

Staff Use of Technology

The Board supports the use of technology, which includes the Internet and electronic communications, social media applications, and artificial intelligence tools by staff to improve interpersonal communication, access to information, research, training and collaboration and dissemination of successful practices, methods and materials relevant to their employment with the EC BOCES.

Through the use of technology, users may access materials and information from many sources. Staff members may take responsibility for their own use of EC BOCES technology devices to avoid contact with material or information that violates this policy. For purposes of this policy, "EC BOCES technology devices" means any EC BOCES-owned computer, hardware, software or other technology that has access to the Internet.

No Expectation of Privacy

EC BOCES technology devices are owned by the EC BOCES and are intended for EC BOCES business at all times. Staff members have no expectation of privacy when using EC BOCES technology devices. The EC BOCES reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of EC BOCES technology devices including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through EC BOCES technology devices shall remain the property of the EC BOCES.

Public Records

Electronic communications sent and received by EC BOCES employees may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All employee electronic communications may 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 may use EC BOCES technology devices in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of EC BOCES 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 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 with regard to race, color, creed, sex, sexual orientation, religion, national origin, ancestry, age, marital status or disability,
- for personal profit, financial gain, advertising, commercial transaction or political purposes,
- that plagiarizes the work of another without express consent,
- 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, 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,
- that accesses fee services without specific permission from the system administrator.

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

Security

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

Staff members may not:

-
- use another person's password or any other identifier;
- gain or attempt to gain unauthorized access to EC BOCES 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 other technology may be denied access to the Internet and electronic communications and/or EC BOCES technology devices.

Confidentiality

Staff members may not access, receive, transmit or retransmit material regarding E C BOCES employees or EC BOCES affairs that is protected by confidentiality laws unless such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law and Board policy.

File: GBEE

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 and EC BOCES records in accordance with applicable Board policies.

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.

Staff 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. Staff 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 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 EC BOCES 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 EC BOCES technology devices.

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 the Internet, electronic communications and EC BOCES 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 EC BOCES may deny, revoke or suspend access to EC BOCES technology or close accounts at any time.

Staff members will be required to sign the EC BOCES's Acceptable Use Agreement annually before EC BOCES permits the staff member's use of technology, including Internet or electronic communications.

BOCES Makes no Warranties

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

EAST CENTRAL BOCES BOARD POLICY

Adopted: June 17, 2015

Revised: April 16, 2025

LEGAL REF.: C.R.S. 24-72-204.5 (*monitoring electronic communications*)

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