Staff Use of the Internet, Electronic Communications and BOCES Technology Devices

The Internet and electronic communications (email, chat rooms and other forms of electronic communication) have vast potential to support curriculum and learning. The Board believes they should be used in schools as a learning resource to educate and to inform.

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

The Internet and electronic communications are fluid environments in which users may access materials and information from many sources. Staff members shall take responsibility for their own use of BOCES technology devices to avoid contact with material or information that violates this policy. For purposes of this policy, "BOCES technology device" means any BOCES-owned computer, hardware, software, or other technology that is used for instructional, learning or business 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, child pornography or otherwise harmful to minors, as defined by the Board, technology that blocks or filters such material and information has been installed on all BOCES technology devices having Internet or electronic communications access. Blocking or filtering technology may be disabled by a supervising teacher, BOCES administrator or BOCES Technology Manager, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18.

BOCES technology devices used only by BOCES staff and not accessible to students, including devices used at the BOCES Central Office, are excluded from the blocking/filtering requirements. Devices used by BOCES staff working at remote locations are also exempt if students have no access. These devices must be physically-secured or "locked," requiring a password to unlock, any time the staff member is away from the device. Remote locations are defined as any locations not in the BOCES Central Office.

No expectation of privacy

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

BOCES staff should also know that personal technology devices, including cell phones, used for business purposes can legally be subpoenaed in case of court actions or investigations related to BOCES business activities. Thus, in the case of legal action, staff members using personal devices for BOCES business may have no expectation of privacy for personal data on those devices.

Public records

Electronic communications sent and received by BOCES employees may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All employee electronic communications shall 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 shall use 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 BOCES technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following.

No staff member shall 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 contains pornographic, obscene or other sexually-oriented materials, either as pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex or excretion
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the BOCES nondiscrimination policies, including “cyber-bullying”
- that is intended to obtain confidential information the staff member is not authorized to access, or cause harm to the BOCES network system or any BOCES technology device, software or data
- that is not related to BOCES objectives, such as for personal profit, financial gain, advertising, commercial transaction or political purposes
- that plagiarizes the work of another
- that uses inappropriate or profane language likely to be offensive to others in the BOCES community

- 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 BOCES policy, including but not limited to software licensing agreements, copyrighted material and material protected by trade secret or other intellectual property laws
- that contains personal information about themselves or others, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account without written permission from that individual and the approval of the Executive Director or Technology Manager
- that impersonates another or transmits through an anonymous remailer
- that accesses fee services without specific permission from the Technology Manager

Security

Security on BOCES technology devices is a high priority. Staff members are expected to take all possible precautions to avoid causing or permitting security vulnerabilities, including physically securing BOCES technology devices and protecting software and data on BOCES devices.

Staff members who identify or suspect a security problem while using BOCES technology devices must immediately notify the Technology Manager. Staff members should not demonstrate the problem to other users.

Logging on to the Internet or electronic communications as a system administrator is prohibited.

Staff members must immediately return technology devices to the Technology Manager at the Technology Manager's request so any security risks or damage can be corrected as quickly as possible.

Staff members shall not:

- use another person's password or any other identifier without the approval of the Technology Manager or the Executive Director
- gain or attempt to gain unauthorized access to BOCES technology devices
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users
- leave BOCES technology devices unattended without logging off or "locking" the computer to prevent unauthorized access to software or data on the device
- open suspicious emails without verifying the emails are legitimate

- visit potentially unsafe websites

Confidentiality

Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians, BOCES employees or 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. When transmitting confidential information, staff members should be aware that email is not considered a secure method of transmission and confidential student information must be transmitted using an approved, secure delivery system. Staff members who use email to disclose student records or other confidential student information in a manner inconsistent with applicable law and Board policy may be subject to disciplinary action.

If material is not legally protected but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a "need to know" are allowed access to the material. Staff members shall handle all employee, student and BOCES records in accordance with applicable Board 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 Personally-Owned Devices for BOCES Business

Staff members may use personal devices, such as cell phones and computers, to conduct BOCES business with proper authorization and up-to-date anti-malware software. Users of personally-owned devices must exercise proper care to protect the security of BOCES data on their devices. If a personal device is lost or stolen, or staff member suspects confidential data may have been compromised in any way, the staff member will immediately report the theft or security breach to the Executive Director and the Manager of Technology.

Use of social media

Staff members may use social media within BOCES 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 shall 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, emails 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 Board policies may form the basis for disciplinary action up to and including termination.

Staff members are discouraged from accessing personal social media accounts using BOCES technology devices.

Vandalism

Vandalism shall 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 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 BOCES technology devices. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized content

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 appropriate registration and payment of any fees.

Staff members are also prohibited from downloading or installing any software applications, including free software, that haven't been approved in writing by the BOCES Technology Manager. If the staff member believes a software application will be beneficial for their job duties, they should contact the Technology Manager to determine if the software will cause harm to BOCES technology devices or software.

Staff member use is a privilege

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff member use of the Internet, electronic communications and BOCES technology devices is a privilege, not a right. Failure to follow the use procedures contained in this policy shall 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 BOCES may deny, revoke or suspend access to BOCES technology or close accounts at any time.

Staff members shall be required to sign the BOCES Acceptable Use Agreement (the Agreement) before Internet or electronic communications accounts shall be issued or access shall be allowed. If changes are made to the Agreement, staff members will be required to sign and agree to the changes.

Adopted: May 12, 2016

LEGAL REFS.: 47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
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