

SECTION 400 – STUDENTS

STUDENT USE OF COMPUTERS, INTERNET AND ELECTRONIC COMMUNICATIONS POLICY 412

ARTICLE 1 DISTRICT AND STAFF RESPONSIBILITIES

- A. Student use of computers, the Internet and electronic communications accessed through District computers and equipment is deemed to be important for student learning. (See Policy 520, Article 5.) However, such use demands personal responsibility and an understanding of the acceptable and unacceptable uses of these tools. Student use of District computers, the Internet and electronic communications is a privilege, not a right. Failure to adhere to requirements listed in this policy (Policy 412) shall result in the loss of the privilege to use these tools, restitution for costs associated with damages, and may result in disciplinary action including suspension or expulsion and/or legal action. The District may deny, revoke or suspend access to District technology or close accounts at any time. The duration of the denial, revocation or suspended access shall be determined by the administrator who has determined the need for such action.
- B. Parents/guardians shall be required to sign the District's Acceptable Use Agreement annually before their son/daughter is authorized to use District computers or the Internet and before electronic communications accounts are issued or access is allowed.
- C. District computers and computer systems are owned by the District and are intended for educational purposes at all times. Students 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 use 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 District.
- D. The Internet and electronic communications are fluid environments in which students may access materials and information from many sources, including some that may be harmful to students. While it is impossible to predict with certainty what information students might locate or come into contact with, the District shall take reasonable steps to protect students from accessing material and information that is obscene, contains pornography, is inconsistent with the mission and philosophy of the District or may otherwise be harmful to minors as defined by the Board of Education:
1. In compliance with state and federal Children's Internet Protection Acts, the District has installed software on its computer network that, to the extent feasible, blocks or filters materials and/or information from websites that are obscene, contain pornography, are inconsistent with the mission and philosophy of the District or may otherwise be harmful to minors, as defined by the Board.
 2. It is not reasonable or feasible to block access to widely used video sharing and internet hosting sites that offer educational resources and access to extensive information that can broaden the range and depth of student learning. Therefore, all student uses of these tools at school shall be supervised and monitored by the administrator, teacher or staff member responsible for the learning activity or assignment or specifically assigned to oversee/monitor such activities or assignments. The staff-student ratio for such supervision shall not exceed established ratios for class size.

References:

C.R.S. 22-32-109.1 (2) (a) Conduct and Discipline Code
C.R.S. 22-87-101 et seq. Children's Internet Protection Act
20 U.S.C. 6801 et seq. elementary and Secondary Education Act
47 U.S.C. 231 Children's Online Privacy Protection Act of 1998
47 U.S.C. 254(h) Children's Internet Protection Act of 2000
Adopted: 12/08/08

SECTION 400 – STUDENTS

STUDENT USE OF COMPUTERS, INTERNET AND ELECTRONIC COMMUNICATIONS POLICY 412

3. Students shall have specific objectives and search strategies prior to accessing material and information on the Internet and through electronic communications.
- 4.

ARTICLE 2 STUDENT RESPONSIBILITIES

- A. Students shall use District computers and computer systems in a responsible, efficient, ethical and legal manner.
- B. Students shall take responsibility for their own use of District computers and computer systems to avoid contact with material or information that is obscene, contains pornography, is inconsistent with the mission and philosophy of the District or that may be harmful to minors as defined by the Board of Education.
- C. Students shall report access to materials and information that are obscene, contain pornography, are inconsistent with the mission and philosophy of the District or may otherwise be harmful to minors, as defined by the Board, to the supervising teacher or staff member. If a student becomes aware of other students accessing such material or information, he or she shall report it to the supervising staff member.
- D. Students who identify a security problem while using the Internet or electronic communications must immediately notify a staff member who is monitoring computer use, their teacher or school administrator. Students should not demonstrate the problem to other student users. Logging on to the Internet or electronic communications as a system administrator, District employee or another student is prohibited. Students shall not:
 1. use another person's password or any other identifier;
 2. gain or attempt to gain unauthorized access to District computers or systems; or
 3. read, alter, delete or copy, or attempt to do so, electronic communications of other system users.
- E. Students shall not reveal personal information, such as home address or phone number, while using the Internet or electronic communications. Without first obtaining permission of the supervising staff member, students shall not use their last name or any other information that might allow another person to locate him or her. Students shall not arrange face-to-face meetings with a person met on the Internet or through electronic communications.
- F. No student shall access, create, transmit, retransmit or forward material or information on a District computer or through a District computer system or other electronic device owned by the District that is not related to District education objectives and that:
 1. 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;
 2. 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;
 3. harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons in violation of the District's non-discrimination policies.

References:

C.R.S. 22-32-109.1 (2) (a) Conduct and Discipline Code
C.R.S. 22-87-101 et seq. Children's Internet Protection Act
20 U.S.C. 6801 et seq. elementary and Secondary Education Act
47 U.S.C. 231 Children's Online Privacy Protection Act of 1998
47 U.S.C. 254(h) Children's Internet Protection Act of 2000
Adopted: 12/08/08

SECTION 400 – STUDENTS

STUDENT USE OF COMPUTERS, INTERNET AND ELECTRONIC COMMUNICATIONS POLICY 412

4. plagiarizes the work of another or copies the work of another without expressed consent of the author;
5. uses inappropriate or profane language likely to be offensive to others in the school community;
6. is knowingly false or could be construed as intending to purposely damage another person's reputation;
7. violates any federal or state law or District policy including but not limited to copyrighted material and material protected by trade secret;
8. contains personal information about themselves or others including information protected by confidentiality laws;
9. uses another individual's Internet or electronic communications account without written permission from that individual;
10. impersonates another or transmits through an anonymous remailer;
11. accesses fee services without specific permission from a school administrator; or
12. is for personal profit, financial gain or advertising, or is a commercial transaction or a political purpose.

ARTICLE 3 VANDALISM OF COMPUTERS, SOFTWARE, ACCESSORIES OR SYSTEMS

- A. Vandalism will result in cancellation of privileges and may result in school disciplinary action including suspension or expulsion, 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 encryption software.

ARTICLE 4 SOFTWARE

- A. All software loaded on any District computer shall be "legal" and licensed. No software shall be loaded onto a District computer or server without the approval of the Principal after consultation with District technology representatives.
- B. Students 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.

ARTICLE 5 PERSONAL COMPUTERS

- A. Students may bring personal computers to school but they shall not connect them to the District's computer system or network without permission of the Principal.

ARTICLE 6 NO WARRANTIES

- A. The District makes no warranties of any kind, whether express or implied, related to the use of District computers, computer systems, Internet access and electronic communication

References:

C.R.S. 22-32-109.1 (2) (a) Conduct and Discipline Code
C.R.S. 22-87-101 et seq. Children's Internet Protection Act
20 U.S.C. 6801 et seq. elementary and Secondary Education Act
47 U.S.C. 231 Children's Online Privacy Protection Act of 1998
47 U.S.C. 254(h) Children's Internet Protection Act of 2000
Adopted: 12/08/08

SECTION 400 – STUDENTS

STUDENT USE OF COMPUTERS, INTERNET AND ELECTRONIC COMMUNICATIONS POLICY 412

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 student 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 student's own risk.

References:

C.R.S. 22-32-109.1 (2) (a) Conduct and Discipline Code
C.R.S. 22-87-101 et seq. Children's Internet Protection Act
20 U.S.C. 6801 et seq. elementary and Secondary Education Act
47 U.S.C. 231 Children's Online Privacy Protection Act of 1998
47 U.S.C. 254(h) Children's Internet Protection Act of 2000
Adopted: 12/08/08