Staff Use of the Internet and Electronic Communications

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

The Board of Education supports the use of the Internet and electronic communications by 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 district technology devices to 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, child pornography or other 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.

Technology protection measures

Staff shall not allow others to have unsupervised access to their district computers, laptops or Internet-ready devices. To ensure that student Internet access on district computers and technology devices is subject to the district’s filtering and technology protection measures, student use of Internet-ready district computers or technology devices shall be primarily restricted to district property and the district’s network. While on district premises, students may use only district networks when using district computers and technology devices. Students shall not be permitted to remove Internet-ready district computers or technology devices from district property unless the devices in question include one or more technology protection measures.

No expectation of privacy

District computer systems and technology devices are owned by the district and are intended for educational purposes and district business at all times. Staff members shall have no expectation of privacy when using the Internet or 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 computer systems and technology devices, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through district computer systems and technology devices shall remain 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 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 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.

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 or 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 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 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 likely to be offensive to others in the school 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 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.

- 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 district technology devices is a high priority. Staff members who identify a security problem while using district technology devices must immediately notify a system administrator. Staff members should not demonstrate the problems to other users.

Staff members shall not:

- use another person's password or any other identifier.
- gain or attempt to gain unauthorized access to district technology devices, district network or district administrative programs.
- 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 or problems with technology, may be denied access to the Internet, electronic communications and/or district technology devices.

Confidentiality

Staff members shall not access, receive, transmit or retransmit material regarding students, parents/guardians or district employees that is protected by confidentiality laws.

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 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). Therefore, the sharing of student records or other confidential information with persons or agencies outside the school district via email is prohibited without prior written consent of the student's parent/guardian, unless disclosure is under an exception to FERPA (see *Board Policy JRA/JRC – Student Records/Release of Information on Students* for detailed information on student records and FERPA). Student records and other confidential information may be shared with other district staff members via email, as long as the staff member with whom the records are shared has a legitimate educational interest in the student and the records are shared for a legitimate educational purpose.

Any student records maintained on district technology, including on the electronic mail system or in any other electronic format are part of the student's record and, as such, are available for parent/guardian review and must be maintained in accordance with FERPA requirements. 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 intentionally use email to disclose student records or other confidential student information in a manner inconsistent with FERPA requirements may be subject to disciplinary action.

Use of social media

Social media is defined as media based on the use of web and mobile technologies that allow for user-generated exchanges of information. With proper administration, social media can foster collaboration and communication as an interactive dialog, enhancing the value of conversations across a global audience.

Applicability

All existing and future policies and behavior guidelines currently applicable to students and staff similarly apply to the online environment. Any employee or associated person engaging in inappropriate conduct involving the use of social media may be subject to discipline up to and including termination.

Professional and personal social media use

Professional social media is a work-related social media activity that can be either school based (e.g., a district principal establishing a social networking page for his/her school, or a teacher establishing a social media site for his/her class), or non-school-based (e.g., a district office establishing a social networking page to communicate with the larger district community).

Personal social media is a non-work-related social media activity (e.g. a district employee establishing a social networking page for his/her personal use).

Employees who engage in strictly personal social media activities must maintain separate professional and personal email addresses, and may not use their professional email address for personal social media activities.

All communications through professional social media tools must remain professional and appropriate, and employees maintain no expectation of privacy with respect to those communications. Employees must obtain their supervisor's approval prior to engaging in a professional social media presence.

Supervisors and their designees are responsible for ensuring access to all professional social media accounts within their school or department, via log-in information and/or administrators' rights when possible.

Professional social media communications will be in compliance with existing district policies and department procedures or directives, including prohibitions on the disclosure of confidential information, and prohibitions on the use of harassing, obscene, discriminatory, defamatory, or threatening language. No confidential or proprietary information about students or staff may be posted by district employees on

social media sites without securing appropriate permission.

In order to maintain a professional and appropriate relationship with students, district employees are strongly encouraged not to communicate with students who are currently enrolled in the district through personal social media activities.

Use of district and school (including all athletic and activities) logos or images on a personal social media website is prohibited; any initial promotion of professional events must be posted on a previously approved professional social media website. Staff are permitted to share the professional postings on their personal social media accounts.

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.

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 applicable fees on district owned technology devices.

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 and, electronic communications and district 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 school district may deny, revoke or suspend access to district technology or close accounts at any time.

Staff members shall be required to sign the district's Acceptable Use Agreement annually before Internet or electronic communications accounts shall be issued or access shall be allowed.

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 school district 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.

Adopted: December 8, 2003
Revised: May 12, 2010
Revised: January 9, 2013
Revised: June 28, 2017
Revised: March 6, 2019

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 School's 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

Staff Use of the Internet and Electronic Communications

(Annual Acceptable Use Agreement)

Staff member

I have read, understand and will abide by the district's policy on Staff Use of the Internet and Electronic Communications. Should I intentionally commit any violation, or in any way misuse my access to the school district's technology devices, including use of the Internet and electronic communications, I understand and agree that my access privileges may be revoked and disciplinary and/or legal action may be taken.

I hereby release the school district from all costs, claims, damages or losses resulting from my use of district technology devices, including use of the Internet and electronic communications, including but not limited to any user fees or charges incurred through the purchase of goods or services.

Your signature on this Acceptable Use Agreement is binding and indicates you have read the school district's policy on Staff Use of the Internet and Electronic Communications and understand its significance.

_____
Staff member's name (printed)

_____ _____
Staff member's signature Date

Issued: December 8, 2003
Revised: March 6, 2019