I. Purpose
The purpose of the Acceptable Use Policy is to establish guidelines for respecting the rights and obligations of academic freedom while protecting the rights of others.

II. Scope
This policy applies to faculty, staff, students, contractors, consultants, temporaries, official university affiliates, and others who use the University’s computing resources. These resources include all phone, video, and data communications. This policy applies to all equipment that is owned or leased by The University of Oklahoma.

III. Policy
Access to the information resource infrastructure both within and beyond the University campus, sharing of information, and security of the intellectual products of the community all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at The University of Oklahoma is a privilege granted to University students, faculty, staff, and third parties who have been granted special permission to use such facilities.

The University reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Data owners—whether departments, units, faculty, students, or staff—may allow individuals other than University faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement, University policy, or any federal, state, county, or local law or ordinance. Users are personally responsible for all activities that take place with their OUNetID (4+4).

Authorized User Purposes
Use of University computers must comply with Federal and State law and University policies. University computing facilities and accounts are to be used for the University-related activities for which they are assigned. When users cease to be members of the academic community (such as by graduating or ceasing employment), or when persons are assigned to a new position and/or responsibilities within the University, the access authorization of such person will be reviewed and may be altered. Users whose relationships with the University change may not use computers and computing resources, facilities, accounts, access codes, privileges, or information for which they are not authorized in their new relation to the University.

Users may use only their own computer accounts. The negligence or naivete of another user in revealing an account name or password is not considered authorized use. Convenience of file or printer sharing is not sufficient reason for sharing a computer account. Users are personally responsible for all use of their computer account(s).

Examples of appropriate use of computing and networking resources include but are not limited to:

- Instruction
- Independent study
- Authorized research
- Independent research
- Communications
- Official work of the offices, units, recognized student and campus organizations, and agencies of the University.

Unauthorized User Purposes
Anyone who accesses, uses, destroys, alters, or damages University information resources, properties or facilities without authorization, may be guilty of violating state or federal law, infringing upon the privacy of others, injuring or misappropriating the work produced and records maintained by others, and/or threatening the integrity of information kept within these systems. Such conduct is unethical and unacceptable and will subject violators of this policy to disciplinary action by the University, including possible termination from employment, expulsion as a student, and/or loss of computing systems privileges.