SECTION: Personnel
Technology Resources, Internet Safety and Responsible Use for Staff
Approved: 7/2021

Technology Resources, Internet Safety Responsible Use Policy for Staff

Permitted Use and Overview

The computer network is the property of Colorado Early Colleges (CEC) and is to be used for legitimate business and education purposes. All users must use CEC's computer resources and the Internet in a lawful and ethical manner. Abuse of the computer network or the Internet, or violation of this policy may result in disciplinary action. IT staff may give to law enforcement officials or CEC administration information that constitutes potential evidence of criminal action or violation of CEC policy. The user understands that said information may result in criminal proceedings or disciplinary actions taken against the user.

Limitations and Guidelines

Prohibited Activities

Occasional limited appropriate personal use of a computer is permitted if such use does not: a) interfere with the user's or another staff member's job performance; b) have an undue effect on the computer or CEC's network performance; c) or violate any other policies, provisions, guidelines, or standards of CEC. All users are responsible for the professional, ethical, and lawful use of the computer system and must remember that all activity conducted on CEC's network or on CEC devices may be public information subject to the Colorado Open Records Act.

The following are examples of unacceptable uses of CEC's technology resources. The list is not inclusive but can include the following. No CEC employee 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 deters from CEC's 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.
- that is part of a mass mailing or mass forwarding.

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 the Head of School and/or IT staff member.

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.

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.

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.

Frivolous Use

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, printing materials for personal use, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet. Sending unsolicited bulk and/or commercial messages over the Internet to other CEC staff or using the service for activities that invade another's privacy is strictly prohibited. IT reserves the right to restrict access as needed to specific users who violate these guidelines and to monitor all usage on its network.

Viruses

Files obtained from sources outside CEC, including media from home, files downloaded from the Internet, e-mail attachments or other online services may contain dangerous computer viruses that may damage the computer network. If a user suspects that a virus has been introduced into the network, notify IT staff immediately.

Any files copied, created, or downloaded to a school computer that is not a server is not backed up. It is the responsibility of the owner of the file to insure it is backed up. Attempts may be made to recover data stored on a user's OneDrive, but there is no guarantee data will not be lost.

No Expectation of Privacy

Employees shall have no expectation of privacy and waive any rights to privacy in anything they create, store, send or receive while using CEC's network 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. Users expressly waive any right of privacy in anything they create, store, send or receive using the CEC's computer equipment or network. Users consent to allow school personnel access to and review of all materials created, stored, sent or received by users using CEC's computer equipment or through any CEC network or Internet connection.

Email

Email is to be used for business purposes and personal email should be kept to a minimum. CEC prohibits the display, transmittal, or downloading of material that is offensive, pornographic, obscene, profane, discriminatory, harassing, insulting, derogatory, or otherwise unlawful.

No one may solicit, promote, or advertise any outside organization, product, or service using their CEC email account at any time. Signature lines are limited to name, title within CEC network, school name, and school contact information. IT monitors e-mail for abuse. Employees' email correspondence may be considered public records under the public records law and may be subject to public inspection (*C.R.S. 24-72-204.5*).

Employees are prohibited from unauthorized use of encryption keys or the use of passwords of other employees to gain access to another employee's email messages.

Account Sharing Prohibited

Internet or network access is only to be used when logged in under the user's own login name. There is never a reason to be logged in under someone else's username (*IT staff are exempt*). The user who is logged in will be responsible for sites visited while logged in. This pertains to inappropriate sites with sexual content as well as politically questionable sites which might come to the attention of government officials under the Patriot Act.

Tampering, Hacking and Destruction.

Under no circumstances should users attempt to hack into or violate CEC's network, accounts, servers, or files. Tampering with and/or destruction of physical hardware, including, but not limited to, mice, keyboards, servers, or files will not be tolerated and is considered vandalism. Knowingly spreading computer viruses or any attempt to compromise the network integrity is also prohibited.

Hacking computer systems or deliberate destruction of computer hardware could result in immediate termination and/or legal prosecution of the employee.

