

PERSONNEL**4040(a) EMPLOYEE USE OF DISTRICT TECHNOLOGY RESOURCES**

Employees of the district must abide by the district's policies and regulations as a condition of employment. The district has elected to create an "Employee Technology Use Agreement" which serves the purpose of assuring each employee has had an opportunity to read and become familiar with the district's policies on the use of technology resources, including Internet or intranet access. The district may require its employees to sign such an agreement as a condition of using these technology resources, but employees are bound by these policies and regulations regardless of whether a signed agreement is on file, and may be subject to discipline for failing to follow those terms and conditions. A copy of the current version of the Employee Technology Use Agreement (Form 4040(b)) follows this section.

Internet Access via District Infrastructure Only

Employees of the district shall not have their own Internet access from any district property, nor shall they attempt in any fashion to bypass the district's network infrastructure to access the Internet. All employee Internet access obtained from school property must be through the district-provided access to the Internet. Any exceptions to this rule necessitated by extraordinary circumstances must be approved by the Superintendent or his/her Designee.

Supervision of Student Access to the Internet

Staff shall provide reasonable supervision under the circumstances for students who are using Internet, intranet or other on-line services, and may ask teacher aides and student aides to assist in such supervision. The purpose of such supervision shall be instructional as well as to prevent students from "misuse of the District's Internet Access" as that phrase is defined in the Student Technology Use Agreement.

Students who fail to abide by regulations promulgated by the Superintendent or designee, or who fail to abide by the Student Technology Use Agreement or school rules regarding Internet use, shall be subjected to disciplinary action, revocation of the user account, and legal or criminal action as appropriate.

Staff shall also make every effort to assure all students are abiding by the district's policies, regulations and the Technology Use Agreement by:

- a. not providing any identifying personal information about themselves or their families to anyone on the Internet;
- b. not entering chat rooms unless curriculum related (and even then, with pre-approval and intense supervision), and;

doing all things reasonably prudent and necessary to protect student safety at all times.

Technology Resource Use for District-Related Business

The district provides technology resources, including the provision of personal computers, software, telephones, voice mail, printers, access to the Internet and intranet, and access to networked resources, for the sole purposes of district-related business, including employee productivity and student instruction. All technology resources are owned by the district, and only loaned to individuals for the purpose of conducting district business.

Any use of these resources by any individual for commercial business or personal gain, or violation of state or federal law or district policy is forbidden, and is subject to disciplinary action as allowed by policy and law. Private or personal non-commercial use of the district's e-mail or Internet access is permitted as long as it:

- (a) is not excessive or done at inappropriate times, as determined by the employee's direct supervisor, district personnel directors, or with final determination by the Superintendent or his/her designee;
- (b) does not interfere in any fashion with the district's normal business practices and the performance of the employee's duties (as determined in section (a));
- (c) reflects sound judgment and sensitivity on the part of the employee, particularly as to avoiding civil or criminal liability or public reproach upon the district; and
- (d) does not violate any state or federal law or district policy.

Use of the employee's personally owned technology resources on district property subjects its use to the same rules and regulations that apply to all other district-owned property.

In addition to this policy, use of the District's e-mail services is subject to all applicable federal and state communications and privacy laws. Attaching programs, sound, video and images to e-mail messages may violate copyright laws, which is addressed in the district policies forbidding all copyright violations by users of district resources.

Soliciting and Selling

District employees shall not use the District access to the Internet, nor shall they use any District created or District related web site, to advertise any private commercial ventures in which they have a financial or proprietary interest, or in which members of their families have financial or proprietary interests. Board Policy 1540(a) controls advertising on District web sites. District related web sites are defined in Board Policy 1540(a).

Expectation of Privacy

Current state and federal law has general guidelines regarding expectations of privacy for employees while at the work place using company technology resources. The district intends to follow what are reasonably prudent standards (as defined by current law, policy, business practices and case law) for assuring the district's resources are not

misused, and liability is not created. Current law also allows employers to create restrictions to protect against liability by prohibiting certain activities, including informing employees in advance that they will not have an expectation of privacy while using district technology resources, such as they may have when using their own property at home.

In order to enforce the policies in place and protect the district from liability, the district reserves the right to do any of the following, and may have to resort to any of the following practices at any time:

1. To use filtering or screening products that look for illegal or inappropriate activity on its networks or e-mail systems, and act on any such information found;
2. To open and examine any file in use or stored on any of its resources, including personal computers, network drives, e-mail files, or district-related web sites, at any time;
3. To attach to or take control of any district workstation at any time, without prior notice;
4. To use any means available to track Internet access or activity while using district resources for violations of district policy;
5. To restrict access to network resources or the Internet, or to revoke technology resource use privileges altogether, if such is warranted;
6. To cooperate in any fashion necessary with any legal investigation if criminal charges are brought against a district technology user, including turning over any relevant data to authorities.

