File: GBEE*

Staff Use of Technology

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

The Board of Education supports the use of technology by staff to improve teaching and learning through interpersonal communication, access to information, research, training, collaboration and dissemination of successful educational practices, methods and materials.

Through the use of technology, users may access materials and information from many sources. Staff members are responsible for their own use of district technology devices and must avoid contact with material or information that violates this policy. For purposes of this policy, "district technology device" means any district-owned computer, hardware, software, or other technology that is used for instructional or learning purposes and has access to the Internet.

Blocking or Filtering Obscene, Pornographic and Harmful Information

To protect students from material and information that is obscene, pornographic, or otherwise harmful to minors, as defined by the Board, technology that blocks or filters such material and information has been installed on all district computers having Internet or electronic communications access. Blocking or filtering technology may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

No Expectation of Privacy

District technology devices are owned by the district and are intended for educational purposes and district business at all times. Staff members 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 is the property of the school district.

Public Records

Electronic communications sent and received by district employees may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All employee electronic communications must be monitored to ensure that all public electronic communication records are retained, archived and destroyed in accordance with applicable law.

Unauthorized and Unacceptable Uses

Staff members 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.

Staff members are prohibited from accessing, creating, transmitting, retransmitting or forwarding 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.

Staff members 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 applicable fees.

Security

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

Staff members will 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 staff member 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.

Confidentiality

Staff members must not access, receive, transmit or retransmit material regarding students, parents/guardians, district employees or district affairs that is protected by confidentiality laws unless such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law and district policy. It is imperative that staff members who share confidential student information via electronic communications understand the correct use of the technology, so that confidential records are not inadvertently sent or forwarded to the wrong party. Staff members who use email to disclose student records or other confidential student information in a manner inconsistent with applicable law and district policy may be subject to disciplinary action.

If material is not legally protected but is of a confidential or sensitive nature, great care must be taken to ensure that only those who "need to know" are allowed access to the material. Staff members must handle all employee, student and district records in accordance with applicable district policies.

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA).

Use of Social Media

Staff members may use social media within school district guidelines for instructional purposes, including promoting communications with students, parents/guardians and the community concerning school related activities and for purposes of supplementing classroom instruction. As with any other instructional material, the application/platform and content must be appropriate to the student's age, understanding, and range of knowledge.

Staff members are discouraged from communicating with students through personal social media platforms/applications or texting. Staff members are expected to protect the health, safety and emotional well-being of students and to preserve the integrity of the learning environment. Online or electronic conduct that distracts or disrupts the learning environment or other conduct in violation of this or related district policies may form the basis for disciplinary action up to and including termination.

Use of Artificial Intelligence

The district supports staff use of Artificial Intelligence (AI) tools that enhance the district's commitment to high-quality learning. Staff must follow the direction of the district regarding permissible AI tools, use of AI tools and acceptable and unacceptable uses for staff and students.

Generally, staff may use AI tools for ideas, outlines and to enhance the educational experience, such as supplementing lesson plans, providing differentiated instruction and aiding in curriculum development. Staff is prohibited from relying solely or primarily on AI tools to carry out their work duties, unless expressly authorized.

Staff may only use AI tools that are approved by the district. Staff should carefully evaluate the appropriateness of AI tools for educational purposes on a case-by-case basis, considering its appropriateness for each educational context, accuracy, reliability, and alignment with curriculum standards.

Staff must comply with all applicable federal, state and local student privacy laws, including FERPA and the Colorado Student Data Transparency Act. To that end, staff should not upload or input any confidential, proprietary or sensitive information into any AI tool.

Teachers who suspect plagiarism or use of AI that violates district policy should first have a conversation with a student to ensure that they understand expectations for acceptable use. Teachers should consult with administration to determine appropriate steps to investigate any possible violation of policy.

Vandalism

Vandalism will result in cancellation of privileges and may result in school disciplinary action and/or legal action. 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.

Staff Member Use is a Privilege

Use of technology demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff member 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 disciplinary action and/or legal action. The school district may deny, revoke or suspend access to district technology or close accounts at any time.

Staff members are required to sign the district's Acceptable Use Agreement annually before the district permits the staff member’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 expressed 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 staff

member suffers in using the technology. This includes loss of data and service interruptions. Use of any information obtained via technology is at the staff member's own risk.

Adopted: January 18 2005
Revised: February 2009
Revised: April 19 2006
Revised: September 23 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)*
C.R.S. 24-72-204.5 *(monitoring electronic communications)*

CROSS REFS.: AC, Nondiscrimination/Equal Opportunity
EGAEA, Electronic Communication