Trinity Alps USD
Board Policy
Student Use Of Technology

BP 6163.4
Instruction

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 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
   (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
7101-7122 Student Support and Academic Enrichment Grants
7131 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

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 Trade Commission, Children's Online Privacy Protection:
http://www.ftc.gov/privacy/privacyinitiatives/childrens.html

(7/07 3/09) 7/15

Policy TRINITY ALPS UNIFIED SCHOOL DISTRICT
Adopted: October 14, 2009 Weaverville, California
Revised: August 8, 2012
Revised: March 14, 2018
The principal or designee shall oversee the maintenance of each school's technological resources and may establish guidelines and limits on their use. All instructional staff shall receive a copy of this administrative regulation, the accompanying Board policy, and the district's Acceptable Use Agreement describing expectations for appropriate use of the system and shall also be provided with information about the role of staff in supervising student use of technological resources. All students using these resources shall receive instruction in their proper and appropriate use.

(cf. 0440 - District Technology Plan)
(cf. 4040 - Employee Use of Technology)
(cf. 4131 - Staff Development)
(cf. 4231 - Staff Development)
(cf. 4331 - Staff Development)

Teachers, administrators, and/or library media specialists shall prescreen technological resources and online sites that will be used for instructional purposes to ensure that they are appropriate for the intended purpose and the age of the students.

(cf. 6163.1 - Library Media Centers)

Online/Internet Services: User Obligations and Responsibilities

Students are authorized to use district equipment to access the Internet or other online services in accordance with Board policy, the user obligations and responsibilities specified below, and the district's Acceptable Use Agreement.

1. The student in whose name an online services account is issued is responsible for its proper use at all times. Students shall keep personal account numbers and passwords private and shall only use the account to which they have been assigned.

2. Students shall use the district's system safely, responsibly, and primarily for educational purposes.

3. Students shall not access, post, submit, publish, or display 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.
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)

4. Unless otherwise instructed by school personnel, students shall not disclose, use, or disseminate personal identification information about themselves or others when using email, chat rooms, or other forms of direct electronic communication. Students are also cautioned not to disclose such information by other means to individuals contacted through the Internet without the permission of their parents/guardians.

Personal information includes the student's name, address, telephone number, Social Security number, or other individually identifiable information.

5. Students shall not use the system to encourage the use of drugs, alcohol, or tobacco, nor shall they promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

(cf. 3513.3 - Tobacco-Free Schools)

6. Students shall not use the system to engage in commercial or other for-profit activities.

7. Students shall not use the system to threaten, intimidate, harass, or ridicule other students or staff.

(cf. 5131 - Conduct)

8. Copyrighted material shall be posted online only in accordance with applicable copyright laws. Any materials utilized for research projects should be given proper credit as with any other printed source of information.

(cf. 5131.9 - Academic Honesty)
(cf. 6162.6 - Use of Copyrighted Materials)

9. Students shall not intentionally upload, download, or create computer viruses and/or maliciously attempt to harm or destroy district equipment or materials or manipulate the data of any other user, including so-called "hacking."

(cf. 5131.5 - Vandalism, Theft and Graffiti)
10. Students shall not attempt to interfere with other users' ability to send or receive email, nor shall they attempt to read, delete, copy, modify, or use another individual's identity.

11. Students shall report any security problem or misuse of the services to the teacher or principal.

The district reserves the right to monitor use of the district's systems for improper use without advance notice or consent. Students shall be informed that computer files and electronic communications, including email, are not private and may be accessed by the district for the purpose of ensuring proper use.

(cf. 5145.12 - Search and Seizure)

Whenever a student is found to have violated Board policy, administrative regulation, 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 technological resources, as appropriate. Inappropriate use also may result in disciplinary action and/or legal action in accordance with law and Board policy.

(cf. 5144 - Discipline)
(cf. 5144.1 - Suspension and Expulsion/Due Process)
(cf. 5144.2 - Suspension and Expulsion/Due Process: Students with Disabilities)

Regulation TRINITY ALPS UNIFIED SCHOOL DISTRICT
approved: October 14, 2009 Weaverville, California
Revised: August 8, 2012
deleted: March 14, 2018