Staff Use of the Internet and Electronic Communications

The Board supports the use of the Internet and electronic communications 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 BOCES.

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 has access to the Internet.

No expectation of privacy

BOCES technology devices are owned by the BOCES and are intended for 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.

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's nondiscrimination policies

- 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 copyrighted material and material protected by trade secret

- 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

- that impersonates another or transmits through an anonymous remailer

- that accesses fee services without specific permission from the system administrator

Security

Security on BOCES technology devices is a high priority. Staff members who identify a security problem while using BOCES technology devices must immediately notify a system administrator. 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 shall not:

- use another person's password or any other identifier

- 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

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, electronic communications and/or BOCES technology devices.

Confidentiality

Staff members shall not access, receive, transmit or retransmit material regarding 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.

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 and BOCES records in accordance with applicable Board policies.

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 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 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's Acceptable Use Agreement annually before Internet or electronic communications accounts shall be issued or access shall be allowed.

BOCES makes no warranties

The 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 BOCES of the content, nor does the BOCES make any guarantee as to the accuracy or quality of information received. The BOCES shall not be 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 the Internet and electronic communications is at the staff member's own risk.

(Adoption Date: September 9, 2015)

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

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