SANTA ROSA JUNIOR COLLEGE

Building on a Legacy of Excellence

2.13P
COMPUTER AND COMMUNICATIONS TECHNOLOGY USE
[formerly 6.9P]
REVIEWED: DECEMBER 12, 2000
REVIEWED: MARCH 11, 2008
REVIEWED: MAY 9, 2012
REVIEWED: April 9, 2013
CATEGORY 3 REVISION: NOVEMBER 12, 2013
REVISED:

STATE OF CALIFORNIA: Education Code Section 67100 et seq,, Government Code, Section 11015.5, California Penal Code, Section 502, California Public Records Act (Government Code Section 6250 et seq.)
FEDERAL: 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, Telecommunications Act of 1934; Telecommunications Act of 1996; Rules of Civil Procedure 2016.
DISTRICT POLICY AND PROCEDURE 2.14, 4.14, 4.9, 7.8,

These procedures apply to all electronic communications resources owned or managed by the Sonoma County Junior College District or provided by the District through contracts and other agreements with the District; and to all users and uses of District electronic communications resources.

~~**ACCESS**~~

~~Students, faculty, staff, and trustees ("District users") are authorized to use District electronic communications resources and services subject to the responsibilities and limitations of this and other District policies.~~

~~Non-District users, including persons and organizations in program, contract, or license relationships with the District, may only access District electronic communications resources or services under programs sponsored by the District and are subject to the responsibilities and limitations of this and other District policies.~~

~~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 suspension or revocation of the use of the District's electronic communications resources, employee or student discipline, and/or referral to outside agencies for prosecution in the event the user's actions constitute a violation of federal, state, or local laws.~~

~~Access to and use of District-provided electronic communications services or electronic communications resources is accorded at the discretion of the District. The District reserves the right to restrict or rescind an individual's user of District-provide electronic communication services or resources without the consent of the user when laws and/or District policies have been violated.~~

PRIVACY

The District shall not routinely inspect, monitor, or disclose any individual's electronic communications except under limited circumstances and only according to requirements for authorization, notification, and other conditions specified in this Procedure. Electronic communications include any Internet Protocol (IP) data that traverses the District's wired or wireless data networks.

~~District contracts with outside vendors for electronic communications services shall explicitly reflect and be consistent with all District policies related to privacy.~~

The District will take reasonable precautions to protect the privacy of users of District electronic communications resources, but ~~given the open and decentralized design of the Internet and networked computer systems, this cannot be guaranteed.~~ due to the nature of the technology and the public character of the District's business, there is no guarantee that a user's files, account, and email are private. Documents created and/or stored on District computers and networks may be considered public records, subject to disclosure under the Public Records Act, other laws, or as a result of litigation.

OFFENSIVE MATERIAL

Users are warned that when utilizing the Internet, they may encounter material that could be considered offensive or objectionable in nature or content which is beyond the control of the District.

CONFIDENTIALITY

District 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. All District employees and students are prohibited from seeking out, using, or disclosing such personal information without appropriate authorization.

Any attempt to circumvent computer and network mechanisms that protect private information from examination 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.

PERSONAL USE

Students, faculty, staff and trustees may use the District's electronic communications systems, services and resources for incidental personal purposes provided that such use does not directly or indirectly interfere with the District's operation of its electronic communications resources, the user's employment, or other obligations to the District; burden the District with incremental costs; or violate any laws or District policies.

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

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.

INTELLECTUAL PROPERTY

The contents of all District electronic communications shall conform to laws and District policies regarding protection of intellectual property, including laws and policies regarding copyright, patents, and trademarks. Users of District electronic communications resources must secure appropriate permission to distribute protected material in any form, including text, photographic images, audio, video, graphic illustrations, and computer software.

REPRESENTATION

Users of District electronic communications resources must abide by District policies on the use of the District's name, logo and identity. Users of District electronic communications resources must not give the impression, whether implicit or explicit, that they are representing, giving opinions, or otherwise making statements on behalf of the District or any unit of the District unless specifically authorized by the Board of Trustees or their designee to do so.

ENDORSEMENTS, SOLICITATION AND COMMERCIAL USE

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.

District electronic communications resources may not be used for soliciting for a non-profit or charity without prior explicit approval by the Board of Trustees.

District electronic communications resources may not be used for commercial purposes not sanctioned by the District.

ANONYMITY AND FALSE IDENTITY

When publishing web pages and/or transmitting voice, video, or text broadcasts, the District sender's name or electronic identification shall not be hidden.

