

Student Use of Technology

The Board of Education recognizes that technology provides staff and students 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. In addition, the use of electronic resources, such as the Internet and e-mail, foster workplace skills that may be transferable to new technologies.

The Board of Education 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.

Before using on-line services, the students and parent/guardian shall sign an Electronic Information Services Acceptable Use Agreement indicating that the student understands and agrees to abide by specified user obligations and responsibilities.

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 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.

Student Use of Technology

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.

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.

Legal References: Education Code 51006; 51007; 60011; 60013; 60017.1; 60044
Penal Code 632
United States Code, Title 20, 6801-7005

Policy Adopted: 10/01/1996
Policy Amended: 08/14/2001; 10/15/2002; 04/11/2017

(Formerly BP 6165)