

Acceptable Use/Social Networking Policy

Central Rivers AEA recognizes the importance of technology devices and resources in support of the mission and goals of the agency and its programs. To this end, Central Rivers AEA encourages the responsible use of all devices; computer networks, including the Internet; and other electronic resources.

Central Rivers AEA employees are expected to use devices, computer networks, including the Internet; and other electronic resources in a professional and ethical manner consistent with state laws governing the behavior of agency employees and federal laws governing copyright. While technology resources are provided primarily for business purposes, limited personal use is permitted, provided that it does not interfere with work responsibilities, consume excessive system resources, or violate Agency policies or applicable laws.

The Agency shall comply with the provisions of the Children's Internet Protection Act of 2001.

The Agency reserves the right to monitor all use of its technology resources, including but not limited to email, internet access, and file transfers, to ensure appropriate use, protect system integrity, and maintain compliance with Board policies and applicable laws. Files may be reviewed, audited, or accessed by authorized personnel as needed for system maintenance, legal compliance, or investigation of misuse. The person in whose name an account is issued is responsible at all times for its proper use.

Employees must take reasonable steps to protect data and system security, including safeguarding passwords, logging out of shared devices, avoiding suspicious links or downloads, and reporting suspected phishing attempts or data breaches to IT staff immediately.

It is the responsibility of the AEA Administration to establish guidelines on Acceptable Use. AEA Administration will publish and disseminate these guidelines to all staff and students. Reasonable efforts will be made to train staff and students on these guidelines.

Social Networking or Other External WebSites.

For purposes of this policy, any website, other than the Agency website or Agency sanctioned websites, are considered external websites. Employees shall not post confidential or proprietary information, including photographic images, about the Agency, its employees, students, agents or others on any external website without consent of the Chief Administrator or designee. The employee shall adhere to all applicable privacy and confidentiality policies adopted by the

Agency when on external websites. Employees shall not use the Agency logos, images, iconography, etc. on external websites. Employees shall not use Agency time or property on external sites that are not in direct-relation to the employee's job. Employees, students, and volunteers need to realize that the Internet is not a closed system and anything posted on an external site may be viewed by others, all over the world. Employees, students and volunteers who don't want Agency administrators to know their personal information, should refrain from exposing it on the Internet.

Employees must maintain appropriate professional boundaries with students when using any online platforms. Connecting with students via personal social media accounts is prohibited unless specifically approved by the Chief Administrator or designee. Employees, who would like to start a social media site for Agency sanctioned activities should contact the Chief Administrator or designee. All social media accounts created for Agency-related purposes must comply with Agency branding, accessibility, and content standards.

Legal Reference:

Iowa Reference:

Iowa Code § 279.8 (1995)

Children's Internet Protection Act of 2001

Approved:06-04-08

Amended: 08-12-15

Reviewed: 11-4-15

Reviewed: 06-03-2020

Amended: 10/01/2025