

EMPLOYEE USE OF TECHNOLOGY

The Board of Trustees recognizes that technological resources can enhance employee performance by improving access to and exchange of information, offering effective tools to assist in providing a quality instructional program, and facilitating district and school operations. 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 training in the appropriate use of these resources.

(cf. 0440 - District Technology Plan)
(cf. 1113 - District and School Web Sites)
(cf. 4032 - Reasonable Accommodation)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)
(cf. 6162.7 - Use of Technology in Instruction)
(cf. 6163.4 - Student Use of Technology)

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources only for purposes related to their employment. Such use is a privilege which may be revoked at any time.

(cf. 4119.25/4219.25/4319.25 - Political Activities of Employees)

Employees should be aware that computer files and communications over electronic networks, including e-mail and voice mail, are not private. These technologies shall not be used to transmit confidential information about students, employees or district operations without authority.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that prevents access to visual depictions that are obscene or child pornography, 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)

To ensure proper use of the system, the Superintendent or designee may monitor the district's technological resources, including e-mail and voice mail systems, at any time without advance notice or consent. If passwords are used, they must be known to the Superintendent or designee so that he/she may have system access.

The Superintendent or designee shall establish administrative regulations which outline employee obligations and responsibilities related to the use of district technology. He/she also may establish guidelines and limits on the use of technological resources. Inappropriate use shall result in a cancellation of the employee's user privileges, disciplinary action and/or legal action in accordance with law, Board policy and administrative regulations.

EMPLOYEE USE OF TECHNOLOGY (continued)

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

The Superintendent or designee shall provide copies of related policies, regulations and guidelines to all employees who use the district's technological resources. Employees shall be asked to acknowledge in writing that they have read and understood these policies, regulations and guidelines.

(cf. 4112 9/4212 9/4312 9 - Employee Notifications)

In the event that the use of an electronic resource affects the working conditions of one or more employees, the Superintendent or designee shall notify the employees' exclusive representative.

(cf. 4143/4243 - Negotiations/Consultation)

Legal Reference

EDUCATION CODE

51870-51874 Education technology

GOVERNMENT CODE

3543 1 Rights of employee organizations

PENAL CODE

502 Computer crimes, remedies

632 Eavesdropping on or recording confidential communications

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

UNITED STATES CODE, TITLE 20

6751-6777 Education Through Technology Act, No Child Left Behind Act, Title II, Part D

6777 Internet Safety

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

CDE. <http://www.cde.ca.gov>

CSBA. <http://www.csba.org>

Federal Communications Commission. <http://www.fcc.gov>

U.S. Department of Education. <http://www.ed.gov>

American Library Association. <http://www.ala.org>

EMPLOYEE USE OF TECHNOLOGY

On-Line/Internet Services: User Obligations and Responsibilities

Employees are authorized to use district equipment to access the Internet or on-line services in accordance with Board of Trustees policy and the user obligations and responsibilities specified below.

1. The employee in whose name an on-line services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses and telephone numbers private. They shall use the system only under their own account number.
2. Employees shall use the system responsibly and primarily for work-related purposes.

(cf. 6162 7 - Use of Technology in Instruction)

3. Employees shall not access, post, submit, publish or display harmful or inappropriate matter that is threatening, obscene, disruptive or sexually explicit, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, gender, sexual orientation, age, disability, religion or political beliefs.

(cf. 4030 - Nondiscrimination in Employment)

(cf. 4031 - Complaints Concerning Discrimination in Employment)

(cf. 4119 11/4219 11/4319 11 - Sexual Harassment)

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy or administrative regulations.
5. Copyrighted material shall not be placed on the system without the author's permission. Employees may download copyrighted material only in accordance with applicable copyright laws.

(cf. 6162 6 - Use of Copyrighted Materials)

6. Employees shall not intentionally upload, download or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or the data of any other user, including so-called "hacking."
7. Employees shall not read other users' electronic mail or files. They shall not attempt to interfere with other users' ability to send or receive electronic mail, nor shall they attempt to read, delete, copy, modify or forge other users' mail.
8. Users shall report any security problem or misuse of the services to the Superintendent or designee.

EMPLOYEE USE OF TECHNOLOGY (continued)

(cf. 6163 4 - Student Use of Technology)