

Student Use of Technology the Internet and Electronic Communications

I. General Considerations

Technology, which includes the Internet, electronic communications, social media, applications and artificial intelligence (“AI”) tools has vast potential to support curriculum and learning. The Board of Education (“Board”) believes appropriate technology should be used in schools as a learning resource to educate and to inform.~~The Internet and electronic communications (including but not limited to e-mail, chat rooms, file sharing and other forms of electronic communication) have vast potential to support curriculum and student learning. The Board of Education believes these resources should be used in schools as a learning resource to educate and to inform.~~

Use of technology the Internet and electronic communications requires students to think critically, analyze information, write clearly, use problem-solving skills, and hone computer and research skills that employers demand. Use of these tools also encourages an attitude of lifelong learning and offers an opportunity for students to participate in distance learning activities, ask questions of and consult with experts, communicate with other students and individuals, and locate material to meet educational and personal information needs.

~~The Internet and electronic communications are~~ Technology is a 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, pornographic or otherwise harmful to minors, as defined by the Board. Students shall take responsibility for their own use of District technology devices to avoid contact with material or information that may be harmful to minors, including any such materials compiled by third parties on non-District Internet sites.

II. Blocking or fFiltering oObscene, pPornographic and hHarmful iInformation

Technology that blocks or filters material and information that is obscene, child pornography or otherwise harmful to minors, as defined by the Board, shall be implemented or installed on each technology device provided by the District that allows for access to the Internet by a minor, from any location. Students shall report access to material and information that is obscene, pornographic, harmful to minors or otherwise in violation of this policy to a the supervising staff member. If a student becomes aware of other students accessing such material or information, the student he or she shall report it to a the supervising staff member.

III. No eExpectation of pPrivacy

District technology devices are owned by the District and are intended for educational purposes at all times. Students shall have no expectation of privacy when using District technology. 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 ~~D~~district technology devices, including all ~~technology Internet and electronic communications~~ access and transmission/receipt of materials and information. All material and information accessed/received through ~~d~~District technology devices shall remain the property of the ~~school-D~~district.

IV. Unauthorized and ~~u~~Unacceptable ~~u~~Uses

Students shall use ~~D~~district technology in a responsible, efficient, ethical, and legal manner.

Because technology and ways of using technology are constantly evolving, every unacceptable use of ~~d~~District technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses are identified in the list below. ~~include, but are not limited to, the following:~~

No student shall access, create, transmit, retransmit or forward material or information or software:

- That is not related to ~~D~~district education objectives;
- 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 in violation of the ~~d~~District's nondiscrimination policies;
- 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;
- That is in violation of any federal or state law, or ~~D~~district policy, including but not limited to District policies ~~y~~ related to ~~on~~ AI, copyrighted material, and material protected by trade secret;
- That impersonates another or transmits through an anonymous remailer;
- That accesses fee services without specific permission from the system administrator;
- That accesses another individual's Internet or electronic communications account without written permission from that individual;
- That runs port scans, network scans, network monitoring, keyloggers, password-cracking programs, hacking software or unauthorized file-sharing. Hacking is defined as "to gain access to a computer, computer file or network illegally or without authorization; or to view, alter, steal, damage or destroy computer data without authorization"; or

- That uses or attempts to use virtual private networks (VPNs), proxy services, alternate DNS services, anonymizers, or any other technology to bypass, evade, or interfere with District content filters, monitoring systems, or network security controls;
- That is generated by an AI tool that has not been explicitly approved by the classroom teacher or the District for the specific assignment or activity, or that uses an AI tool in a manner inconsistent with the scope of such approval; or
- That incorporates AI-generated content submitted as the student's own original academic work without explicit instructor authorization and without disclosing the use and extent of AI assistance as required by the District.

V. Use of Internet Resources and Tools

The use of Generative AI tools, defined as a subset of AI that creates new content, such as essays, art, or multimedia, which may resemble human-created work is permitted only if it aligns with instructional goals, is approved by the classroom teacher, and complies with all District data privacy policies. Students using Generative AI tools to create, submit, or claim original academic work must be explicitly authorized by an instructor. All AI-generated content incorporated into student work must be properly attributed, and the level of AI assistance must be disclosed (e.g., in a footnote, header, or method statement as directed by the instructor).

Only AI tools that have been reviewed and approved by the District for compliance with applicable student data privacy requirements, including but not limited to the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA), shall be used for instructional purposes. Students should not upload or input any personal, confidential, ~~propriety~~-proprietary or sensitive information into any AI tool. Examples include passwords and other personal information such as names, likenesses, or social security, credit card or bank account numbers.

Students are prohibited from using generative AI to create, distribute, or submit any content that realistically depicts, impersonates, or simulates the likeness, voice, or image of another student, staff member, or any other individual without that individual's explicit consent. Violation of this provision is subject to disciplinary action as set forth in Section XIII of this policy and applicable Board policy.

