STUDENT USE OF TECHNOLOGY

The Governing Board intends that technological resources provided by the district be used in a safe, responsible and proper manner in support of the instructional programs and for the advancement of student learning. The Governing Board recognizes that technology provides ways to access the most current and extensive sources of information and enables students to practice skills and to develop reasoning and problem-solving abilities. In addition, electronic resources foster workplace skills that may be transferable to new technologies.

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 district regulations 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 the district's technological resources, the student and his/her parent/guardian shall sign and return the Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree not to hold the district or any district staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or user mistakes or negligence. They shall also agree to indemnify and hold harmless the district and district personnel 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 their 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.

STUDENT USE OF TECHNOLOGY

Whenever a student is found to have violated Board policy or regulation, or the 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 shall regularly review and update this policy, the accompanying administrative regulation, and other relevant 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.

Use of District Computers for Online Services/Internet Safety

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet 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. Staff shall supervise students while they are using online services and may have teacher aides, student aides, and volunteers assist in the supervision.

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)

STUDENT USE OF TECHNOLOGY

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, harassing, or that could be construed as harassment or disparagement of others based on their race/ethnicity, national origin, sex, gender, gender identity, gender expression, 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 personal 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.

Student use of district technology to access social networking sites is prohibited. To the extent possible, the Superintendent or designee shall block access to such sites on district computers with Internet access.

Harassment or bullying of student and staff, including, but not limited to, cyberbullying, intimidation, hazing or initiation activity, extortion, or any other verbal, written, or physical conduct that causes or threatens to cause violence, bodily harm, or substantial disruption, in accordance with this section entitled “Bullying/Cyberbullying” below:

Cyberbullying includes the transmission of communications, posting of harassing messages, direct threats, or other harmful texts, sounds, or images on the Internet, social networking sites, or other digital technologies using a telephone, computer, or any wireless communication device. Cyberbullying also includes breaking into another person’s electronic account and assuming that person’s identity in order to damage that person’s reputation.

STUDENT USE OF TECHNOLOGY

District staff is expected to provide appropriate supervision to enforce standards of conduct and, if they observe or receive a report of a violation of these standards, to immediately intervene or call for assistance. If a District staff believes a matter has not been resolved, he/she shall refer the matter to his/her supervisor or administrator for further investigation.

STUDENT USE OF TECHNOLOGY

Bullying/Cyberbullying

The Governing Board desires to prevent bullying and cyberbullying by establishing a positive, collaborative school climate and clear rules for student conduct.

The district may provide students with instruction, in the classroom or other educational settings, that promotes communication, social skills, and assertiveness skills and educates students about appropriate online behavior and strategies to prevent and respond to bullying and cyberbullying.

School staff shall receive related professional development, including information about early warning signs of harassing/intimidating behaviors and effective prevention and intervention strategies. Parents/guardians, students, and community members also may be provided with similar information.

Students may submit a verbal or written complaint of conduct they consider to be bullying to a teacher or administrator. Complaints of bullying shall be investigated and resolved in accordance with the district's board policies.

When a student is suspected of or reported to be using electronic or digital communications to engage in cyberbullying against other students or staff, or to threaten district property, the investigation shall include documentation of the activity, identification of the source, and specific facts or circumstances that explain the impact or potential impact on school activity, school attendance, or the targeted student's educational performance.

Students shall be encouraged to save and print any messages sent to them that they feel constitute cyberbullying and to notify a teacher, principal, or other employee so that the matter may be investigated.

Any student who engages in cyberbullying on school premises, or off campus in a manner that causes or is likely to cause a substantial disruption of a school activity or school attendance, shall be subject to discipline in accordance with district policies and regulations. If the student is using a social networking site or service that has terms of use

that prohibit posting of harmful material, the Superintendent or designee also may file a complaint with the Internet site or service to have the material removed.

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

STUDENT USE OF TECHNOLOGY

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

Board Adopted: 09/23/1997
Revised: 05/30/2012
Board Adopted: 06/29/2012
Revised: 06/13/2017
Board Adopted: 06/27/2017