



SECTION J: Students
JS-O Technology Resources, Internet Safety
Responsible Use Policy for Students
Effective: 8/1/2015
Reviewed: 7/1/2018
Effective: 8/1/2018

JS-O Technology Resources, Internet Safety Responsible Use Policy for Students

Limitations and Guidelines

1. Student 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.

Student 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 disciplinary action, including suspension or expulsion, and/or legal action. CEC may deny, revoke, or suspend access to CEC technology at any time.

Use of the Internet and electronic communications empower students to analyze information from a global perspective, work collaboratively, and use problem solving skills necessary for success in a modern society. CEC believes these tools are an essential foundation to creating students who are lifelong learners. Students and parents/guardians shall be required to sign the CEC's Acceptable Use Agreement as a part of the enrolment process.

2. Illegal Copying

Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. Users may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of CEC. See CEC Policy JRC-G Privacy and Protection of Confidential Student Information.

3. Accessing the Internet

Bypassing the CEC computer network security by accessing the Internet directly is strictly prohibited unless the computer the user is using is not connected to CEC network.

4. Monitoring of computer and Internet usage.

CEC has the right to monitor and log any and all aspects of its computer system including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users.

5. Blocking websites.

In compliance with the Federal Children's Internet Protection Act (CIPA), CEC has the right to, and does, block or filter Internet access to pictures that are: (a) obscene, (b) child pornography, (c) harmful to minors or (d) other material deemed inappropriate in the workplace and institution. Attempting to, or successfully bypassing the filter, whether directly or through a proxy, without prior approval is forbidden.

6. Vandalism

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 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 technology device. This includes, but is not limited to, the uploading or creation of computer viruses and the use of encryption software.

7. No Expectation of Privacy

Student's shall have no expectation of privacy in anything they create, store, send or receive while using a CEC Information Technology and Internet access. Student's expressly waive any right of privacy in anything they create, store, send or receive while using CEC's Information Technology and Internet access. CEC reserves the right at any time and without notice to monitor usage and to inspect, copy, review, segregate, store and/or remove any or all communications, documents, data, software and other information related to such use.

8. Use of Personal Electronic Devices.

Students may carry electronic communication devices approved by the building principal, but these devices must be turned off and put away during instructional time, unless they are being used for instructional purposes and with approval of the teacher. Regarding non-instructional time, school staff members have the authority to restrict students' use of such devices in school buildings, on school buses, at school-sponsored activities and on field trips, if in the judgment of the staff member, the use of the device interferes with the educational environment. Use of electronic communication devices with cameras is prohibited in locker rooms, bathrooms, or other locations where such operation may violate the privacy rights of another person. Use of cameras to record all or part of any classroom instruction is permissible only with the approval of the teacher.

It is the student's responsibility to ensure that the device is turned off and out of sight during unauthorized times.

9. Social Media Guidelines

Social media is any form of online publication or presence that allows interactive communication, including social networks, blogs, photo sharing platforms, Internet websites, Internet forums, and wikis. Examples of social media include, but are not limited to, Facebook,

Twitter, Edmodo, Schoology, Instagram, YouTube, Google+, and Flickr.

If you are being cyberbullied or hear about/observe someone else being cyberbullied, report the behavior and get help. You can tell a parent, school staff, another adult family member, a trusted adult, or use Safe2Tell.

While at times, it is easy to tell whether a social media use is school-related or personal, at other times, it may be difficult to distinguish fully between different uses. Sometimes, personal social media use, including off-hours use, may result in disruption at school and the school may need to get involved. This could include disciplinary action such as a parent conference or suspension. It is important to remember that infractions outlined in the Discipline Code prohibiting certain types of communication also apply to electronic communication. To be safe, be in control of what you do online, even if it is during personal time.

For school-related social media, do not tag student posts, photos, or videos unless your teacher gives you permission, as this may expose the content to audiences for whom it was not intended.

Once a comment is posted online, you cannot later say, "never mind." It may seem funny or harmless when you post it, but it could hurt or offend someone. As guidance, take a few extra minutes to think about whether a post will be hurtful or embarrassing or whether it could negatively affect a future opportunity

10. Prohibited Activities

Because technology and ways of using technology are constantly evolving, every unacceptable use of CEC technology devices cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following.

No student 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 text.
- that harasses, threatens, demeans, or promotes violence or hatred against another person or group of persons with regard to race, color, national origin, ancestry, creed, religion, sex (which includes marital status), sexual orientation (which includes transgender), disability or need for special education services
- 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, including information protected by confidentiality laws
- using another individual's Internet or electronic communications account
- that impersonates another or transmits through an anonymous remailer
- that accesses fee services without specific permission from the system administrator

Legal Ref:

15 U.S.C. 6501 et seq. (Children's Online Privacy Protection Act)

20 U.S.C. 1232g (Family Educational Rights and Privacy Act)

20 U.S.C. 1232h (Protection of Pupil Rights Amendment)

34 C.F.R. 99.1 et seq. (FERPA regulations)

34 C.F.R. 300.610 et seq. (IDEIA regulations concerning confidentiality of student education records)

C.R.S. 19-1-303 and 304 (records and information sharing under Colorado Children's Code)

C.R.S. 22-1-123 (district shall comply with FERPA and federal law on protection of pupil rights)

C.R.S. 24-72-204 (3)(a)(VI) (schools cannot disclose student address and phone number without consent)

C.R.S. 24-72-204.5

Policy References:

Student Handbook

ADD-G Safe Schools

JRC-G Privacy and Protection of Confidential Student Information