EHC-O Technology Resources, Internet Safety Responsible Use Policy for Staff

Limitations and Guidelines

1. 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.

2. 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.

3. 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.

4. 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.

5. 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 harassing, intimidating and/or threatening messages is also prohibited. I.T. reserves the right to restrict access as needed to specific users who violate these guidelines to ensure optimal network bandwidth.

6. 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. Users should never download files from the Internet or accept e-mail attachments from sources outside of CEC, or use media from non-CEC sources, without first scanning the material with a CEC-approved virus checking software. If a user suspects that a virus has been introduced into the network, notify I.T. personnel 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. Colorado Early Colleges will not be responsible for loss of these files for any reason or event.

7. No Expectation of Privacy

Employee's shall have no expectation of privacy in anything they create, store, send or receive while using ~~a~~ CEC Information Technology and Internet access. Employee'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. Email

E-mail is to be used for business purposes. While personal e-mail is permitted, it is to be kept to a minimum. Personal e-mail should be brief and sent or received as seldom as possible. CEC prohibits the display, transmittal, or downloading of material that is offensive, pornographic, obscene, profane, discriminatory, harassing, insulting, derogatory, or otherwise unlawful at any time.

No one may solicit, promote, or advertise any outside organization, product, or service using e-mail or anywhere else on CEC premises at any time I.T. personnel may monitor e-mail at the request of aa supervisor. That employees' correspondence on e-mail may be a public record 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 passwords of other employees to gain access to another employee's e-mail messages.

9. 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 user name (*I.T personnel 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.

10. Tampering, Hacking and Destruction.

Under no circumstances should users attempt to hack into or violate the 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. Any student caught hacking or destroying a computer must be reported to the school leadership.

11. 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. CEC will make copies of this policy upon request to the parent of an enrolled student; and will post the policy on its website.

12. Use of Personal Electronic Devices.

The use or 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 connect the CEC network. CEC reserves the right to ban particular personal electronic devices from school property.

When using CEC internet service there are significant security, privacy and confidentiality risks inherent in accessing or transmitting information through the internet, whether the connection is facilitated through wired or wireless technology. Security issues include, without limitation, interception of transmissions, loss of data, and the introduction or viruses and other programs that can corrupt or damage your computer.

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

13. Social Media

CEC permits employees' use of social media on working time using CEC equipment and systems and 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. All other postings made by an employee on a blog, wiki, or social networking site are considered personal communications and are not CEC communications. Use of personal mobile devices during work time should be kept to a minimum. 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 or in this handbook.

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

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 is not the ideal place to make a complaint to CEC regarding alleged discrimination, unlawful harassment, or safety issues. Complaints regarding these issues to CEC must be made consistent with the complaint procedures in this handbook so that CEC may address them.

When you use social media, use good judgment. We request that you 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.

Nothing in this guideline is meant to interfere with employees' right under federal law to engage in protected and concerted activity, including employees' ability to discuss terms and conditions of their employment.

14. Prohibited Activities

Occasional limited appropriate personal use of the computer is permitted if such use does not: a) interfere with the user's or any other's job performance; b) have an undue effect on the computer or company network's performance; c) or violate any other policies, provisions, guidelines or standards of CEC. At all times users are responsible for the professional, ethical and lawful use of the computer system.

The following are representative examples only and do not comprise a comprehensive list of illegal uses:

1) Spamming and invasion of privacy - Sending of unsolicited bulk and/or commercial messages over the Internet using the Service or using the Service for activities that invade another's privacy.
2) Intellectual property right violations - Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, service marks, trade secrets, or any other proprietary right of any third party.
3) Accessing illegally or without authorization computers, accounts, equipment or networks belonging to another party, or attempting to penetrate/circumvent security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to, port scans, stealth scans, or other information gathering activity.
4) The transfer of technology, software, or other materials in violation of applicable export laws and regulations.
5) Using the Service in violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available ponzi schemes, pyramid schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items, or services.
6) Distribution of pornographic materials to minors; and
7) Child pornography.

Examples of Unacceptable Uses

The following are representative examples only and do not comprise a comprehensive list of unacceptable uses:

1) Using the Service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.
2) Forging or misrepresenting message headers, whether in whole or in part, to mask the

originator of the message.

3) Advertising, transmitting, or otherwise making available any software product, product, or service that is designed to violate these Terms of Use, which includes the facilitation of the means to spam, initiation of pinging, flooding, mail-bombing, denial of service attacks, and piracy of software.
4) The sale, transfer, or rental of the Service to customers, clients or other third parties, either directly or as part of a service or product created for resale.
5) Seeking information on passwords or data belonging to another user.

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)
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
ADD-G Safe Schools
JRC-G Privacy and Protection of Confidential Student Information