

Platte Canyon School District

Agreement for Student Use of District Computers, the Internet and Electronic Communications

Student use of computers, the Internet and electronic communications accessed through District computers and equipment is important for student learning. However, such use demands personal responsibility and an understanding of the acceptable and unacceptable use of these tools. **Policy 412, Student Use of Computers, Internet and Electronic Communications** describes District requirements to comply with the Child Internet Protection Act and provides a detailed list of student responsibilities associated with the privilege of using District computers, computer systems, the Internet and electronic communications. You are encouraged to read Policy 412 prior to signing this Agreement. The policy is available on the District’s website, www.plattecanyonsd1.org. You may request a copy of the Policy from your child’s school or obtain one from the Platte Canyon School District Office at 57393 U.S. Highway 285, Bailey, Colorado 80421.

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.

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 be otherwise harmful to minors as defined by the Board of Education.

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.

Middle and high school students and a parent/guardian must read and sign this agreement prior to being given permission to use District computers and/or the Internet and electronic communications through District systems.

Parents of elementary students are asked to review responsibilities with their child as appropriate for his/her age level and to grant permission by signing below. Internet use by elementary children at school is limited. Students are not allowed to freely search the Internet. Any use of bookmarked sites is closely monitored.

Student:

As a student, I agree to fulfill my responsibilities for use of Platte Canyon School District computers, the Internet and electronic communications as listed in Policy 412 and as shown on the reverse side of this agreement.

Student _____ Date _____ Entering Grade _____

Parent:

I have discussed the contents of this agreement with my middle or high school student and feel that he/she understands his/her responsibilities as listed in Policy 412 and shown on the reverse side of this agreement or I have reviewed responsibilities with my elementary child as appropriate for his/her age. I understand that 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 be otherwise harmful to minors as defined by the Board of Education.

I grant permission for (print full name of student) _____ to use District computers, the Internet and electronic communications within the conditions of this agreement.

Parent _____ Date _____

POLICY 412

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 are otherwise 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.
 - 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. 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.