

Northwestern Oklahoma State University

Networked Information Resources Acceptable Use Policies and Procedures

The NWOSU network is a shared resource acquired and maintained to carry out the education, research, and public service mission of the University. The NWOSU network comprises email messages, text messages, social media and social networking sites; computers, laptops, cell phones, email, and other electronic devices whether University owned or privately owned when linked to LAN and WiFi provided by the University. Communications over the network are often public in nature; therefore, faculty and staff are reminded that general rules and standards for professional behavior and communications will apply. Except for insignificant and incidental use, faculty and staff may not use the NWOSU network for personal, non-public or non-University purposes. The network is primarily intended for the use of faculty, staff and students. Others wanting access to the network, including PC's in labs, must first check with the supervisor of the equipment and pay such fees as set by the University.

Faculty, staff and students may employ e-mail as a mode of official communication. All NWOSU faculty, staff and students will be assigned and be required to use NWOSU email accounts for any official email correspondence. The University may rely on this medium to communicate official information; therefore, faculty, staff and students are responsible for checking and reading messages on their NWOSU email account on a regular basis.

Electronic mail and communication are not to be utilized by employees and students to share confidential information about students or employees. Employees have no expectation of privacy with regards to the use of electronic mail.

Network administrators may review files and communications to maintain system integrity. Users should not assume that files stored on university servers will be private. (Electronic Communications Privacy Act 18 USC §2701 (1988).) Users have no expectation of privacy with regards to any computer equipment belonging to NWOSU or to the use of the NWOSU network with private computer equipment. 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.

Behaviors which are not permitted by the University include but are not limited to:

- Violation of local, State or federal laws, RUSO or University policy
- Sharing confidential information on students or employees
- Sending, sharing or displaying obscene pictures, images or messages
- Searching for, downloading, uploading, storing, sending, sharing or displaying child pornography
- Assisting a campaign for election of any person to any office or for the promotion of or opposition to any ballot proposition
- Using obscene language
- Threatening, stalking, or harassing communications in violation of federal, state, or local laws, including but not limited to the Violence Against Women Act, Title IX of the Education Amendments of 1972 as amended, and Titles VI and VII of the Civil Rights Act of 1964, as amended
- Engaging in practices that threaten the integrity of the University computer facilities, services and information technologies (e.g., loading files that may introduce a virus or installing software not previously approved). Downloading and installation of software is only allowed with prior approval from Information Technology. This also applies to the installation of hardware
- Violating copyright laws. 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.
- 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://onenet.net/current-customers/acceptable-use-policy/>)
- Surveillance or taping of others and/or taking non-consensual or abusive advantage of another; examples include, but are not limited to, non-consensual video or audio taping of sexual activity.
- Internet use that constitutes invading rights of others to include, but not limited to, harassment based on sex, race, color, national origin or disability

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.

Each employee will be given copies of this policy and procedures and will sign an acceptable use agreement before establishing an account.