Superintendent Policy 6163.4: Student Use Of Technology

Status: ADOPTED

Original Adopted Date: 08/25/2022 **| Last Revised Date:** 09/08/2025 **| Last Reviewed Date:** 09/08/2025

The County Superintendent of Schools believes that effective use of technology is integral to the education and development of students. In order to promote digital citizenship, the County Superintendent of Schools 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 county office of education (COE) goals, objectives, and academic standards. The use of technology shall augment the use of COE adopted instructional materials.

The County Superintendent of Schools intends that technological resources provided by the COE 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 local 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 understanding the potential for biases and errors in artificially generated content.

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

Technological resources and online sites that will be used in the classroom or assigned to students shall be reviewed to ensure that they are appropriate for the intended purpose and the age of the students.

Students and parents/guardians shall be notified about authorized uses of COE technology, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities in accordance with this Superintendent policy and the COE's Acceptable Use Agreement.

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

The COE reserves the right to monitor student use of technology within the jurisdiction of the COE without advance notice or consent. Students shall be informed that the use of COE technology, as defined above, is not private and may be accessed by the COE for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in the use of COE 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, COE policy, or school rules.

Information pertaining directly to school safety or student safety from the social media activity of any COE student may be gathered and maintained in accordance with Education Code 49073.6.

Whenever a student is found to have violated Superintendent policy or the COE's Acceptable Use Agreement, the student's user privileges may be canceled or limited or there may be increased supervision of the student's use of the COE'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.

With input from students and appropriate staff, procedures to enhance the safety and security of students using COE technology shall regularly be reviewed and updated to help ensure that the COE adapts to changing technologies and circumstances.

Internet Safety

All COE computers with Internet access shall 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)

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

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 COE'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 COE equipment or materials or manipulate the data of any other user, including so-called "hacking"

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

The current guidance regarding cybersecurity, data privacy, and digital media awareness shall regularly be reviewed and recommended practices may be incorporated into the COE's processes and procedures related to the protection of the COE's network infrastructure, the monitoring and response to cyberattacks, ensuring data privacy, and monitoring suspicious and/or threatening digital media content.

Age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services shall be provided to COE students. 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.

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.

State	Description
Civ. Code 3120-3123	Digital equity bill of rights
Ed. Code 49073.6	Student records; social media
Ed. Code 51006	Computer education and resources
Ed. Code 51007	Programs to strengthen technological skills
Ed. Code 60044	Prohibited instructional materials
Pen. Code 313	Harmful matter
Pen. Code 502	Computer crimes; remedies
Pen. Code 632	Eavesdropping on or recording confidential communications
Pen. Code 653.2	Electronic communication devices, threats to safety

Federal	Description
15 USC 6501-6506	Children's Online Privacy Protection Act
16 CFR 312.1-312.12	Children's Online Privacy Protection Act
20 USC 7101-7122	Student Support and Academic Enrichment Grants
20 USC 7131	Internet Safety
47 CFR 54.520	Internet safety policy and technology protection measures, E-rate discounts
47 USC 254	Universal service discounts (E-Rate)

Management Resources	Description
California Department of Education Publication	Artificial Intelligence: Learning With AI Learning About AI
Court Decision	New Jersey v. T.L.O. (1985) 469 U.S. 325
CSBA Publication	Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
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
Website	CSBA District and County Office of Education Legal Services
Website	U.S. Department of Education
Website	Federal Trade Commission, Children's Online Privacy Protection
Website	Federal Communications Commission
Website	CSBA
Website	Center for Safe and Responsible Internet Use
Website	California Governor's Office of Emergency Services
Website	California Department of Education
Website	California Coalition for Children's Internet Safety
Website	American Library Association

Cross References	Description
4040	Acceptable Use Of Technology
4040-E(1)	Acceptable Use Of Technology
5131.2	Bullying
5131.2	Bullying
5131.9	Academic Honesty
5145.12	Search And Seizure
5145.12	Search And Seizure
5145.3	Nondiscrimination/Harassment
5145.3	Nondiscrimination/Harassment
5145.7	Sexual Harassment
5145.7	Sexual Harassment
5145.7-E(1)	Sexual Harassment
5145.9	Hate-Motivated Behavior
6154	Homework/Makeup Work
6162.5	Student Assessment

SAN LUIS OBISPO COUNTY
OFFICE OF EDUCATION
LEADERSHIP ▪ COMMUNITY ▪ SERVICE
JAMES J. BRESCIA, ED. D., SUPERINTENDENT

STUDENT PROGRAMS & SERVICES

ACCEPTABLE USE AGREEMENT AND RELEASE OF COUNTY OFFICE OF EDUCATION FROM LIABILITY (STUDENTS)

The County Office of Education (COE) authorizes students to use technology as defined in Superintendent Policy 6163.4 - Student Use Of Technology. The use of COE technology is a privilege permitted at the COE's discretion and is subject to the conditions and restrictions set forth in applicable Superintendent/Board policies, administrative regulations, and this Agreement. The COE reserves the right to suspend access at any time, without notice, for any reason.

