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 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, child pornography or otherwise harmful to minors, as defined by the Board, software that blocks or filters such material and information has been installed on all district networks having Internet or electronic communications access. Blocking or filtering software may be disabled by a school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by staff members over the age of 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 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 computers and computer systems in a responsible, efficient, ethical and legal manner. Employees are expected to protect personal login and password information, and should never share access with anyone, including a co-worker, student, parents/guardian or volunteer. Employees are responsible for

exercising good judgment when utilizing district resources and should be wary of unknown email solicitations, pop-up boxes or writing anything in an email message that is inappropriate to say to others face-to-face. Any staff member identified as a security risk or having a history of problems with other computer systems may be denied access to the CCSD computer network.

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
- 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, age, marital status or disability
- for personal profit, financial gain, advertising, commercial transaction or political purposes that interrupts the educational process or as defined in board policy GBEB
- 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, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account, including email address of staff and students, 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
- Adversely affects the reputation or image of this organization.
- Shares student or district staff home addresses, phone numbers, email addresses, or other private information except as allowed in policy JRAJRC.

The following activities are also prohibited:

- Unauthorized attempts to log in to any network as a system administrator.
- Any malicious attempt to harm or destroy CCSD data, data of another user, or other CCSD computing facilities.
- Downloading, installing, storing or using malicious software, viruses, "cracking," and keystroke monitoring software.
- Attempting to evade, disable, or "crack" password or other security provisions of the systems on the network.
- Interfering with or disrupting another information technology user's work as well as the proper function of information processing and network services or equipment.
- Intercepting or altering network packets.
- Sharing or loaning accounts: All computer/security accounts are for the use of the single individual, the person for whom the account was approved. Sharing or loaning accounts is prohibited.
- The individual assigned a computer/security account is accountable for any and all transactions entered under that computer/security account login.
- Leaving an active system unattended, thereby allowing an unauthorized person to gain access to district resources through the user's login session.
- Attempting to gain unauthorized access to any other computer/security accounts is expressly prohibited.
- Using a computer for unlawful purposes, such as the illegal copying or installation of software, or violation of copyright laws.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Staff members should consult with their supervisor prior to exporting any material in question.
- Taking home technology equipment (hardware or software) without permission of a school administrator.
- Using information services for personal use or gain, including all web services, file transfer services or Telnet/SSH services.
- Using district electronic communication resources to participate in activities including, but not limited to, news groups, wikis, blog discussions, and social networking except for bona fide educational purposes.

Passwords

It should not be assumed that communications and information accessible via the network is private. Accounts must be protected as follows:

- All accounts, including accounts within major applications, must have a password.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords should be changed at least every 90 days.
- Passwords or use of the account must not be given to anyone

Security

Security and integrity on district computer systems is a high priority and requires participation of all staff members. 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.

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).

Personally Identifiable Information

Questions about the classification of protected information should be directed to your supervisor. Electronic mail (e-mail) should not be used for confidential matters or privileged communications such as student records.

Use of social media

Staff members may use social media within school 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 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 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-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

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. It is the responsibility of the staff member to insure that all software on their district computer is legal and appropriate for educational purposes.

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 school 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 should realize that while limited personal use of district resources is permitted by board policy GBEB, district administration maintains the responsibility and authority to determine when use of the internet or electronic communications with district resources is inappropriate.

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 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. The district will make every reasonable effort to ensure effective implementation and use of content filtering. However, staff members must realize that no content filtering system is 100% effective. Staff members must use professional judgment and appropriate caution when accessing internet and electronic communications services with district resources.

Adopted: September 10, 2013

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)*

Staff Use of Network and Internet

(Acceptable Use Agreement)

In order to provide for the appropriate use of the Internet in keeping with Board of Education policy, the following "Acceptable Use Agreement" has been developed. (A copy of this agreement will be distributed for signature before a staff member is issued an Internet account.)

Terms and conditions

All computers having district network and Internet access must be used in a responsible, efficient, ethical and legal manner. Failure to adhere to this Agreement, and the conditions set forth in Policy GBEE will result in revocation of access privileges.

I have been provided a copy of, and have read and understand and will abide by Policy GBEE. I further understand that a violation of the regulations of this policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action and/or appropriate legal action may be taken up to, and including, termination of employment.

Your signature on the Acceptable Use Agreement is legally binding and indicates that you have read the terms and conditions carefully and understand their significance.

Employee's signature _____ Date _____