

All Personnel

EMPLOYEE USE OF TECHNOLOGY

The Governing Board recognizes that technological resources can 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. The Governing Board supports uses of internet and social media sites to supplement the educational process. As needed, employees shall receive professional development 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. 6163.4 - Student Use of Technology)

Employees shall be responsible for the appropriate use of technology and shall use the district's technological resources primarily for purposes related to their employment. Compliance with the law and all policies, guidelines and procedures for the appropriate use of the district's technology resources is a condition of employment. The Superintendent or designee will provide access to current policies, guidelines and procedures relating to technology use via the district's website, any of which may periodically be updated. District employees agree to periodically review, familiarize themselves with, and ensure they understand any current policies, guidelines and procedures as the district deems necessary before using any district technology resources.

The Superintendent or designee shall establish administrative regulations and guidelines 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 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 - Suspension/Disciplinary Action)
(cf. 4218 - Dismissal/Suspension/Disciplinary Action)

Expectation of Privacy

While using district technology resources, employees understand they have no expectation of privacy such as they would have at home. The district reserves its rights to research or monitor any use of its resources as it deems necessary, with or without notice or consent, to protect students, or to protect itself from misuse of resources or exposure to potential liability. Such monitoring may include, but not be limited to, review of internet or computer activity, files, e-mail, or any other inspection required. The district may act on the findings

EMPLOYEE USE OF TECHNOLOGY (continued)

from any such monitoring as it deems appropriate or as is legally required, including turning over any such information to legal authorities.

Confidential Data

District employees may be required to access and manage a variety of electronically stored confidential data relating to students, employees or others. Authorization to access confidential data shall be limited only to that required to complete necessary tasks and duties, as determined by the Superintendent or designee. Technological resources shall not be used to transmit confidential information about students, employees or other district operations without authority and without appropriate technological security applied to protect the data. It is the responsibility of any employee transmitting such data to be familiar with appropriate security practices. Inappropriate access to, sharing, or use of district confidential data by an employee may lead to disciplinary (up to and including dismissal) or legal action, as appropriate.

(cf. 4119.23/4219.23/4319.23 - Unauthorized Release of Confidential/Privileged Information)

(cf. 5125 - Student Records)

(cf. 5125.1 - Release of Directory Information)

Network and Data Security and Access

As part of being granted access to district data and systems, employees may be assigned or asked to create a variety of passwords. Such passwords serve the purpose of protecting student, employee and other potentially confidential data, and protecting district systems from unauthorized access, damage or destruction. Unauthorized sharing of or receipt of others' passwords exposes the district and its schools to potential loss, liability, or legal action.

Every employee accessing district data must be personally authorized to access such data with his/her own login and password, and may not use others' logins/passwords to gain such access. Employees may not share passwords or provide access to any secured electronic resources to others. Unauthorized access gained or provided to others may lead to disciplinary (up to and including dismissal) or legal action, as appropriate.

Additionally, employees may not secure any district technological resources or data with passwords that block access by the district to its resources, including BIOS or CMOS-level passwords, or other third-party security. Any needs for additional levels of security should be arranged through the district's department of Educational Technology and Information Systems.

Employees shall not make additions, moves, or changes to district infrastructure, including but not limited to: network hardware, cable plant. Additionally, protective filters, firewalls, or similar mechanisms to restrict access or monitoring are strictly prohibited unless authorized by the Chief Technology Officer or designee. Violation of this policy by an

EMPLOYEE USE OF TECHNOLOGY (continued)

employee may lead to removal of equipment, disciplinary (up to and including dismissal) or legal action, as appropriate.

Employees may only access network resources remotely by methods or means provided for and authorized by the Chief Technology Officer or designee and at no time shall install software or hardware on district property to facilitate this.

Online/Internet Services

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 maintain the necessary protection measures and with the exceptions noted in “Use of Cellular Phone or Mobile Communications Device” below, 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 or filtering to access the internet. Any efforts to bypass access protections, or to facilitate the bypass of such protections by others, may lead to disciplinary or legal action, as appropriate. Any exceptions to this rule necessitated by extraordinary circumstances must be expressly approved by the Superintendent or designee.

Supervision of Student Access to the Internet

All district employees shall provide reasonable supervision for students who are using internet, or other online services. The purpose of such supervision is to ensure student safety, to facilitate and improve instruction, and to ensure students are complying with the district's policies and procedures relating to students use of technology (BP 6163.4), including the Student Technology Use Agreement.

Use of Cellular Phone or Mobile Communications Device

An employee shall not use a cellular phone or other mobile communications device for personal business while on duty, except in emergency situations and/or during scheduled work breaks. Employees may also utilize such devices to access the Internet while on scheduled work breaks but at no time may “tether” or otherwise connect such devices to district computers or district property.

Any employee that uses a cell phone or mobile communications device in violation of law, Board policy, or administrative regulation shall be subject to discipline and may be referred to law enforcement officials as appropriate.

EMPLOYEE USE OF TECHNOLOGY (continued)

(cf. 3513.1 - Cellular Phone Reimbursement)
(cf. 3542 - School Bus Drivers)
(cf. 4156.3/4256.3/4356.3 - Employee Property Reimbursement)

Legal Reference:

EDUCATION CODE

51870-51874 Education technology

52270-52272 Education technology and professional development grants

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

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

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>