Employee Use of Technology

Adopted: 05/21/2002 **| Last Revised:** 02/03/2026 **| Last Reviewed**: 02/03/2026

The Board of Education 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; enriching curriculum; and enhancing student learning. 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.

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.

District technology includes, but is not limited to, computer hardware, software, or software as a service provided or paid for by the district, whether accessed on or off site or through district-owned or personally owned equipment or devices, including tablets and laptops; computer servers, wireless access points (routers), and wireless computer networking technology (wi-fi); the Internet, email, applications (apps), including artificial intelligence (AI) apps; telephones, cellular or mobile telephones, smartphones, smart devices, and wearable technology, or any wireless communication device, including radios.

Employees shall be notified that computer files and electronic communications, including email and voicemail, are not private. Technological resources shall not be used to transmit confidential information about students, employees, or district operations without authority.

An employee may use technology, including AI apps, to assist the employee in the performance of the employee's professional duties, including, but not limited to, the following specific tasks: developing syllabi, creating curriculum, reviewing student work, suggesting instructional strategies, and researching academic content or instructional techniques. Any employee using technology, including AI, shall review and be responsible for any final product or document; not share confidential student records with a third party, such as an AI app, except as permitted by law; and use the technology in accordance with Board Policy 6162.6 - Use of Copyrighted Materials, and in a manner otherwise consistent with law, Board policies, and rules. If an employee is unsure about the appropriate use of technology, the employee shall confer with the Superintendent or designee before using.

As determined by the Superintendent or designee, employees shall receive professional development in the appropriate use of these resources, including in the use of AI apps.

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, contain child pornography, or are considered 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 purposes.

To ensure proper use, the Superintendent or designee may monitor employee usage of technological resources, including the accessing of email and stored files. Monitoring may occur at any time without

advance notice or consent. When passwords are used, they may be changed by the Superintendent or designee so that employees may have system access.

The Superintendent or designee shall establish rules and an Acceptable Use Agreement which outlines employee obligations and responsibilities related to the use of district technology. The Superintendent or designee 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 rule.

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 rule.

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.

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

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. The district discourages the use of personal devices and/or personal email accounts as being used for district business. An employee shall not transmit student or staff personal identifiable information to personal devices and/or personal email accounts.

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 rule.

Employees may access their mobile or other communications device if there is a need to seek emergency assistance, assess the safety of a situation, or communicate with a person to confirm the person's safety.

Policy Reference Disclaimer:
These references are not intended to be part of the policy itself, nor do they indicate the basis or authority for the Board to enact this policy. Instead, they are provided as additional resources for those interested in the subject matter of the policy.

Legal References:

STATE
GOVERNMENT CODE
11549.3 Cybersecurity
3543.1 Rights of employee organizations
7920.000-7930.170 California Public Records Act
LABOR CODE
1139 Emergency assistance
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
FEDERAL
UNITED STATES CODES
20 USC 7101-7122 Student Support and Academic Enrichment Grants
20 USC 7131 Internet Safety
CODE OF FEDERAL REGULATIONS
47 CFR 54.520 Internet safety policy and technology protection measures; E-rate discounts
MANAGEMENT RESOURCES
CALIFORNIA DEPARTMENT OF EDUCATION PUBLICATION
Artificial Intelligence: Learning With AI Learning About AI
COURT DECISIONS
City of San Jose v. Superior Court (2017) 2 Cal.5th 608
City of Ontario v. Quon et al. (2010) 000 U.S. 08-1332
PUBLICATION
Guidelines for AI integration throughout education in the commonwealth of Virginia
U.S. DEPARTMENT OF EDUCATION PUBLICATION
2024 National Education Technology Plan
USDOE OFFICE OF EDUCATIONAL TECHNOLOGY PUBLICATION
Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations, May 2023
WEBSITES
California Governor's Office of Emergency Services https://www.caloes.ca.gov/
CSBA District and County Office of Education Legal Services https://legalservices.csba.org/
Federal Communications Commission http://www.fcc.gov/
American Library Association http://www.ala.org/
California Department of Education http://www.cde.ca.gov/
CSBA http://www.csba.org/
U.S. Department of Education http://www.ed.gov/

Policy Adopted: 08/01/1995
Revised: 02/03/1998
Revised: 01/15/1999
Revised: 01/15/2008
Revised: 02/03/2026