Users of District electronic communications resources shall not, either directly or by implication, employ a false identity (the name or electronic identification of another), unless:

1. A supervisor directs an employee to use the supervisor's proxy to transact District business for which the supervisor is responsible.

2. A user of District electronic communications resources uses 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.

INTERFERENCE

District electronic communications resources shall not be used for purposes that could reasonably be expected to directly or indirectly disrupt or degrade any District electronic communications resources, or cause unwarranted or unsolicited interference with others' use of District electronic communications resources. This includes, but is not limited to:

1. Sending or forwarding electronic mail chain letters or their equivalents in other services;

2. Distributing "spam" and exploiting electronic communications systems and services for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications;

3. Sending an extremely large message or sending multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic communications systems and services;

4. Intentionally engaging in other practices such as denial of service attacks that impede the availability of electronic communications services; or

5. Knowingly or negligently introducing any purposefully invasive or destructive programs into District computers or networks.

DISTRICT E-MAIL

The District provides its students, faculty, staff and Trustees with e-mail access for academic and administrative purposes only. Only the ~~Board of Trustees~~ President/Superintendent, or their designee may approve offering email accounts to others.

~~Access to these systems is a privilege, and every user is expected to use good judgment when using the e-mail system.~~

The District e-mail system is considered an official means of communication, and all members of the District community are expected to use and maintain their ~~College~~ District e-mail account on a regular basis.

E-mail messages express the views of the individual author and may not reflect the views or opinions of the District as a whole.

The District e-mail system must not be used to send messages containing material that is fraudulent, harassing, sexually explicit, and obscene, intimidating, defaming, or otherwise unlawful. Violations and appropriate discipline will be addressed according to District policy.

In compliance with State and Federal statutes, the District retains all email for a period of 4 years (1461 days).

BROADCAST MESSAGES AND DISTRIBUTION LISTS

Faculty and staff may send email broadcast messages to employees using one of the District's large distribution lists (e.g., DL.STAFF.ALL) in accordance with the following guidelines:

1. Broadcast messages must have a clear, concise subject line.

2. Broadcast messages must be relevant to the majority of the recipients on the distribution list as judged by the sender.

3. Broadcast Messages should not to be used for personal financial gain, to advertise nonprofits, and/or personal advertising not authorized by the District.

4. Broadcast Messages sent on behalf of another employee must state that employee's name.

5. Reasonable efforts must be made to minimize the total number of such emails sent.

ONLINE FORUMS

The District approves of the creation and use of online forums to allow self-selected groups of students, faculty and staff to exchange ideas in a professional and collegial manner and/or to receive notifications of events. Participation in online forums will remain completely voluntary, and is subject to the following restrictions:

1. Anonymous forum posts are not permitted.

2. Forum posts must have clear and concise subjects (or labels). Forum discussions should remain focused on the stated subject (or label).

3. Forum posts must be professional and work appropriate and follow relevant netiquette standards.

4. Forum posts must conform to all District Policies and Procedures.

5. Forum posts that constitute harassment, discrimination, cyber bullying, or other illegal behaviors will not be permitted and are subject to discipline.

6. Forum users must report inappropriate use to the System Administrator or immediate supervisor.

~~Users may sign up to receive email notifications when items post to the forums.~~

ACCOUNT TERMINATION

In order to protect the campus computing infrastructure and manage costs, the District will terminate access to District email and other electronic communications resources on a regular basis, following an audit at the end of each semester (December, May and August). Account termination is determined by:

1. **Employee Resignation or Cessation of Contract Faculty Assignment**. Access will be available for one (1) week following the resignation date or termination of assignment. It is the immediate supervisor's responsibility to notify the Human Resources Department about the departure, instruct employees to dispose of account contents appropriately, and follow record retention guidelines.

2. **Cessation of Adjunct Faculty Assignment**: Adjunct faculty who complete their current assignment will have email access continued per the terms of their union contract with the District.

3. **Terminated employees**: Accounts are deactivated immediately following termination, as directed by Human Resources and/or the employee's supervisor.

4. **Any staff not covered by the previous categories:** Any employee who has not been in a paid status for more than 12 months will have his/her email account deactivated.

Exceptions will be considered on a case-by-case basis and require approval by the area Vice President.

~~INAPPROPRIATE USE~~

~~System Administrators may informally resolve unintentional or isolated minor violations of use policies or procedures through email or face-to-face discussion with the user or users concerned. If there is probable cause to believe that any user is engaging in activities that constitute an~~

illegal, inappropriate or emergency circumstance, a System Administrator may take immediate action to safeguard the District and/or the user.

