BOARD POLICY
San Mateo County Community College District

***Subject*:** 2.34 Computer and Network Use
***Revision Date*:** xx/xx
***Policy References*:** Education Code Section 70902; Government Code Section 3543.1(b); Penal Code Section 502; California Constitution, Article 1 Section 1; 17 U.S. Code Sections 101 et seq.

---

1. The District provides various electronic media, including laptop and/or desktop computers for use by employees. Employees are encouraged to use these media in their work to communicate with students, with each other and with the administration, and to improve their access to research and instructional tools.

2. District computers and networks are property of the District. Employees and students may use the District's network services and computers for personal purposes provided that such use does not directly interfere with the normal performance of duties, or with the normal operation of District systems or facilities. Use of these systems for unlawful purposes is not authorized and can constitute grounds for revocation of user privileges, removal of offensive material, and potentially result in disciplinary action.

3. While the District respects all employees' and students' right to privacy in work place communications, employees, students and others should realize that District communications systems are not always private. The District cannot routinely protect users' confidentiality in some situations. Some email or computer use, when created or stored on District equipment, may constitute a District record subject to disclosure under the California Public Records Act or other laws, or as a result of litigation. Users of District computer resources should be aware that such situations or laws may not permit the confidentiality of email or other documents or data on a computer in some circumstances.

4. The District shall not inspect, monitor, or disclose email or other computer files without the holder's consent, except (1) when required by and consistent with the law; (2) when there is a substantiated reason to believe that violations of law or provisions herein have taken place and the holder or user is the subject of suspicion; or (3) under time-dependent emergency circumstances or critical compelling circumstances.

    a. Substantiated reason means that reliable evidence indicates the probability that violation of law or provisions herein has occurred, as distinguished from rumor, gossip, speculation or other unreliable evidence.
    b. Time-dependent, emergency circumstances means where time is of the essence and where there is a high probability that delaying action would almost certainly result in critical compelling circumstances.
    c. Critical compelling circumstances means that a failure to act may result in significant bodily harm, significant property damage or loss, loss of significant evidence of the violation of law or provisions herein, significant liability to the District or District employees or students.

5. Except in emergency circumstances as defined above, District inspection, monitoring or disclosure of emails or other documents or data must be authorized in advance and in writing by the Chancellor. This authority shall not be further delegated. Unless precluded by law, law enforcement or related agencies, the District shall make a full and complete written record of the rationale for such access, which shall be provided to the affected employee within two work days of obtaining access.

6. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation. All inspection and/or monitoring pursuant to this Section is limited to the specific computer hardware which the District has a substantiated reason to believe were used in the violations as alleged and described in the written authorization. All inspection and/or monitoring shall be limited to the investigation of the violations as alleged and described.

7. Users should be aware that during the performance of their duties, Information Technology Services personnel occasionally need to observe certain transactional addressing information to ensure proper functioning of the District's computer services, including email. Except as provided in this Section or by law, they shall not intentionally read the contents of email or other ~~electronically transmitted~~ documents, or to read transactional information where not germane to the foregoing purpose, or to disclose or otherwise use what they have seen.

8. Employees and students who use District computers and networks and the information they contain, and related resources, have a responsibility to respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

9. The District cannot and does not wish to be the arbiter of contents of documents in any physical or electronic media. The District shall not protect users from receiving transmitted or physically conveyed language or images which they may find offensive or objectionable in nature or content, regardless of whether such documents originated within or outside the District. Employees and students are strongly encouraged to use the same personal and professional courtesies and considerations in such communications as they would with face-to-face conversation.