Staff Use of the Internet and Electronic Communications

The Internet, a global computer network sometimes referred to as the World Wide Web, and electronic communications (e-mail, 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 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 Board believes the educational opportunities inherent in these tools far outweigh the possibility that users may procure material not consistent with the education goals of the District. However, 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 computers and computer 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, pornographic or otherwise harmful to minors, as defined by the Board, a system has been installed to block or filter such material and information from being accessed on all District computers having Internet or electronic communications access. The blocking or filtering system may be bypassed 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 eighteen (18).

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 computers and computer 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 monitored in accordance with EGAEA-R to ensure that all public electronic communication records are retained, archived and destroyed in accordance with state law.

Unauthorized and unacceptable uses

Staff members shall use District computers and computer 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 computers 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
- 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, sex, religion, national origin, age, marital status, disability or handicap
- 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 personal information about themselves or others protected by confidentiality laws
- using another individual's Internet or electronic communications account
- that impersonates another or transmits through an anonymous remailer
- that would incur any unauthorized expense to the district

Security

Security on District computer systems is a high priority. 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
- gain or attempt to gain unauthorized access to district computers or computers systems
- subvert or attempt to subvert any security controls in place on any district or other computer or computer system
- read, alter, delete or copy, or attempt to do so, electronic communications of other system users
- connect any unauthorized device or component physically or wirelessly to any district computer, computer system or network
- carelessly handle any district computer such that it becomes subject to physical damage, loss, or theft

Any staff member identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications and may be subject to disciplinary and/or legal action.

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 policies GBJ (Personnel Records and Files), JRA/JRC (Student Records/Release of Information on Students) and EGAEA (Public Electronic Mail Records).

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by the Family Educational Rights and Privacy Act (FERPA). Therefore, the sharing of student records or other confidential information with persons or agencies outside the District via e-mail or other electronic communications is prohibited without prior written consent of the student's parent/guardian, unless disclosure is under an exception to FERPA (See 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 e-mail or other electronic communications, 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 use e-mail or other electronic communications to disclose student records or other confidential student information in a manner inconsistent with FERPA requirements may be subject to disciplinary action.

Vandalism

Vandalism will result in cancellation of privileges and may result in disciplinary 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 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 unauthorized encryption software.

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 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 will result in the loss of the privilege to use these tools 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 upon hire and when this policy or the Acceptable Use Agreement is revised before Internet or electronic communications accounts shall be issues or access shall be allowed.

School District makes no warranties

The 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 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: March 4, 1999.
Recoded: August 28, 2001 *(previously File: EHD)*.
Revised: January 10, 2002.
Revised: May 8, 2008
Revised: August 11, 2011.:

LEGAL REFS.:
47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
47 U.S.C. 231 *(Child Online Protection Act of 1998)*
20 U.S.C. 6801 *et seq. (Elementary and Secondary Education Act)*
C.R.S. 24-72-204.5 *(monitoring electronic communications)*

CROSS REFS: GBJ (Personnel Records and Files)
JRA/JRC (Student Records/Release of Information on Students)
EGAEA (Public Electronic Mail Records)