CSBA Sample
Board Policy
Employee Use Of Technology

BP 4040
Personnel

The Governing Board recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting district and school operations; and improving access to and exchange of information. The Board expects all employees to learn to use the available technological resources that will assist them in the performance of their job responsibilities. As needed, employees shall receive professional development in the appropriate use of these resources.

(cf. 0440 - District Technology Plan)
(cf. 1100 - Communication with the Public)
(cf. 1113 - District and School Web Sites)
(cf. 1114 - District-Sponsored Social Media)
(cf. 4032 - Reasonable Accommodation)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

Employees shall be responsible for the appropriate use of technology and shall use district technology primarily for purposes related to their employment.

(cf. 0410 - Nondiscrimination in District Programs and Activities)
(cf. 4119.11/4219.11/4319.11 - Sexual Harassment)
(cf. 4119.21/4219.21/4319.21 - Professional Standards)
(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential/Privileged Information)
(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)
(cf. 5125 - Student Records)
(cf. 5125.1 - Release of Directory Information)
(cf. 6162.6 - Use of Copyrighted Materials)
(cf. 6163.4 - Student Use of Technology)

District technology includes, but is not limited to, computers, the district's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through district-owned or personally owned equipment or devices.

Note: The following paragraph is optional and may be revised to reflect district practice. It is recommended that districts develop an Acceptable Use Agreement containing rules for the use of district technology, which should be signed by each employee. See the accompanying Exhibit for an example of an Acceptable Use Agreement for employees.

The Superintendent or designee shall establish an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. Upon employment and whenever significant changes are made to the district's Acceptable Use Agreement, employees shall be required to acknowledge in writing that they have read and agreed to the Acceptable Use Agreement.

Note: The following paragraphs may be revised to reflect district practice.

Note: To qualify for federal universal service discounts for Internet access, Internet services, or internal connections (E-rate discounts), districts are mandated by 47 USC 254 to adopt an Internet safety policy that includes, but is not limited to, provisions addressing access by minors to "inappropriate matter" on the Internet; see BP 6163.4 - Student Use of Technology. Consistent with those requirements, the following paragraph provides that employees shall not use district technology to access inappropriate matter. "Inappropriate matter" is not defined in the law and the determination of what matter is considered inappropriate is a local decision to be made by the district. Penal Code 313 provides a definition of "harmful matter" as specified below. Districts that have adopted their own definition should revise the following paragraphs as appropriate.

Employees shall not use district technology to access, post, submit, publish, or display harmful or inappropriate matter that is threatening, obscene, disruptive, sexually explicit, or unethical or that promotes any activity prohibited by law, Board policy, or administrative regulations.

Harmful matter includes matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest and is matter which depicts or describes, in a patently offensive way, sexual conduct and which lacks serious literary, artistic, political, or scientific value for minors. (Penal Code 313)

Note: 47 USC 254 mandates that the district's Internet safety policy for E-rate discounts include the operation and enforcement of a "technology protection measure" that protects against Internet access to visual depictions that are obscene, child pornography, or harmful to minors. Similarly, as a condition of receiving technology funds under Title II, Part D of the No Child Left Behind Act (20 USC 6751-6777) for the purpose of purchasing computers with Internet access or paying for direct costs associated with Internet access, 20 USC 6777 mandates that districts adopt an Internet safety policy that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography. Although these requirements focus on measures designed to protect students using district technology (see BP 6163.4 - Student Use of Technology), they also require policy that affects Internet access by adults.

Note: The following paragraph is for use by districts that desire to use E-rate or federal technology funding sources and may be adapted by other districts that choose to install technology protection measures.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors and that the operation of such measures is enforced. The Superintendent or designee may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. (20 USC 6777; 47 USC 254)

Note: The following optional paragraphs may be revised to reflect district practice.

Note: Although 20 USC 6777 and 47 USC 254 require districts receiving federal Title II technology funds or E-rate discounts to enforce the operation of technology protection measures, the legislation clarifies that nothing in the Children's Internet Protection Act shall be construed to require the tracking of individual students' or adults' Internet use. Thus, it appears to be left to the discretion of districts as to whether they wish to track Internet use through personally identifiable web monitoring software or other means.

Note: It is recommended that districts notify employees that they should have no expectation of privacy when using district equipment or technological resources. In City of Ontario v. Quon, the U.S. Supreme Court held that a search of an employee's pager messages was reasonable because the search was motivated by a legitimate work-related purpose and was not excessive in scope. In addition, the city had adopted a policy stating that employees should have no expectation of privacy or confidentiality when using city equipment.

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any equipment or other technological resources provided by or maintained by the district, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, even when provided their own password. To ensure proper use, the Superintendent or designee may monitor employee usage of district technology at any time without advance notice or consent and for any reason allowed by law.

Note: In City of San Jose v. Superior Court, an appellate court held that the California Public Records Act does not cover otherwise disclosable communications (e.g., emails, text messages) that were not directly accessible by a governmental entity because they were sent or received via private electronic devices and were not stored on government servers. However, this case has been appealed to the California Supreme Court.

In addition, employees shall be notified that records maintained on any personal device or messages sent or received on a personal device that is being used to conduct district business may be subject to disclosure, pursuant to a subpoena or other lawful request.

Employees shall report any security problem or misuse of district technology to the

Superintendent or designee.

Inappropriate use of district technology may result in a cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law, Board policy, and administrative regulation.

(cf. 4118 - Dismissal/Suspension/Disciplinary Action)
(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

Legal Reference:
EDUCATION CODE
52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program
GOVERNMENT CODE
3543.1 Rights of employee organizations
PENAL CODE
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
VEHICLE CODE
23123 Wireless telephones in vehicles
23123.5 Mobile communication devices; text messaging while driving
23125 Wireless telephones in school buses
UNITED STATES CODE, TITLE 20
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:
6777 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts
COURT DECISIONS
City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332

Management Resources:
WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Department of Education: http://www.cde.ca.gov
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov

(7/01 7/07) 7/15