Policy 4040: Employee Use Of Technology **Status:** ADOPTED

Original Adopted Date: 07/01/2001 | **Last Revised Date:** 09/01/2024 | **Last Reviewed Date:** 09/01/2024

CSBA NOTE: This policy addresses employee use of technology, including artificial intelligence (AI), and may be modified to reflect district practice. The U.S. Department of Education, Office of Educational Technology's, "Artificial Intelligence and the Future of Teaching and Learning: Insights and Recommendations," provides information related to the opportunities for using AI to improve education, the challenges in doing so, and recommendations to guide further policy development. Districts are encouraged to continue to monitor the development of new technologies, including AI.

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; improving access to and exchange of information; enriching curriculum; and enhancing student learning.

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 review the prohibited and permitted uses of technology as specified in Board Policy 5131.9 - Academic Honesty, be responsible for the appropriate use of technology, and use district technology primarily for purposes related to their employment consistent with board policies and administrative regulations.

CSBA NOTE: The following optional paragraphs address employee use of technology, particularly AI applications, are permissive as they relate to such use, and should be modified to reflect district practice.

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 administrative regulations. 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.

CSBA 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, including the use of AI apps. 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.

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

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, to an extent, 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, display, or otherwise engage with 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)

CSBA 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 using federal Student Support and Academic Achievement Grants (20 USC 7101-7122) for the purpose of purchasing computers with Internet access or paying for direct costs associated with Internet access, 20 USC 7131 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, they also require policy that affects Internet access by adults; see BP 6163.4 - Student Use Of Technology.

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 7131; 47 USC 254)

CSBA NOTE: Government Code 11549.3 authorizes districts, at district expense, to request the Military Department, in consultation with the California Cybersecurity Integration Center, to perform an independent security assessment of the district or individual district school. It is recommended that districts consult with the California Office of Emergency Services (OES) and utilize resources such as the State Threat Assessment System and Regional Fusion Centers to help assess potential threats. For more information, see OES' website.

The Superintendent or designee shall regularly review current guidance regarding cybersecurity, data privacy, and digital media awareness and incorporate recommended practices into the district's processes and procedures related to the protection of the district's network infrastructure, the monitoring and response to cyberattacks, ensuring data privacy, and managing suspicious and/or threatening digital media content, in accordance with Board Policy 3580 - District Records.

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

Although 20 USC 7131 and 47 USC 254 require districts receiving Student Support and Academic Achievement Grants 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 is recommended that districts consult with CSBA's District and County Office of Education Legal Services or district legal counsel before tracking Internet use through personally identifiable web monitoring software or other means.

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 following paragraph, which may be modified to reflect district practice, includes a statement that employees should have no expectation of privacy when using district technology.

The Superintendent or designee shall annually notify employees in writing that they have no reasonable expectation of privacy in the use of any district technology, as defined above, even when using their personal devices. 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.

CSBA NOTE: In City of San Jose v. Superior Court, the California Supreme Court held that a government employee's communications about public business are not excluded from a request under the California Public Records Act (CPRA) simply because they have been sent or received on a personal account or personal device. Thus, employees should be aware that if they use personal accounts or devices to communicate about district business, they may be required to temporarily provide the district with access to their personal accounts or devices. Alternatively, employees may search their personal communications using reasonable effort, sign a sworn declaration regarding the nature of their search, and provide any responsive communications to the district as directed. The court observed that the CPRA requires districts to use "reasonable effort" to locate existing records in response to a public records request, but that such searches need not be extraordinary or intrusive. For further information, see CSBA's, "Legal Alert: Tips for Governing Boards in Response to Public Records Act Ruling on Electronic Communications."

In addition, employees shall be notified that records, including communications, maintained on any personal accounts or devices used to conduct district business are subject to disclosure at the district's request, and 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.

CSBA NOTE: Labor Code 1139 prohibits an employer from preventing any employee from accessing the employee's mobile device or other communications device for seeking emergency assistance, assessing the safety of the situation, or communicating with a person to confirm the person's safety.

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. (Labor Code 1139)