

Regulations for Acceptable Use

Information for Students, Parents, and Guardians

The purpose of Central Rivers AEA Regulations for Acceptable Use is to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act ("CIPA"). As used in this policy, "user" includes anyone using the electronic devices, equipment, or "network," which includes but is not limited to the Internet, email, messaging/chat tools, Zoom phone, and other forms of direct electronic communications provided by the agency.

Central Rivers AEA will use technology protection measures to block or filter, to the extent practical, access of visual depictions that are obscene, pornographic, and harmful to minors over the network. The agency reserves the right to monitor users' online activities and to access, review, copy, and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy when using Agency-provided devices, systems, or network services, including email, cloud storage, and internet access.

Acceptable Uses of the Central Rivers AEA Network

Each year schools must verify that students using the network(s) and/or have signed the form acknowledging the Regulations for Acceptable Use. Students who are under 18 must have their parents or guardians sign this form and schools must keep it on file. Once signed that permission/acknowledgement form remains in effect until revoked by the parent or guardian, or the student loses the privilege of using the agency's network due to violation of this policy or is no longer a student.

By using the network, users have agreed to this policy. Even without signature, all users must follow this policy and report any misuse of the network to a teacher, supervisor or other appropriate administrator. If a user is uncertain about whether a particular use is acceptable or appropriate, he or she should consult a teacher, supervisor or other appropriate administrator.

Network Access

Access to the network is available to teachers and students as a source of information and a vehicle of communication. Students will be able to access the Internet through their teachers. Individual student accounts and e-mail addresses may be issued to students as authorized.

- Equal Opportunity – The Internet shall be available to all students within the Agency and its instructional programs.
- Making Internet access available to students carries with it the potential that some students might encounter information that may not be appropriate for students. Because information on the Internet appears, disappears, and changes, it is not always possible to predict or control what students may locate.
- The smooth operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines which require efficient, ethical and legal utilization of network resources.

Online Etiquette

The use of the network is a privilege and may be taken away for violation of Board policy or regulations. Users may be allowed access to other networks. Each network may have its own set of policies and procedures. It is the user's responsibility to abide by the policies and procedures of these other networks.

- Users should adhere to online protocol.
 1. Respect all copyright and license agreements.
 2. Cite all quotes, references, and sources.
 3. Apply the same privacy, ethical, and educational considerations utilized in other forms of communication.
- Students who are authorized for e-mail accounts by their teachers or principal will adhere to the following guidelines:
 1. Others may be able to read or access the mail, so private messages should not be sent.
 2. Delete unwanted messages
 3. Use of objectionable language is prohibited.

Unacceptable Uses of the Network

The agency reserves the right to take immediate action regarding activities (1) that create security and/or safety issues for the agency, students, employees, schools, network or computer resources, or (2) that expend agency resources on content the agency determines lacks legitimate educational content/purpose, or (3) other activities as determined by administrators as inappropriate. These are examples of inappropriate activity on the agency network:

- Violating any state or federal law or municipal ordinance, such as: Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials;
- Criminal activities that can be punished under law;
- Selling or purchasing illegal items or substances;
- Obtaining and/or using anonymous email sites; spamming; spreading viruses;
- Causing harm to others or damage to their property, such as:
 1. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials;
 2. Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity, impersonating other users, or sending anonymous email;
 3. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance;
 4. Using any agency computer to pursue "hacking," internal or external to the agency, or attempting to access information protected by privacy laws; or
 5. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes".

- Engaging in uses that jeopardize access or lead to unauthorized access into others' accounts or other computer networks, such as:
 1. Using another's account password(s) or identifier(s);
 2. Interfering with other users' ability to access their account(s); or
 3. Disclosing anyone's password to others or allowing them to use another's account(s).
- Using the network for Commercial purposes:
 1. Using the network for personal financial gain;
 2. Using the network for personal advertising, promotion, or financial gain; or
 3. Conducting for-profit business activities and/or engaging in non-government related fundraising or public relations activities such as solicitation for religious purposes, lobbying for personal political purposes.

Student Internet Safety

1. When using the Internet, students shall not reveal personal information about themselves or other persons. (e.g. name, home address, telephone number, or display photographs of themselves or others)
2. Students shall not meet in person anyone they have met only on the Internet; and
3. Students must abide by all laws, this Regulations for Acceptable Use and all other applicable agency policies.

The AEA will monitor the online activities of students and will educate students about appropriate online behavior, including interacting on social networking sites and chat rooms. Students will also be educated on cyberbullying, including awareness and response. Employees will provide age appropriate training for students who use the Internet. The training provided will be designed to promote the AEAs commitment to:

The standards and acceptable use of Internet services as set forth in the Internet Safety policy;
Student safety with regard to:

Safety on the Internet;

Appropriate behavior while online; on social networking web sites and in chat rooms;

Cyberbullying awareness and response.

Compliance with E-rate requirements of the Children's Internet Protection Act

In compliance with federal law, this policy will be maintained for at least five years beyond the termination of funding under the Children's Internet Protection Act (CIPA) or E-rate.

Penalties for Improper Use

The use of the agency equipment and network is a privilege, not a right, and misuse will result in the restriction or cancellation of those privileges. Misuse may also lead to disciplinary and/or legal action including suspension, expulsion (based on building "Student Code of Conduct" regulations), or criminal prosecution by government authorities. The agency will attempt to tailor any disciplinary action to the specific issues related to each violation.

Disclaimer

Central Rivers AEA makes no guarantees about the quality of the services provided and is not responsible for any claims, losses, damages, costs, or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the agency's network are to be borne by the user. Central Rivers AEA also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the agency, its affiliates, or employees.

Adopted: 06-04-2008

Amended: 08-12-2015

Reviewed: 11-04-2015

Reviewed: 06-03-2020

Amended: 10/01/2025