Staff Responsible Use of the Internet and Electronic Communications

The Internet and electronic communications 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 systems to avoid contact with material or information that violates this policy.

Blocking or filtering obscene, pornographic and harmful information

To protect students from material and information that is obscene, pornography or otherwise harmful to minors, as defined by law, software that blocks or filters such material and information has been installed on the district network. Blocking or filtering software may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects.

No expectation of privacy

District computers and computer systems 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 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 computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through district technology systems 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 retained, archived and destroyed in accordance with applicable law.

Unauthorized and unacceptable uses

Staff members shall use district technology systems in a responsible, efficient, ethical and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of district computers and computer systems 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.
- is not related to district education objectives.
- contains pornographic, obscene or other sexually oriented materials, either as pictures or writings.
- harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in accordance with Board Policy AC.
- is for personal profit, financial gain, advertising, commercial transaction or political purposes.
- plagiarizes the work of another without express consent.
- uses inappropriate or profane language likely to be offensive to others in the school community.
- is knowingly false or could be construed as intending to purposely damage another person's reputation.
- is in violation of any federal or state law, including but not limited to copyrighted material and material protected by trade secret.
- contains personal information about themselves or others, including information protected by confidentiality laws.
- uses another individual's Internet or electronic communications account without written permission from that individual.
- impersonates another or transmits through an anonymous remailer.
- accesses fee services without specific permission from District Technology Services (IT).

Security

Security on district technology systems is a high priority. Staff members who identify a security problem while using the Internet or electronic communications must immediately notify District Technology Services (IT). Staff members should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as an unauthorized 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 district technology 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 problems with other technology systems, may be denied access to the Internet 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. 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.

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 state and federal law, including the Family Educational Rights and Privacy Act (FERPA). (See policy JRA/JRC, Student Records/Release of Information on Students for detailed information on student records).

Disclosure of health or medical information about an employee is strictly prohibited and staff must follow Health Insurance Portability and Accountability Act (HIPAA) rules and regulations.

Use of social media

Staff members may use social media 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 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.

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 or device 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-owned software or hardware. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

Unauthorized software and services

Staff members are prohibited from using or possessing any software or service 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. All license and service conditions must be adhered to.

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 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 before Internet or electronic communications accounts shall be issued or access shall be allowed.

The school district makes no warranties of any kind, whether expressed or implied, related to the use of district computers and computer 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 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: September 27, 1995
Revised: April 10, 2002
Revised: March 9, 2005
Revised: May 12, 2010
Revised: January 9, 2013
Revised: June 10, 2015
Reviewed: November 11, 2015

LEGAL REFS.: 20 U.S.C. 6801 *et seq.* (Enhancing Education through Technology Act of 2001)
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)
47 C.F.R. Part 54, Subpart F (Universal Support for Schools 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
GBJ, Personnel Records and Files
JRA/JRC, Student Records/Release of Information on Students

St. Vrain Valley School District RE-1J, Longmont, Colorado