Student Use of Technology

Technology, which includes the Internet, electronic communications, social media, applications and artificial intelligence tools has vast potential to support curriculum and student learning. The Board of Education believes appropriate technology should be used in schools as a learning resource to educate and to inform.

Use of technology requires students to think critically, analyze information, write clearly, use problem-solving skills and hone computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals and locate material to meet educational and personal information needs.

Through the use of technology, students may access materials and information from many sources, including some that may be harmful to students. Although it is impossible to predict with certainty what information students might locate or come in contact with, the district will take reasonable steps to protect students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, as defined by the Board. Students are responsible for their own use of district technology devices to avoid contact with material or information that may be harmful to minors. For purposes of this policy, "district technology device" means any district-owned computer, hardware, software, or other technology that is used for learning purposes and has access to the Internet.

Blocking or Filtering Obscene, Pornographic and Harmful Information

Technology that blocks or filters material and information that is obscene, pornographic or otherwise harmful to minors, as defined by the Board, has been installed on all district computers having Internet or electronic communications access. Students must report access to material and information that is inappropriate, offensive or otherwise in violation of this policy to a staff member. If a student becomes aware of other students accessing such material or information, they must report it to a staff member.

No Expectation of Privacy

District technology devices are owned by the district and are intended for educational purposes at all times. Students have no expectation of privacy when using district technology devices. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district technology devices, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through district technology devices remains the property of the school district.

Unauthorized and Unacceptable Uses

Students must use district technology devices in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of district technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following.

Students must not access, create, transmit, retransmit or forward material or information:

- that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons;
- that is not related to district education objectives;
- that contains pornographic, obscene or other sexually oriented materials, either as pictures or writings;
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the district's nondiscrimination policies;
- for personal profit, financial gain, advertising, commercial transaction or political purposes;
- that plagiarizes the work of another;
- that uses inappropriate or profane language;
- that is knowingly false or could be construed as intending to purposely damage another person's reputation;

- in violation of any federal or state law or district policy, including but not limited to copyrighted material and material protected by trade secret;
- that contains personal information about themselves or others, including information protected by confidentiality laws;
- that impersonates another or transmits through an anonymous remailer; or
- that accesses fee services without specific permission from the system administrator.

Security

Security on district technology devices is a high priority. Students who identify a security problem while using district technology devices must immediately notify a staff member. Logging on to the Internet or electronic communications as a system administrator is prohibited.

Students must not:

- use another person's password or any other identifier;
- gain or attempt to gain unauthorized access to district technology devices;or
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users.

Any user identified as a security risk, or as having a history of problems with technology, may be denied access to the Internet, electronic communications and/or district technology devices.

Safety

In the interest of student safety and security, the district will educate students and parents about appropriate online behavior, including cyberbullying awareness and response; interacting on social media; appropriate use of artificial intelligence and other forms of direct electronic communications.

Students must not reveal personal information, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of a staff member, students must not use their last name or any other information that might allow another person to locate him or her. Students must not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

Vandalism

Vandalism will result in cancellation of privileges and may result in legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion and other disciplinary interventions. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse or disrupt operation of any network within the school district or any network connected to the Internet, operation of any form of electronic communications, the data contained on any network or electronic communications, the data of another user, usage by another user, or district technology device. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Artificial Intelligence

The district supports student use of Artificial Intelligence (AI) tools that enhance the district's commitment to high-quality learning. Generally, students may use AI tools for explaining concepts, exploring new topics of interest and seeking guidance on research directions. Students may be permitted to use AI tools on assignments if clearly stated in the assignment or specified by the teacher. However, students must not rely solely or primarily on AI tools in completion of coursework unless expressly authorized.

In any use of AI, students should be mindful that AI tools are prone to "hallucinations," false answers/information, or outdated, misleading and/or biased information. Thus, students must always verify information provided by AI tools using reliable sources such as textbooks, scientific papers and reputable educational websites.

Students should not upload or input any personal, confidential, propriety or sensitive information into any AI tool. Examples include passwords and other personal information such as names, likenesses, or social security, credit card or bank account numbers.

Specific acceptable and unacceptable uses of AI tools may vary based on new technological developments and students must follow the guidance of the district's administrators. Offenses or violations of this Policy will be addressed by the teacher and administrators.

Unauthorized Content

Students are prohibited from using or possessing any software applications, mobile applications or other content that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees.

Assigning Student Projects and Monitoring Student Use

The district will make reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of technology, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals. Students must have specifically defined objectives and search strategies prior to accessing material and information using technology.

Opportunities will be made available on a regular basis for parents to observe student use of technology in schools.

Student use of technology will be supervised by staff. Staff members assigned to supervise student technology use must have received training in technology safety and monitoring student use.

Student Use is a Privilege

Use of technology demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student use of technology and district technology devices is a privilege, not a right. Failure to follow the use procedures contained in this policy will result in the loss of the privilege to use these tools and restitution for costs associated with damages, and may result in legal action and/or disciplinary action, including suspension and/or expulsion, in accordance with Board policy concerning suspension, expulsion and other disciplinary interventions. The school district may deny, revoke or suspend access to district technology or close accounts at any time.

Students and parents/guardians are required to sign the district's Acceptable Use Agreement annually before the district permits the student's use of technology, including Internet or electronic communications accounts.

School District Makes no Warranties

The school district makes no warranties of any kind, whether express or implied, related to the use of district technology devices, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the district of the content, nor does the district make any guarantee as to the accuracy or quality of information received. The district is not responsible for any damages, losses or costs a student suffers in using technology. This includes loss of data and service interruptions. Use of any information obtained via technology is at the student's own risk.

Adopted: July 1996
Revised: September 1997, February 2003, March 2007, August 2007, April 2009,
January 2013, December 2013, May 12, 2025

LEGAL REFS.: 20 U.S.C. 6751*et seq. (Enhancing Education Through Technology Act of 2001)*
47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
47 C.F.R. Part 54, Subpart F *(Universal Support for Schools and Libraries)*
C.R.S. 22-87-101 *et seq. (Children's Internet Protection Act)*

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
EGAEA, Electronic Communication
JB, Equal Educational Opportunities
JKD/JKE, Suspension/Expulsion of Students (and Other Disciplinary Interventions)