Policy 6163.4: Student Use Of Technology

Original Adopted Date: 2/14/2024

The Governing 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. 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 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.

District technology includes, but is not limited to, computers, the district'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 district-owned or personally owned equipment or devices.

Before a student is authorized to use district 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 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.

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 their use of district 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 district for the purpose of ensuring proper use. Students have no reasonable expectation of privacy in use of the 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.

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 BP/AR 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

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)

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 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"
- 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 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.

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

Ed. Code 49073.6 <u>Student records; social media</u>

Ed. Code 51006 <u>Computer education and resources</u>

Ed. Code 51007 <u>Programs to strengthen technological skills</u>

Ed. Code 60044 Prohibited instructional materials

Pen. Code 313 <u>Harmful matter</u>

Pen. Code 502 <u>Computer crimes; remedies</u>

Pen. Code 632 <u>Eavesdropping on or recording confidential communications</u>

Pen. Code 653.2 <u>Electronic communication devices; threats to safety</u>

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

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>CSBA District and County Office of Education Legal Services</u>

Website <u>California Coalition for Children's Internet Safety</u>

Website Center for Safe and Responsible Internet Use

Website Federal Trade Commission, Children's Online Privacy

<u>Protection</u>

Website American Library Association

Website <u>Federal Communications Commission</u>

Website <u>California Department of Education</u>

Website <u>U.S. Department of Education</u>

Website <u>CSBA</u>

Cross References

Code 0440	Description District Technology Plan
0440	<u>District Technology Plan</u>
1113	<u>District And School Websites</u>
1113	<u>District And School Websites</u>
1113-E(1)	District And School Websites
1114	District-Sponsored Social Media
1114	<u>District-Sponsored Social Media</u>
3260	Fees And Charges
3260	Fees And Charges
3512	Equipment
3512-E(1)	Equipment
4040	Employee Use Of Technology
4040-E(1)	Employee Use Of Technology
4131	Staff Development
5125	Student Records
5125	Student Records
5125.2	Withholding Grades, Diploma Or Transcripts
5131	Conduct
5131.2	Bullying
5131.2	Bullying
5131.8	Mobile Communication Devices
5131.9	Academic Honesty
5144	<u>Discipline</u>
5144	<u>Discipline</u>
5144.1	Suspension And Expulsion/Due Process
5144.1	Suspension And Expulsion/Due Process
5144.2	Suspension And Expulsion/Due Process (Students With Disabilities)
5145.12	Search And Seizure
5145.12	Search And Seizure
5145.3	Nondiscrimination/Harassment
5145.3	Nondiscrimination/Harassment
5145.7	<u>Sexual Harassment</u>

5145.7	Sexual Harassment
5145.9	Hate-Motivated Behavior
5148.2	Before/After School Programs
5148.2	Before/After School Programs
6142.8	Comprehensive Health Education
6142.8	Comprehensive Health Education
6154	Homework/Makeup Work
6162.5	Student Assessment
6162.6	Use Of Copyrighted Materials
6162.6	Use Of Copyrighted Materials
6162.8	Research
6162.8	Research
6163.1	Library Media Centers