The COE expects all students to use technology responsibly in order to avoid potential problems and liability. The COE may place reasonable restrictions on the sites, material, and/or information that students may access through the system.

The COE makes no guarantee that the functions or services provided by or through the COE will be without defect. In addition, the COE is not responsible for financial obligations arising from unauthorized use, or misuse, of the system.

Each student who is authorized to use COE technology and the student's parent/guardian shall sign this Agreement, which indicates that the student has read and understands the Agreement and Superintendent Policy 6163.4 - Student Use of Technology.

Student Obligations and Responsibilities

Students are expected to use COE technology safely, responsibly, and for educational purposes only, and in accordance with the accompanying Superintendent policy and applicable copyright laws. The student in whose name COE technology is issued is responsible for its proper use at all times. Students shall not share their assigned online services account information, passwords, or other information used for identification and authorization purposes, and shall use the system only under the account to which they have been assigned.

Students shall not gain unauthorized access to the files or equipment of others, access electronic resources by using another person's name or electronic identification, or send anonymous electronic communications. Furthermore, students shall not attempt to access any data, documents, emails, or programs in the COE's system for which they do not have authorization.

Students are prohibited from using COE technology for improper purposes, including, but not limited to, use of COE technology to:

1. Access, post, display, create, or otherwise use material that is discriminatory, libelous, defamatory, obscene, sexually explicit, or disruptive

2. Bully, harass, intimidate, or threaten other students, staff, or other individuals ("cyberbullying")

3. Disclose, use, or disseminate personal identification information (such as name, address, email, telephone number, Social Security number, or other personal information) of another student, staff member, or other person with the intent to threaten, intimidate, harass, or ridicule that person

4. Share confidential information or personally identifiable information with an open artificial intelligence (AI) system of themselves, another student, staff member, or other person

5. Adjust the privacy settings on any technology tool or AI app unless directed to do so by a teacher or staff member

6. Violate the direction of teachers or other staff members, age restrictions, or the intended use of the technology

7. Infringe on copyright, license, trademark, patent, or other intellectual property rights

8. Intentionally disrupt or harm COE technology or other COE operations (such as destroying COE equipment, placing a virus on COE computers, adding or removing a computer program without permission from a teacher or other COE personnel, changing settings on shared computers)

9. Install unauthorized software

10. "Hack" into the system to manipulate data of the COE or other users

11. Engage in or promote any practice that is unethical or violates any law or Superintendent/Board policy, administrative regulation, or COE practice

Privacy

Since the use of COE technology is intended for educational purposes, students shall not have any expectation of privacy in any use of COE technology.

The COE reserves the right to monitor and record all use of COE technology, including, but not limited to, access to the Internet or social media, Internet searches, browsing history, use of AI, communications sent or received from COE technology, or other uses. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Students should be aware that, in most instances, their use of COE technology (such as web searches and emails) cannot be erased or deleted.

All passwords created for or used on any COE technology are the sole property of the COE. The creation or use of a password by a student on COE technology does not create a reasonable expectation of privacy.

Personally Owned Devices

If a student uses a personally owned device to access COE technology, the student shall abide by all applicable Superintendent/Board policies, administrative regulations, and this Acceptable Use Agreement. Any such use of a personally owned device may subject the contents of the device and

any communications sent or received on the device to disclosure pursuant to a lawful subpoena or public records request.

Reporting

If a student becomes aware of any security problem (including, but not limited to a cyberattack, phishing, or any compromise of the confidentiality of any login or account information) or misuse of COE technology, the student shall immediately report such information to the teacher or other COE personnel.

Consequences for Violation

Violations of the law, Superintendent/Board policy, or this Agreement may result in revocation of a student's access to COE technology and/or discipline, up to and including suspension or expulsion. In addition, violations of the law, Superintendent/Board policy, or this Agreement may be reported to law enforcement agencies as appropriate.

Student Acknowledgment

I have received, read, understand, and agree to abide by this Agreement and other applicable laws and COE policies and regulations governing the use of COE technology. I understand that there is no expectation of privacy when using COE technology. I further understand that any violation may result in loss of user privileges, disciplinary action, and/or appropriate legal action.

Name: _____ Grade: _____
(Please print)

School: _____

Signature: _____ Date: _____

Parent or Legal Guardian Acknowledgment

If the student is under 18 years of age, a parent/guardian must also read and sign the agreement.

As the parent/guardian of the above-named student, I have read, understand, and agree that my child shall comply with the terms of the Agreement. By signing this Agreement, I give permission for my child to use COE technology and/or to access the school's computer network and the Internet. I understand that, despite the COE's best efforts, it is impossible for the school to restrict access to all offensive and controversial materials. I agree to release from liability, indemnify, and hold harmless the school, COE, COE personnel, the County Superintendent of Schools, and the County Board of Education against all claims, damages, and costs that may result from my child's use of COE technology or the failure of any technology protection measures used by the COE. Further, I accept full responsibility for supervision of my child's use of my child's access account if and when such access is not in the school setting.

Name: _____ Date: _____
(Please print)

Signature: _____