VI. Security

Security on ~~D~~istrict technology devices is a high priority. Students who identify a security problem while using District technology ~~the Internet or electronic communications~~ shall ~~must~~ immediately notify a staff member. ~~system administrator.~~ Students should not demonstrate the problem to other users. Students ~~Logging on to~~ technology ~~the Internet or electronic communications~~ as a staff member is prohibited.

Students shall not:

- Use another person's password or any other identifier;
- Gain or attempt to gain unauthorized access to District technology or computer devices;
- or
- Read, alter, delete or copy or attempt to do so, electronic communications of other system users

Any user of District technology devices identified as a security risk, or as having a history of problems with technology devices may be denied access to District technology; ~~the Internet and electronic communications.~~

VII. Use of Personal Computers

Students may be allowed to connect their own personal computers and/or electronic communication devices to the CCSD Network at any time or through any means, including wireless or telecommunications, for legitimate educational or other purposes deemed appropriate by the District.

Students shall have no expectation of privacy once they have been authorized to connect to the District's electronic network.

The ~~school-district~~ District is not responsible for any loss or damage to the student's computer while it is connected to the CCSD Net, including but not limited to losses or damage caused by hardware failure, data loss, or the incurring of a virus.

VIII. Use of Electronic Communications for a Public Audience

The use of District computers is limited to educational and school business. Personal blogs, wikis, podcasts or other electronic communications or online discussions that do not pertain to school or District educational assignments or educational programming should not be accessed from District computers or through the District's electronic networked resources.

Electronic communications for a public audience and forms of online discussion including, but not limited to, blogs, wikis, bulletin boards, podcasts, ~~chatrooms~~ online discussion boards, ~~listservs~~ messaging platforms, collaborative tools, or other forms of electronic ~~mailing lists~~ communication being used for District educational programming are considered an extension of the classroom or educational programming and are subject to all applicable school board policies and regulations.

Students must have written parent/guardian permission to access the Internet through District electronic networked resources ~~in order~~ to participate in any educational or classroom related blog, wiki, podcast, or other electronic communication or online discussion that are accessible through the District's electronic networked resources.

IX. Safety

Students shall not reveal personal information, such as home address~~es~~ or ~~telephone numbers~~, while using the Internet or electronic communications. Without first obtaining permission of ~~the supervising a~~ staff member, students shall not use their last name or any other information that might allow another person to locate ~~the student. him or her.~~ Students shall not arrange face-to-face meetings with persons met on the Internet or through electronic communications.

X. 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 d~~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 ~~D~~district-owned software or hardware. ~~This Vandalism~~ includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

XI. Unauthorized sSoftware

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.

XII. Assigning sStudent pProjects and mMonitoring Sstudent Uuse

The ~~D~~district will take all reasonable efforts to see that the Internet and electronic communications are used responsibly by students. Administrators, teachers and staff have a professional responsibility to work together to monitor students' use of the Internet and electronic communications, help students develop the intellectual skills needed to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet their educational goals. Students shall have specifically defined objectives and search strategies prior to accessing material and information on the Internet and through electronic communications. Administrators, teachers, and staff also have a professional responsibility to support students in developing critical AI literacy skills, including the ability to evaluate the accuracy, limitations, and potential bias of AI-generated content, and to use AI tools responsibly and in accordance with District policy and instructional expectations.

XIII. Student uUse as a pPrivilege

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Student 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 school disciplinary action and/or legal action. The ~~school d~~District may deny, revoke or suspend

access to ~~d~~District technology or close accounts at any time for misuse of this privilege in violation of this policy and/or impose disciplinary consequences consistent with Board policy.

Students and parents/guardians shall be required to sign the ~~D~~istrict's Acceptable Use Agreement annually before Internet or electronic communications accounts shall be issued or access shall be allowed.

~~XIV. School-D~~istrict ~~m~~Makes ~~N~~o ~~W~~arranties

The ~~school-district~~District makes no warranties of any kind, whether expressed or implied, related to the use of ~~D~~istrict technology devices, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the ~~d~~District of the content, nor does the ~~D~~istrict make any guarantee as to the accuracy or quantity of information received. The ~~school-district~~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.

Originally Adopted: January 9, 2012

Revised: ~~December 12, 2012~~

Adopted: ~~January 9, 2012~~

Current Revision: October 5, 2026

LEGAL REFS.: 47 ~~§~~ U.S.C. 254(h) (Children's Internet Protection Act of 2000)
 47 C.F.R. Part 54, Subpart F (Universal Support for Schools and
 Libraries)
 20 U.S.C. ~~§~~ 6751 et seq. (Enhancing Education Through Technology Act of
 2001)
 C.R.S. ~~§~~ 22-87-101 et. seq. (Children's Internet Protection Act)

CROSS REFS.: AC - Nondiscrimination/Equal Opportunity
 EGA - Electronic Mail
 EGAD - Copyright/Royalties
 EHC - Networked Electronic Resources
 EHCA - Web and Internet Publishing
 JB - Equal Educational Opportunities
 JICDA - Conduct and Discipline Code
 JICJ - Student Use of Electronic Communication Devices