

Instruction

Student Use Of Technology

The Board of Education believes that effective use of technology is integral to the education and development of students. In order to promote digital citizenship, the Board recognizes that students must have access to the latest digital tools and receive instruction that allows students to positively engage with technology in ways that respect human rights and avoids Internet dangers. Technological resources provided to students, including technology based on artificial intelligence (AI), shall be aligned to District goals, objectives, and academic standards. The use of technology shall augment the use of Board adopted instructional materials.

The 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. Students shall be allowed to use such technology, including AI technology, in accordance with District policies, including, but not limited to, policies on academic honesty, data privacy, nondiscrimination, and copyright protections. All students using these resources shall receive instruction in the proper and appropriate use of technology. Such instruction shall incorporate students' responsibilities regarding academic honesty, honoring copyright provisions, assessing the reliability and accuracy of information, protecting personal data, and the potential for biases and errors in artificially generated content.

District technology includes, but is not limited to, computer hardware, software, or software as a service provided or paid for by the District, whether accessed on or off site or through District-owned or personally owned equipment or devices, including tablets and laptops; computer servers, wireless access points (routers), and wireless computer networking technology (wi-fi); the Internet; email; applications (apps), including AI apps; telephones, cellular telephones, smartphones, smart devices, and wearable technology; or any wireless communication device, including radios.

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 Board Policy, District regulations and the District's Acceptable Use Agreement.

The Superintendent or designee shall provide age-appropriate instruction regarding the District's acceptable use agreement.

BP 6163.4(b)

Before using the District's technological resources, each student and his/her parent/guardian shall sign and return an Acceptable Use Agreement specifying user obligations and responsibilities. In that agreement, the student and his/her parent/guardian shall agree to not hold the District or any District staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' 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 the use of District technology, as defined above, 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 the use of 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.

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, 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)

The Board desires to protect students from access to inappropriate matter on the Internet. 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.

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:

BP 6163.4(c)

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 regularly review current guidance regarding cybersecurity, data privacy, and digital media awareness and incorporate recommended practices into the District's processes and procedures related to the protection of the District's network infrastructure, the monitoring and response to cyberattacks, ensuring data privacy, and monitoring suspicious and/or threatening digital media content, in accordance with Board Policy 5125 - Student Records.

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.

Student use of District computers 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.

Staff shall supervise students while they are using online services and may ask teacher aides, student aides, and volunteers to assist in this supervision.

Legal Reference:

CIVIL CODE

3120-3123 Digital equity bill of rights

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

CODE OF FEDERAL REGULATIONS, TITLE 16

312.1-312.12 Children's Online Privacy Protection Act

CODE OF FEDERAL REGULATIONS, TITLE 16

54.520 Internet safety policy and technology protection measures; E-rate discounts

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)