

La Canada USD

Board Policy

Student Use Of Technology

BP 6163

The Governing Board recognizes that technology provides ways to access the most current and extensive sources of information. Technology also enables students to practice skills and to develop reasoning and problem-solving abilities. Every effort shall be made to provide equal access to technology throughout the district's schools and classes.

The Board intends that technological resources provided by the district be used in a safe, responsible, and proper manner in support of the instructional program and for the advancement of student learning.

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district computers, user obligations and responsibilities, and consequences of unauthorized use and/or unlawful activities in accordance with district regulations and the district's Student Technology and the Internet Responsible Use agreement.

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.

Before using the district's online resources, each student and his/her parent/guardian shall sign and return a Responsible Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree to not hold the district responsible and shall agree to indemnify and hold harmless the district and all district personnel for the failure of any technology protection measures, loss of service, violations of copyright restrictions, users' mistakes or negligence, or any costs incurred by users.

(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, school accounts, computer files, digital 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)

~~Use of District Computers for Online Services/Internet Access~~ Internet Safety

The Board intends that the internet and other online resources provided by the district be used to support the instructional program and further student learning.

The Superintendent or designee shall ensure that all district computers with Internet access and 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. Student owned devices using the district network will also have filtered Internet. When using either district owned devices or student owned devices on the district network, Internet searches are logged. Filtering and logs do not extend off of the district network. (20 USC 7001, 47 USC 254)

The Superintendent or designee shall establish regulations governing student access to technology that are age appropriate. These regulations shall prohibit access to harmful matter on the internet which may be obscene or pornographic and preclude other misuses of the system. In addition, these regulations shall establish the fact that users have no expectation of privacy and that district staff may monitor or examine all system activities to ensure proper use of the system. Students who fail to abide by district rules shall be subject to disciplinary action, revocation of user access to district technology services and tools, and legal action as appropriate.

To reinforce these measures, the superintendent or designee shall implement rules and procedures designed to restrict students' access to harmful or inappropriate manner on the Internet and to ensure that students do not engage in unauthorized or unlawful online activities. Staff shall supervise students while using online services and may ask teacher aides and student aides to assist in this 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)

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 also establish regulations and guidelines to address the safety and security of students' information when using email, chat rooms, and other forms of electronic communication.~~

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 may 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 computers to access public, unmonitored 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. The district may provide access to private, district monitored and protected social networking sites for the purpose of fostering online classroom learning and collaboration while teaching appropriate online behavior.

In order to help ensure that the district adapts to changing technologies and circumstances, the Superintendent or designee shall regularly review this policy, the accompanying administrative regulation, the Student Technology and Internet Responsible Use Agreement, and other procedures. He/she shall also monitor the district's filtering software to help ensure its effectiveness.

Legal Reference:

EDUCATION CODE

49073.6 Student records; social media

51006 Computer education and resources

51007 Programs to strengthen technological skills

51870-51874 Education technology
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

~~MY SPACE.COM PUBLICATIONS~~

~~The Official School Administrator's Guide to Understanding MySpace and Resolving Social Networking Issues~~

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>

California Department of Education: <http://www.cde.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>

Web Wise Kids: <http://www.webwisekids.org>

Common Sense Media <https://www.commonsense.org/>

Policy LA CAÑADA UNIFIED SCHOOL DISTRICT

adopted: ~~July 10, 2012~~ **February 13, 2018** La Cañada Flintridge, California

(7/12)