Superintendent Policy 6163.4: Student Use Of Technology

Status: ADOPTED

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

The County Superintendent of Schools or designee intends that technological resources provided by the County Office of Education (COE) be used in a safe and responsible manner in support of the instructional program and for the advancement of student learning. All students using these resources shall receive instruction in their proper and appropriate use.

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.

The County Superintendent of Schools or designee shall notify students and parents/guardians 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.

COE technology includes, but is not limited to, computers, the COE's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through COE-owned or personally owned equipment or devices.

Before a student is authorized to use COE technology, the student and his/her 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 their use of COE technology, including, but not limited to, computer files, email, text messages, instant messaging, and other electronic communications, 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 use of the 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.

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

Whenever a student is found to have violated Superintendent policy or the COE'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 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.

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

Internet Safety

The County Superintendent of Schools or designee shall ensure that all COE 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)

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.

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 County Superintendent of Schools 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.

Federal References	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 References	Description
Court Decision	New Jersey v. T.L.O., (1985) 469 U.S. 325
CSBA Publication	Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
Federal Trade Commission Publication	How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
Website	U.S. Department of Education - https://simbli.eboardsolutions.com/SU/XcSsJimoslsh3XhJKy4tplus7wplusA==
Website	Federal Trade Commission, Children's Online Privacy Protection - https://simbli.eboardsolutions.com/SU/eQpViE31H157EJ2W3Pr6hg==
Website	Federal Communications Commission - https://simbli.eboardsolutions.com/SU/rFmFn0jtplusslshkbdn8jDPcIIg==
Website	CSBA - https://simbli.eboardsolutions.com/SU/W3QxkK2FPsDsQBnMIENxGg==
Website	Center for Safe and Responsible Internet Use - https://simbli.eboardsolutions.com/SU/SYNvZCFDU9rOyHBP2bWINA==
Website	California Department of Education - https://simbli.eboardsolutions.com/SU/os2jq5DcA2RawmY2VZ5FZQ==
Website	California Coalition for Children's Internet Safety - https://simbli.eboardsolutions.com/SU/a1CbmypnLBtn39tsoqi9eA==
Website	American Library Association - https://simbli.eboardsolutions.com/SU/ziXdKiQzPM5ZnufeaKplus7jQ==

State References	Description
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

Exhibit 6163.4-E(2): Student Use Of Technology

Status: ADOPTED

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

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

The County Office of Education authorizes students to use technology owned or otherwise provided by the COE as necessary for instructional purposes. 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 Acceptable Use 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.

Each student who is authorized to use COE technology and his/her parent/guardian shall sign this Acceptable Use Agreement as an indication that they have read and understand the agreement.

Definitions

COE technology includes, but is not limited to, computers, the COE's computer network including servers and wireless computer networking technology (wi-fi), the Internet, email, USB drives, wireless access points (routers), tablet computers, smartphones and smart devices, telephones, cellular telephones, personal digital assistants, pagers, MP3 players, wearable technology, any wireless communication device including emergency radios, and/or future technological innovations, whether accessed on or off site or through COE-owned or personally owned equipment or devices.

Student Obligations and Responsibilities

Students are expected to use COE technology safely, responsibly, and for educational purposes only. 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 are prohibited from using COE technology for improper purposes, including, but not limited to, use of COE technology to:

1. Access, post, display, 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, 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. Infringe on copyright, license, trademark, patent, or other intellectual property rights

5. 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)

6. Install unauthorized software

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

8. Engage in or promote any practice that is unethical or violates any law or Supererintendent/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, 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, he/she shall abide by all applicable 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 (such as any compromise of the confidentiality of any login or account information) or misuse of COE technology, he/she 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 Acceptable Use 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 Acceptable Use 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, and COE personnel 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 his/her access account if and when such access is not in the school setting.

Name: _____ Date: _____
(Please print)
Signature: _____

Federal References	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 References	Description
Court Decision	New Jersey v. T.L.O., (1985) 469 U.S. 325
CSBA Publication	Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007
Federal Trade Commission Publication	How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000
Website	U.S. Department of Education - https://simbli.eboardsolutions.com/SU/XcSsJimoslsh3XhJKy4tplus7wplusA==
Website	Federal Trade Commission, Children's Online Privacy Protection - https://simbli.eboardsolutions.com/SU/eQpViE31H157EJ2W3Pr6hg==
Website	Federal Communications Commission - https://simbli.eboardsolutions.com/SU/rFmFn0jtplusslshkbdn8jDPcIIg==
Website	CSBA - https://simbli.eboardsolutions.com/SU/W3QxkK2FPsDsQBnMIENxGg==
Website	Center for Safe and Responsible Internet Use - https://simbli.eboardsolutions.com/SU/SYNvZCFDU9rOyHBP2bWINA==
Website	California Department of Education - https://simbli.eboardsolutions.com/SU/os2jq5DcA2RawmY2VZ5FZQ==
Website	California Coalition for Children's Internet Safety - https://simbli.eboardsolutions.com/SU/a1CbmypnLBtn39tsoqi9eA==
Website	American Library Association - https://simbli.eboardsolutions.com/SU/ziXdKiQzPM5ZnufeaKplus7jQ==

State References	Description
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