

## INSTRUCTION

### Student Use of Technology

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.

*(cf. 0440 - District Technology Plan)*

*(cf. 1113 - District and School Web Sites)*

*(cf. 1114 - District-Sponsored Social Media)*

*(cf. 4040 - Employee Use of Technology)*

*(cf. 6163.1 - Library Media Centers)*

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.

*(cf. 6162.6 - Use of Copyrighted Materials)*

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.

*(cf. 5145.12 - Search and Seizure)*

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.

*(cf. 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.

*(cf. 5125.2 - Withholding Grades, Diploma or Transcripts)*

*(cf. 5144 - Discipline)*

*(cf. 5144.1 - Suspension and Expulsion/Due Process)*

*(cf. 5144.2 - Suspension and Expulsion/Due Process (Students with Disabilities))*

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 6777; 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

(cf. 5131 - Conduct)  
 (cf. 5131.2 - Bullying)  
 (cf. 5145.3 - Nondiscrimination/Harassment)  
 (cf. 5145.7 - Sexual Harassment)  
 (cf. 5145.9 - Hate-Motivated Behavior)

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.

*Legal Reference:*

*EDUCATION CODE*  
 49073.6 Student records; social media  
 51006 Computer education and resources  
 51007 Programs to strengthen technological skills  
 60044 Prohibited instructional materials  
*PENAL CODE*  
 313 Harmful matter  
 502 Computer crimes, remedies  
 632 Eavesdropping on or recording confidential communications  
 653.2 Electronic communication devices, threats to safety  
*UNITED STATES CODE, TITLE 15*  
 6501-6506 Children's Online Privacy Protection Act  
*UNITED STATES CODE, TITLE 20*  
 6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:  
 6777 Internet safety  
*UNITED STATES CODE, TITLE 47*  
 254 Universal service discounts (E-rate)  
*CODE OF FEDERAL REGULATIONS, TITLE 16*  
 312.1-312.12 Children's Online Privacy Protection Act  
*CODE OF FEDERAL REGULATIONS, TITLE 47*  
 54.520 Internet safety policy and technology protection measures, E-rate discounts  
*COURT DECISIONS*  
 New Jersey v. T.L.O., (1985) 469 U.S. 325

*Management Resources:*

*CSBA PUBLICATIONS*

*Cyberbullying: Policy Considerations for Boards, Policy Brief, July 2007*

*FEDERAL TRADE COMMISSION PUBLICATIONS*

*How to Protect Kids' Privacy Online: A Guide for Teachers, December 2000*

*WEB SITES*

*CSBA: <http://www.csba.org>*

*American Library Association: <http://www.ala.org>*

*California Coalition for Children's Internet Safety: <http://www.cybersafety.ca.gov>*

*Center for Safe and Responsible Internet Use: <http://csriu.org>*

*Federal Communications Commission: <http://www.fcc.gov>*

*Federal Trade Commission, Children's Online Privacy Protection:*

*<http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>*

*U.S. Department of Education: <http://www.ed.gov>*

Policy adopted: 7/23/02

Policy revised: 1/10/06; 2/14/06; 4/22/08; 10/9/12; 5/9/17