

**Auraria Higher Education Center
Office of the Executive Vice President for Administration
Administrative Policies and Procedures**

**Policy #11
Electronic Communications**

Page 1 of 2

Approved: February 1999

Revised: October 8, 2001
Revised: May 22, 2003

EVPA Signature: 

Policy

Electronic Communications at the Auraria Higher Education Center is provided to employees as a tool to improve productivity and empower them to better serve their campus customers. Electronic Communications includes transmission, receipt, retention, monitoring, and disclosure of electronic communications including, but not limited to e-mail and voice mail communications at the Auraria Higher Education Center (AHEC). All electronic messages transmitted through internal, local, regional, or global computer or voice networks shall be governed by this policy.

Status of Electronic Correspondence

All electronic correspondence by AHEC employees may be a public record under the Colorado Public Records Law, and may be subject to public inspection under CRS Section 24-72-203.

Transmission and Receipt of Information

All electronic transmissions or communications, whether generated or received by an AHEC employee, shall be considered to be subject to this policy. E-mail and voice mail systems are maintained for AHEC business purposes, and all entries are considered AHEC property. Transmission and receipt of messages should be limited to business purposes. AHEC employees have no right of privacy to electronic communications. Only persons formally designated by the Executive Vice President for Administration and/or the Division Directors are authorized to send all user e-mails.

Acceptable Use

People using AHEC computers, who have access to the network, will be expected to abide by the following rules:

- All illegal activities are prohibited. Prohibited activities include but are not limited to distributing copyrighted materials such as software, text or images in ways prohibited by the copyright holder, breaking into computers or computer accounts that are not authorized to use, and monitoring network traffic or obtaining passwords or other private information.
- All commercial activities other than Auraria Higher Education Center business are prohibited. Specifically, resale of network connectivity or operations of a business through the network are prohibited.
- Placing an excessive load on central computers is prohibited. If monitoring reveals that a program is placing an excessive load on the central computer, the offending program will be

terminated. Special arrangements must be made for running programs that legitimately require large amounts of computer time.

- Interfering with legitimate use of network resources by others is prohibited. For example, activities such as using packet sniffers to monitor network communications, harassing others of the network, damaging other people's files, propagating chain electronic letters, sending junk electronic mail, and posting articles to multiple inappropriate newsgroups are prohibited. Persons found to be interfering with legitimate use of network resources by others may have their network access privileges revoked.
- AHEC policies regarding workplace violence and discrimination including sexual harassment apply without exception to all computer usage, including electronic mail and viewing, downloading and forwarding potentially violent, discriminatory and/or sexually explicit internet sites or emails.

Persons found using AHEC computers or the campus network for illegal, commercial activities, excessive personal use, interfering with legitimate use of network resources by others, or to download or forward potentially violent, discriminatory and/or sexually explicit materials, may have their network access privileges revoked, may be subject to corrective and/or disciplinary action up to and including termination and evidence of illegal use of the network turned over to appropriate authorities.

Retention

AHEC shall retain back-up records of e-mail disks on the mail server computers for 30 days after transmission or receipt of electronic communication. After such time, all back up shall be deleted from the mail server computers. Work related emails may be stored indefinitely, but all users are strongly encouraged to use discipline and common sense in minimizing the storage of any email more than 30 days. In the event of a public or "open records" request, each employee may be responsible for searching his or her email files and responding as directed.

Monitoring

Traffic on the AHEC computer network is monitored by the IT department. More detailed monitoring may occur if there is reason to suspect unauthorized or unacceptable computer usage of the computer or network. AHEC reserves the right to monitor all electronic communications if it is determined by the sole discretion of the Executive Vice President for Administration.

Disclosure

AHEC will engage in the discovery and disclosure of electronic communication or correspondence where necessitated by law, rule, regulation, or legal proceeding. AHEC is in compliance and cooperation with the Patriot Act and the Office of Homeland Security.

Access to electronic communications and computers by AHEC employees must be approved on a continuing basis by each employee's supervisor, and may be terminated at any time.