Use of Third-party or On Demand Service Providers

CEC Network staff members shall ensure that student education records are disclosed to persons and organizations outside the network only as authorized by applicable law and CEC policy. The term "organizations outside the network" includes school service on-demand providers and school service contract

providers. Acquisition and use of any third-party apps and services that use student data in any capacity must be pre-approved be CEC. Staff must follow the procedure to secure approval before using the contract provider or on-demand provider. CEC will identify specific programs or apps that are approved for school and teacher use, and make that list available in the CEC website.

Use of Personal Electronic Devices.

The use of personal devices is generally permitted as long as the use does not violate CEC policy. CEC reserves the right to remove any harmful software, utilities or other data from a personal electronic device that is being used to connect to the CEC network. CEC reserves the right to ban particular personal electronic devices from school property. Use of personal mobile devices during work time must be kept to a minimum.

All electronic devices on CEC property are subject to temporary confiscation, search, and inspection. The length of confiscation will be based on the particular circumstances but shall not be for more than one week without good cause.

CEC is not liable for any interception or transmissions, computer worms or viruses, loss of data, file corruption, hacking or damage to your personal computer or other personal devices that result from the transmission or download of information or materials through CEC's internet service.

Use of the wireless network is subject to the general restrictions outlined in "Prohibited Activities". If abnormal, illegal, or unauthorized behavior is detected, including heavy consumption of bandwidth, the network provider reserves the right to permanently disconnect the offending device from the wireless network.

Social Media

Definitions of Social Media:

- Social network - a dedicated website or other application that enables users to communicate with each other by posting information, comments, messages, images, etc. This includes Facebook, Instagram, LinkedIn, Pinterest, Snapchat, and Twitter.
- Microblog – an online space where authors create communities to share information, ideas, personal messages, and other content.
- Listserv, newsgroup – An email exchange where messages are broadcast to every member of a group at once.
- Forum – a web-based place where users post their comments or opinions on topics. Users may comment on or respond to previous posts. Readers can read and/or respond to all prior posts.
- Chatroom – An internet space where groups of people meet for live conversations via typed messages.

CEC is aware that employees may use social media during non-work time. All postings on a blog, microblog, forum, chatroom, listserv or newsgroup, wiki, or social networking site on behalf of CEC must be preapproved and sent by authorized employees only. All other postings made by an employee on a blog, wiki, or social networking site are personal communications and an employee may not present as a CEC representative. Employees are personally responsible for the content they publish. Postings by an employee concerning CEC are not prohibited provided they comply with guidelines set forth below.

- If you post any comment that promotes or endorses CEC products or services in any way, the law requires that you disclose that you are employed by CEC.
- You must comply with all applicable laws, including copyright and fair use laws. You may not disclose any sensitive, proprietary, confidential, or financial information about CEC. You may not post anything related to CEC inventions, strategy, financials, or products that have not been made public. Confidential information includes trade secrets or anything related to the CEC's inventions, strategy, financials, or products that have not been made public, internal reports, procedures or other internal business-related confidential communications.

- A blog, forum, chatroom, listserv or newsgroup, wiki, or social networking site are not the ideal place to make a complaint to CEC regarding alleged discrimination, unlawful harassment, or safety issues. Complaints regarding these issues should be directed to the Executive Director of Organizational Development and HR in alignment with CEC policy.
- Use good judgment when you use social media. Be respectful of CEC, our employees, our students and families, our partners and affiliates, and others. Avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene or threatening, that defames or libels our employees, students or families, partners and affiliates, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment.

Additional Legal References:
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)
20 U.S.C. 1415 (IDEIA procedural safeguards, including parent right to access student records) 20 U.S.C. 8025 (access to student information by military recruiters)
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. 22-16-101 et seq. (Student Data Transparency and Security Act)
C.R.S. 22-16-107 (2)(a) (policy required regarding public hearing to discuss a material breach of contract by school service contract provider)
C.R.S. 22-16-107 (4) (policy required regarding student information privacy and protection)
C.R.S. 22-16-112 (2)(a) (policy required concerning parent complaints and opportunity for hearing)
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:
Employee Handbook
Safe Schools
Rights Concerning Student Records