplinary policy applicable to the relevant user. However, the college may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.
4. Security
- a. The college employs various measures to protect the security of its computing and voice transmission resources and of users' accounts. Users should be aware, however, that the college cannot guarantee such security. Users should therefore engage in secure practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing passwords regularly.
  - b. The employees and students of Pasadena City College may expect that the privacy of their communications will be respected except where access is required by law or by the requirements of maintaining the technology.
5. Privacy
- a. Users should also be aware that their uses of college computing and voice transmission resources are not completely private. While the college does not routinely, without cause, monitor individual usage of its computing and voice transmission resources, the normal operation and maintenance of the college's computing and voice transmission resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service.
  - b. The college may also specifically monitor the activity and accounts of individual users of college computing and voice transmission resources, including individual login sessions and communications, without notice, when
    - (1) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page;
    - (2) it reasonably appears necessary to do so to protect the integrity, security, or functionality of college or other computing and voice transmission resources or to protect the college from liability;
    - (3) there is reasonable cause to believe that the user has violated, or is violating, this policy;
    - (4) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or
    - (5) it is otherwise required by law. Any such individual monitoring, other than that specified in "(5)," required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the College President.

- c. A copy of the written authorization must be provided to the Manager who is directed to provide the access. Within 72 hours of the President's authorization of such monitoring, the President and Manager shall give written notice to the appropriate representative of the employee or student whose electronic or voice transmissions have been monitored without personally identifiable information - notice shall be given in all instances unless prohibited by court order. The notices shall include the reasons for the monitoring, and the section (1) through (5) above under which the monitoring occurred, but shall not include any personally identifying information regarding the person whose electronic or voice mail transmissions have been monitored, other students or employees of the College, or other persons who are referenced in or involved in the transmissions.
- d. In all cases except 5(b)(5) above, the individual will be notified within 72 hours that their electronic resources have been accessed. Before or at notification, the District may, at its discretion, take action to prevent messages, information, or data from being destroyed, altered, mutilated, enciphered, or removed.
- e. An authorized agent of the college may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate college personnel or law enforcement agencies and may use those results in appropriate college disciplinary proceedings. Communications made by means of college computing and voice transmission resources are also generally subject to California's Public Records Statute to the same extent as they would be if made on paper.
- f. Nothing in this policy/procedures is intended to contradict or override the existing policies and procedures of the College, including but not limited to, the disciplinary articles of the collective bargaining agreements and the College's sexual harassment policy/procedures.