Policy 6163.4: Student Use Of Technology **Status:** ADOPTED

Original Adopted Date: 07/01/2007 | **Last Revised Date:** 09/01/2024 | **Last Reviewed Date:** 09/01/2024

CSBA NOTE: This policy addresses student use of technology, including artificial intelligence (AI), and may be modified to reflect district practice. The U.S. Department of Education's (USDOE), "2024 National Education Technology Plan," provides actionable recommendations to advance the effective use of technology to support teaching and learning and aims to close the digital divide by ensuring that all students can equitably access the latest digital tools and technology. Additionally, the USDOE 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 believes that effective use of technology is integral to the education and development of students. In order to promote digital citizenship, the Board recognizes that students must have access to the latest digital tools and receive instruction that allows students to positively engage with technology in ways that respect human rights and avoids Internet dangers. Technological resources provided to students, including technology based on artificial intelligence (AI), shall be aligned to district goals, objectives, and academic standards. The use of technology shall augment the use of Board adopted instructional materials.

The Board intends that technological resources provided by the district be used in a safe and responsible manner in support of the instructional program and for the advancement of student learning. Students shall be allowed to use such technology, including AI technology, in accordance with district policies, including, but not limited to, policies on academic honesty, data privacy, nondiscrimination, and copyright protections. All students using these resources shall receive instruction in the proper and appropriate use of technology. Such instruction shall incorporate students' responsibilities regarding academic honesty, honoring copyright provisions, assessing the reliability and accuracy of information, protecting personal data, and the potential for biases and errors in artificially generated content.

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 AI apps; telephones, cellular telephones, smartphones, smart devices, and wearable technology; or any wireless communication device, including radios.

Teachers, administrators, and/or library media specialists are expected to review the technological resources and online sites that will be used in the classroom or assigned to students in order to ensure that they are appropriate for the intended purpose and the age of the students.

CSBA NOTE: The following optional paragraphs 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 students and their parents/guardians should be required to sign. See the

accompanying Exhibit for an example of an "Acceptable Use Agreement" for students.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district technology, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with this board policy and the district's Acceptable Use Agreement.

Before a student is authorized to use district technology, the student and the student's parent/guardian shall sign and return the Acceptable Use Agreement. In that agreement, the student and parent/guardian shall agree not to hold the district or any district staff responsible for the failure of any technology protection measures or user mistakes or negligence and shall agree to indemnify and hold harmless the district and district staff for any damages or costs incurred.

CSBA NOTE: The following optional paragraph may be revised to reflect district practice. If the district chooses to monitor student use of district equipment or other technological resources, it is recommended that the district adopt an express, written policy and notify students of the policy through the "Acceptable Use Agreement."

Searches of students' personally owned devices (e.g., cell phones, computers, other communications devices) may be subject to the Fourth Amendment of the U.S. Constitution which prohibits unreasonable search and seizure. In New Jersey v. T.L.O., the U.S. Supreme Court held that the legality of a search of a student's belongings depends on whether the search is "reasonable." The "reasonableness" of a search depends on two factors: (1) whether there is individualized suspicion that the search will turn up evidence of a student's violation of the law or school rules and (2) whether the search is reasonably related to the objectives of the search and not excessively intrusive in light of the student's age, gender, and/or the nature of the infraction. See BP 5145.12 - Search And Seizure.

The district reserves the right to monitor student use of technology within the jurisdiction of the district without advance notice or consent. Students shall be informed that the use of district technology, as defined above, is not private and may be accessed by the district for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in the use of district technology. Students' personally owned devices shall not be searched except in cases where there is a reasonable suspicion, based on specific and objective facts, that the search will uncover evidence of a violation of law, district policy, or school rules.

CSBA NOTE: The following optional paragraph is for use by districts that have adopted a program, pursuant to Education Code 49073.6, to gather or maintain information from students' social media activity that pertains directly to school safety or student safety. Districts that choose to adopt such a program must comply with specified notification and program requirements; see BP/AR 5125 - Student Records.

The Superintendent or designee may gather and maintain information pertaining directly to school safety or student safety from the social media activity of any district student in accordance with Education Code 49073.6 and Board Policy/Administrative Regulation 5125 - Student Records.

Whenever a student is found to have violated board policy or the district's Acceptable Use Agreement, the principal or designee may cancel or limit a student's user privileges or increase supervision of the student's use of the district's equipment and other technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and board policy.

The Superintendent or designee, with input from students and appropriate staff, shall regularly review and update procedures to enhance the safety and security of students using district

technology and to help ensure that the district adapts to changing technologies and circumstances.

Internet Safety

CSBA NOTE: 20 USC 7131 mandates that districts adopt an Internet safety policy as a condition of receiving 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 accessing the Internet. 47 USC 254 mandates that districts adopt an Internet safety policy in order to qualify for federal universal service discounts for Internet access (E-rate discounts). This mandate applies to districts that receive E-rate discounts for Internet access, Internet services, or internal connections, but not to districts that receive discounts for telecommunications services only.

Both 20 USC 7131 and 47 USC 254 require that the district's policy include the operation and enforcement of a "technology protection measure" that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors. As part of the funding application process, a district is required to certify that it has the required policy in place and is enforcing the operation of the technology protection measure.

The following paragraph is mandated for districts that use E-rate discounts or Student Support and Academic Achievement Grants 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. (20 USC 7131; 47 USC 254; 47 CFR 54.520)

CSBA NOTE: Districts receiving E-rate discounts for Internet access, Internet services, or internal connections are also mandated by 47 USC 254 to adopt policy that addresses (1) access by minors to "inappropriate matter" on the Internet, (2) safety and security of minors when using email, chat rooms, and other forms of direct electronic communication, (3) unauthorized access, including "hacking" and other unlawful online activities by minors, (4) unauthorized disclosure, use, and dissemination of personal identification information regarding minors, (5) measures designed to restrict minors' access to harmful materials, and (6) education of students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms as well as cyberbullying awareness and response.

The remainder of this section addresses these mandates and may be revised to reflect district practice. Districts that do not receive E-rate discounts may choose to use or adapt this material at their discretion.

To reinforce these measures, the Superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate matter on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities.

CSBA NOTE: "Inappropriate matter" is not defined in the law and the determination of what matter is considered inappropriate for minors 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 paragraph as appropriate.

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)

The district's Acceptable Use Agreement shall establish expectations for appropriate student conduct when using the Internet or other forms of electronic communication, including, but not limited to, prohibitions against:

1. Accessing, posting, submitting, publishing, or displaying 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, sex, gender, sexual orientation, age, disability, religion, or political beliefs

2. Intentionally uploading, downloading, or creating computer viruses and/or maliciously attempting to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking"

CSBA NOTE: Penal Code 653.2 makes it a crime for a person to distribute another person's personal identification information electronically with the intent to cause harassment by a third party or to threaten a person's safety or that of a person's family (e.g., placing a person's picture or address online so that the person receives harassing messages).

3. Distributing personal identification information, including the name, address, telephone number, Social Security number, or other personally identifiable information, of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

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. Districts are encouraged to 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 monitoring suspicious and/or threatening digital media content, in accordance with Board Policy 5125 - Student Records.

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, but not be limited to, the dangers of posting one's own personal identification information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.