A 6.9 ASSUMPTION OF PRIVACY AND INTERNET USE

Nothing contained within this Handbook may be interpreted as giving an employee an expectation of privacy. Offices, desks, computers, email, file cabinets, and other furniture and equipment provided by the State or from a grant, are not private although certain spaces may contain records that are specifically confidential. Each employee must ensure that there is clear access at all times to any materials or information which may be needed to conduct the business of ECU.

If you abuse your right to use the Internet, this right may be taken from you. In addition, you may be subject to disciplinary action, including possible termination, and civil and criminal liability.

Your use of the Internet is governed by this policy.

There is no expectation of privacy. The computers and computer accounts given to employees are to assist them in performance of their jobs. Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the University and may only be used for business purposes.

A 6.9.1 Monitoring Computer Usage

The university has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites visited by employees on the Internet, monitoring chat groups and news groups, reviewing material downloaded or uploaded by users to the Internet, and reviewing e-mail sent and received by users. The University cooperates fully with all duly constituted law enforcement agencies in cases of violation of applicable law. Use of University Network facilities, services, and information technologies does not alter basic codes of behavior of academic life.

A 6.9.2 Blocking of Inappropriate Content

The University may use software to identify inappropriate or sexually explicit Internet sites. Such sites may be blocked from access by University networks, unless you have prior approval to view such sites as part of regiment research. In the event you nonetheless encounter inappropriate or sexually explicit material while browsing on the Internet, immediately disconnect from the site, regardless of whether the site was subject to university blocking software.

A 6.9.3 Prohibited Activities

Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful, inappropriate, offensive (including offensive material concerning sex, race, color, national origin, religion, age, disability, sexual orientation or other characteristic protected by law), or violating ECU's equal employment opportunity policy and its policies against sexual or other harassment may not be downloaded from the Internet or displayed or sent or stored in ECU's computers. Employees encountering or receiving this kind of material should immediately report the incident to their supervisors or the Employment Services Office.

Behaviors which are not permitted on university networks include but are not limited to:

- Violation of local, state or federal laws, RUSO or University policy
- Sharing confidential information on students or employees
- Assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition
- Engaging in practices that threaten the integrity of the University computer facilities, services and information technologies network (e.g., loading files that may introduce a virus or installing software not previously approved). Downloading and installing software is only allowed with prior approval from Information Technology. This also applies to the installation of hardware.
- Using others' accounts
- Trespassing in others' folders, documents, or files
- Intentionally wasting limited resources
- Employing the network for personal enterprises or business purposes
- Violating the ONENET Acceptable Use Policy (http://lib.ok.us/clientservices/category1/sub3/acceptableuse.htm)
- Violation of the ECU Electronic Mail Acceptable Use Policy

The Network Supervisor will report inappropriate behaviors to the University administration who will take appropriate disciplinary action. Any other reports of inappropriate behavior, violations, or complaints will be routed to the employee's supervisor for appropriate action. Violations may result in a loss of access and/or disciplinary action, including termination.

A 6.9.4 Games and Entertainment Software

Employees may not use the university's Internet connection to download games or other entertainment software, including wallpaper and screen savers, or to play games over the Internet.

A 6.9.5 Illegal Copying

Employees may not illegally copy material protected under copyright law or make that material available to others for copying. You 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. For example, copying or downloading movies, music or other copyrighted materials is against the law. Peer-to-peer sharing of the copyrighted materials is also against the law.

A 6.9.6 Amendments and Revisions

This policy may be amended or revised from time to time, in writing, by the President as the need arises. Users will be provided with copies of all amendments and revisions.

Violations of this policy will be taken seriously and may result in disciplinary action, including termination, and possible civil and criminal liability.

A 6.10 E-MAIL POLICY

Computing services at East Central University are provided to promote administrative, educational, and research efforts of the faculty, students, and staff. All persons utilizing these services are responsible to ensure that computing services are used in an ethical and lawful manner.

Violations of electronic mail may result in the revocation of computer privileges. In addition, such actions may result in disciplinary review, sanctions, dismissal from the University, and legal action. Violations of the Electronic Mail Policy may constitute a criminal offense, punishable by local, state, or federal law.

Electronic mail communications are often the only contact you may have with a constituent. Therefore, email sent via any of the University's electronic communications systems must project a positive image of the University.

- All emails sent via the University’s electronic communications systems should contain your name, title, and University contact information.
- No logos, slogans, quotes, or taglines including, but not limited to the ECU logo and tagline, should be part of an email signature.