STAFF USE OF TECHNOLOGY AND ELECTRONIC COMMUNICATIONS

The Internet, social media, and electronic communications (email, texting, discussion forums, and other forms of electronic communication) have vast potential to support curriculum and learning. The Board of Education believes they should be used as a learning resource to educate and to inform.

The Board supports staff use of the technology and electronic communications to improve teaching and learning through:

- Digital Curriculum and Textbooks
- Learning Management Systems
- Subject Specific Practice Applications
- Productivity and Organization Applications
- Teacher-Student School Communications
- Internet Access
- Professional development including the sharing of resources and best practices

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 to avoid contact with material or information that violates this policy.

RESTRICTING OBSCENE, PORNOGRAPHIC AND HARMFUL INFORMATION

To protect students from material and information that is obscene or otherwise harmful to minors, as defined by law such as the federal Children's Internet Protection Act and the Board, software that restricts such material and information regulates all network access and content. Network restrictions may be disabled by a technician or or school/district administrator, as necessary, for purposes of bona fide repair, research, or educational projects being conducted by staff members over the age of 18.

NO EXPECTATION OF PRIVACY

District technology is owned by the district and is intended for educational purposes and district business at all times. Staff members shall have no expectation of privacy when using the technology or electronic communications. The district reserves the right to monitor, inspect, copy, review and store (at any time and without prior notice) all usage of district technology, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through district technology and network systems shall remain the property of the 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. 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 shall use district technology and network systems in a responsible, efficient, ethical, and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following. [Note: *The Board has discretion to determine which uses are unacceptable. The following list provides examples the Board may wish to consider.*]

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 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 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 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, including but not limited to copyrighted material and material protected by trade secret
- that contains very personal information about themselves or others such as information protected by confidentiality laws
- using any other individual’s online accounts 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

Network security and virus/malware protection are high priorities. Staff members who identify a security problem while using the Internet or electronic communications 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

- "Remote in" to another person's computer without their knowledge and consent except in the case of emergency repair or an approved investigation into violations of the Staff Use of Technology and Electronic Communications policy.
- gain or attempt to gain unauthorized access to district technology and/or network systems
- 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 violations of the Staff Use of Technology and Electronic Communications policy, may be denied access to technology and electronic communications.

CONFIDENTIALITY

Staff members shall 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. 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 policies GBJ (Personnel Records and Files), JRA/JRC (Student Records/Release of Information on Students) and EGAEA (Electronic Communication).

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by law, including the Colorado Student Data Transparency and Security Act and the Federal Family Educational Rights and Privacy Act. (See policy JRA/JRC, Student Records/Release of Information on Students for detailed information on student records).

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.

USE OF SOCIAL MEDIA

Staff members may use social media that has been requested and approved as part of the district's Catalog of Digital Learning Resources, within 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 shall be appropriate to the student's age, understanding, and range of knowledge.

Staff members are discouraged from communicating with students through <u>personal</u> 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 of employment.

VANDALISM

Vandalism will result in cancellation of privileges and may result in school disciplinary action, financial responsibility, and/or legal action. Vandalism is defined as any neglectful or malicious attempt to harm, destroy, modify, abuse, or disrupt operation of any district provided or contracted (cloud-based) network, 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-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses, the use of encryption software, or neglecting to properly secure issued devices and therefore making them susceptible to harm or theft.

UNAUTHORIZED SOFTWARE

Staff members are prohibited from using or possessing any software that has been downloaded or is otherwise in the user's possession without appropriate registration and payment of any fees owed to the software owner.

STAFF MEMBER USE IS A PRIVILEGE

Use of district technology and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff member use is a privilege, not a right. Failure to follow the use procedures contained in this policy shall result in 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 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.

DISTRICT MAKES NO WARRANTIES

The district makes no warranties of any kind, whether expressed or implied, related to the use of district technology and network systems, 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 shall not be responsible for any damages, losses, or costs a staff member suffers in using technology 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 September 2, 1998
Revised and recorded March 7, 2018

Legal Refs.: 47 U.S.C. 254(h) (Children's Internet Protection Act of 2000)
47 U.S.C. 231 et seq. (Child Online Protection Act of 2000)
20 U.S.C. 6801 et seq. (Elementary and Secondary Education Act)
C.R.S. 22-87-101 et seq. (Children’s Internet Protection Act)
C.R.S. 24-72-204.5 (monitoring electronic communications)