Disciplinary action will follow state and federal law, including the Education and Penal Codes, and district policy and regulations.

Receipt of Inappropriate Materials

The district recognizes that due to the nature of the Internet, users may from time to time involuntarily receive something of an inappropriate nature via a web site, e-mail or other access point. Technology users who encounter such situations should follow the guidelines provided by the district, including those in the employee Internet Use Agreement, which may include, but not be limited to:

1. Deleting the file immediately, if e-mail or an attachment (and emptying the Trash or Recycling Bin from the computer's system);
2. Being careful not to open unrecognized mail or unfamiliar web sites in the presence of students;
3. Notifying the district's Department of Technology & Information Systems immediately if an inappropriate site has made its way past the district's filtering system;
4. Not forwarding, copying or referring others in any way to the offending material;

5. If receiving inappropriate materials repeatedly from the same party, notifying that party to immediately stop sending such materials.

Users who follow district guidelines and show evidence of reasonable standards of behavior will not be subjected to disciplinary action for receipt of such inappropriate materials.

Additional Security Measures

The district must maintain a variety of data that must be kept secure for safety or legal reasons, including personal student information, personal employee information, secure financial data, etc. The district may add additional security measures to assure that only authorized users are allowed to access technology resources. Additional measures may be added to assure that data that must be kept secure is only accessible to those authorized to access it.

To that end, district employees must abide by the district's security procedures, which may be included in the Employee Technology Use Agreement, and may be updated from time to time. It is particularly critical that district employees and other users never share passwords with others. Sharing of passwords can leave an employee responsible for any activities that take place under that password.

Additionally, to assure that the district can access, support and monitor its technology resources at all times, district technology users may not add their own additional security, passwords or other protection to their data without authorization from the district's Department of Technology & Information Systems. BIOS or CMOS passwords, or the addition of third party software designed to block access to a personal computer or network directory with a password are specifically prohibited unless authorized as noted above.

Use of District Voice Mail, Fax, Other Communications Technologies

District users of voice mail, fax or other communications technologies should expect the same standards of use as with the other technologies listed in this section. District employees may not listen in on others' phone calls. However, the district reserves the right to screen, review or otherwise intercept messages stored on district voice mail systems, sent via district fax machines, or via other communications technologies available, if necessary to protect against potential liability.

Technology Copyright Laws

All users, including employee users, of district technology resources agree at all times to abide by all current laws respecting copyright of software, content or other technologies. Installation of software on district equipment that is not legally licensed is strictly forbidden and subject to discipline and/or legal penalties.

(Cf. 1540(a) - District Related Internet Web sites)

(Cf. 4040 - Employee Use of Technology)

(Cf. 6118 – Student Use of Technology and the Internet)

(Cf. 6143, 6144 – Audio/Visual, Library Media Centers)
(Cf. 6145 – Copyright Law)

Legal References:

EDUCATION CODE

51006 Computer education and resources
51007 Programs to strengthen technological skills
51870-51884 Education Technology Act
60011 Instructional materials definition
60022 Prohibited instructional materials

PENAL CODE

313 Harmful matter
632 et seq Eavesdropping on or recording confidential communications

UNITED STATES CODE

20 U.S.C. § 6801-7005 Technology for Education Act of 1994
Board of Education, Island Trees Union Free District # 26 v. Pico (1982) 457 U.S. 853
McCarthy v. Fletcher (1989) 207 Cal.App.3d 130 [254 Cal.Rptr. 714].

Management Resources:

CDE PUBLICATIONS

K-12 Network Technology Planning Guide: Building the Future, 1994

CDE PROGRAM ADVISORIES

1223.94 Acceptable Use of Electronic Information Resources

WEB SITES

CSBA: <http://www.csba.org> (California School Board Association)
CDE: <http://www.cde.ca.gov> (California Department of Education)
AASA: <http://www.aasa.org/FrontBurner/TechPlans/plansTC.htm>
(American Association of School Administrators)
FCUSD: <http://www.fcusd.k12.ca.us> (Folsom Cordova Unified School District)

Policy Approved: August 17, 2000

FOLSOM CORDOVA UNIFIED SCHOOL DISTRICT