Violations of this policy may result in disciplinary action consistent with District 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. 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.

1. **Student Violations**

a. Suspected violation of this Policy or Procedures by a student shall be reported to the System Administrator who will determine if the student's conduct constitutes probable cause to initiate any disciplinary action and will then take appropriate action according to the Student Conduct Standards.

b. If the System Administrator 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 Administrator must provide the user with written notice of the suspension including a statement of reasons for the actions taken.

c. Any suspension of a student's user privileges must be reported in writing to the Dean of Student Services responsible for student discipline within one day of such action. Thereafter, the Dean may determine whether additional disciplinary action should be taken.

d. The determination to suspend a student's user privileges may be appealed.

2. **Faculty Violations**

Suspected violations of this Policy or Procedures by District faculty shall be reported to the appropriate Department Chair, Area Supervisor or Dean, who may contact the faculty member to attempt to resolve the matter informally, or refer the matter to the area Dean or Vice President for investigation and potential disciplinary action following District Policy.

3. **Staff Violations**

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

4. **Non-District User (non-employee or non-student) Violations**

a. Suspected violations of this Policy or Procedures by a non-district user shall be reported to the System Administrator. The System Administrator will determine if the non-district user's conduct constitutes a violation of the District Policy or Procedure.
b. In the event of a violation, the System Administrator will take appropriate actions to protect the District's resources and refer the matter to the appropriate District authority.

c. ~~Policy violations by non-district users may be referred to the District's 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.~~

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:

1. When required by and consistent with laws such as the California Public Records Act;

2. When there is probable cause and reliable evidence to believe that the user has violated law or District policies.

3. When there are compelling circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, or loss of significant evidence of one or more violations of law or of District policies.

4. Under time-dependent, critical operational 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.

Authorization

Except in compelling circumstances, or under time-dependent, critical operational circumstances, or emergency circumstances, access without consent must be authorized in advance and in writing by the Superintendent/President or appropriate Vice President. This authority may not be further delegated. Authorization shall be limited to action no broader than necessary to resolve the situation.

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. When emergency action is taken, the user must be notified, in writing, within seven (7) business days of the inquiry.

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.

Compliance with the Law

Any access without consent 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 stored on equipment not owned or housed by the District, or protected under the federal Family Educational Rights and Privacy Act of 1974.

Recourse

Faculty and Staff may request review and appeal any access without consent through District personnel grievance procedures, Students may request review and appeal any access without consent through the Student Grievance Policy.

ENFORCEMENT

District employees who discover violations of this policy in the normal course of their duties are required to report those violations to their supervisor or the Senior Director of Information Technology. The Senior Director of Information Technology, or their designee will inform the appropriate supervisor of computer use violations, In the case of students, the Senior Director of Information Technology or their designee will inform the appropriate conduct administrator of computer use violations. Violations of this regulation will be enforced pursuant to applicable District policies, procedures, and/or collective bargaining agreements.

~~APPENDIX A: FEDERAL AND DISTRICT STATUTES, REGULATIONS AND POLICIES REFERENCES~~

a. ~~State of California Statutes~~
   i. ~~State of California Education Code Section 67100 et seq. ii. State of California Education Code 92000~~
   iii. ~~State of California Government Code, Section 11015.5~~
   iv. ~~State of California Penal Code, Section 502~~
   v. ~~State of California Public Records Act (Government Code Section 6250 et seq.)~~
b. ~~Federal Statutes and Regulations~~
   i. ~~Communications Decency Act of 1996~~
   ii. ~~Copyright Act of 1976 Digital Millennium Copyright Act of 1998~~
   iii. ~~Electronic Communications Privacy Act of 1986 Electronic and Information Technology, Section 508 iv. Family Educational Rights and Privacy Act of 1974~~
   ~~v. Federal Communications Commission Rules and Regulations Federal Copyright Act of 1976~~
   ~~vi. Privacy Act of 1974~~
   vii. ~~Telecommunications Act of 1934~~
   viii. ~~Telecommunications Act of 1996~~
c. ~~District Policies~~
   i. ~~Intellectual Property, District Governance Policies, section 2.14~~
   ii. ~~Student Conduct & Discipline, District Policies for Student Rights & Responsibilities, section 8.2 iii. Soliciting Funds on Campus, District Policies for Community Relations, section 7.8~~
   iv. ~~Employee Discipline, District Policies for Employee Discipline, section 4.9 Employee Grievance, District Policies for Employee Complaint and Grievance, section 4.14~~