



## Acceptable Use Policy

---

**Effective: 05/14/2008**

**Updated: 3/14/2014**

**Pages: 6**

---

### I. Purpose

Wilkes University owns and operates a variety of technology resources that are provided for the use of Wilkes University students, faculty, staff, alumni, contractors, and guests in support of the mission of the University and are to be used for education, research, academic development, and public service. All users are responsible for seeing that these resources are used in an effective, efficient, ethical, and lawful manner.

Appropriate and responsible use of the Wilkes University technology resources is defined as use that is consistent with the teaching, learning, research, and administrative objectives of the University and with the specific objectives of the project or task for which such use was authorized. All uses inconsistent with these objectives are considered to be inappropriate use.

This document establishes rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited and is grounds for loss of computing privileges as well as University disciplinary sanctions and/or legal sanctions under Federal, State, and local laws.

### II. Applicability

This policy applies to all persons accessing Wilkes University's technology resources, which include faculty, staff, students, alumni, emeriti, contractors, guests or any other authorized user. All technology resources of the University are covered by this policy, including without limitation all networks, supported infrastructure, servers, computers, printers, copiers, scanners, other peripherals, mobile devices

including tablets and cell phones, remote systems, software, and connecting resources of any kind, including external networks.

### III. **Policy**

#### **Agreement**

By using any of Wilkes University's technology resources, users consent to assume personal responsibility for their appropriate use and agree to comply with all applicable university policies and local, State, and Federal laws and regulations. Commercial and partisan political activity not related to the mission of the University is prohibited.

#### **Rights**

These technology resources are owned and operated by Wilkes University. The University reserves all rights, including termination of service without notice, to the technology resources that it owns and operates. These procedures shall not be construed as a waiver of any rights of Wilkes University, nor shall they conflict with applicable acts of law. Users have rights that may be protected by Federal, State, and local laws.

#### **Privileges**

Access and privileges on Wilkes University technology resources are assigned and managed by the administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system. Users may not, under any circumstances, transfer or confer these privileges or share their access credentials with other individuals with the exception of Information Technology Services support staff for support-related functions. The authorized user is responsible for the proper use of the system, including any password protection.

#### **Accounts**

Once an account is assigned to an individual, others must not use that account. The individual is responsible for the proper use of the account, including proper password protection, safeguarding confidential data, and following security policies.

#### **Confidentiality**

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. Wilkes University reserves the right to access all information stored on Wilkes University systems. File owners will be notified of file access and/or maintenance in advance if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately to the appropriate supervisor.

**System Usage**

Technology resources are for University related and sanctioned activities. Fraudulent, harassing, or obscene messages and/or materials are not to be sent except for investigative purposes.

**System Performance**

No one should deliberately attempt to degrade the performance of a University system or to deprive authorized personnel of resources or access to any University system.

**Unauthorized Access**

Security loopholes or knowledge of access credentials should not be used to damage systems, obtain extra resources, take resources from another user, gain access to systems, or use systems for which proper authorization has not been given. Discovery of the ability for unauthorized access should be reported immediately to Information Technology Services.

**Copyright**

Software protected by copyright is not to be copied from, into, or by using University systems, except as permitted by law or by the contract with the owner of the copyright. This means that such software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original licenses purchased by that department. License codes provided to individuals or departments should be kept confidential. Users will be responsible for assuring that they do not violate the terms of the software licenses installed on their systems.

Additionally, the downloading of electronic information (e.g. text, music, video) that is copyright protected is prohibited beyond Federal "fair-use" limitations without the permission of the holder of the copyright. Again, users must comply with all applicable university policies and local, State, and Federal laws and regulations regarding copyright protection of electronic resources.

**Violations**

An individual's access and computing privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations among employees will be confidentially reported to the appropriate supervisors. Suspected violations among students will be reported to the Dean of Students.

Violations of these policies will be dealt with in the same manner as violations of other University policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computing privileges, dismissal from the university, and legal action. Violations of some of the above policies may constitute a criminal offense.

## **Privacy**

The University respects the privacy of its users and does not routinely inspect or monitor user files. In the course of their duties, system administrators may see your electronic files. Subject to the requirements for authorization, notification, and other conditions specified in this policy, the University may inspect, monitor, disclose, or deny access to user data:

- (a) when required by and consistent with law;
- (b) when there is substantiated reason (reliable evidence indicating that violation of law or of policies probably has occurred) to believe that violations of law or of University policies have taken place;
- (c) when there are compelling circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of University policy, or significant liability to the University or to member of the University community; or
- (d) under time-dependent, critical operational circumstances where failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations.

Whether or not it is created or stored on University systems, data may constitute a University record subject to disclosure under the Pennsylvania Open Records Laws (Sunshine Act and the Right-to-Know Law), or other laws, or as a result of litigation. However, the University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

Destruction of such records is governed by the University's records retention policies.

### **Additional Guidelines**

The IT Committee may establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines may cover such issues as allowable disk space, responsibility for account approval, and other items related to administering the system.

## **IV. Responsibilities**

Users are responsible for maintaining the following:

- a. An environment conducive to learning. A user who harasses or makes defamatory remarks shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that Wilkes University's role in managing these systems is only as an information carrier

and that they will never consider transmission through these systems as an endorsement of said transmission by Wilkes University.

Users agree not to misrepresent themselves or mask their identities.

Users should assume that anything they access might be copyrighted. Absence of a © notice does not mean that the material is not copyrighted. This means that before a user downloads a document, image, or any other media they should ensure that its use is in accordance with “fair-use” limitations or should obtain the author’s permission.

Many University systems provide access to outside networks, both public and private, which furnish electronic mail, information services, discussion boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that Wilkes University does not assume responsibility for the contents of any of these outside networks.

The user agrees to comply with the Acceptable Use guidelines for whichever outside networks or systems they may access through Wilkes University systems.

Further, the user agrees to follow proper etiquette on non-Wilkes systems and networks. Information regarding etiquette is available through system administrators and through specific individual networks.

The user agrees never to knowingly attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service). The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not Wilkes University, which is acting solely as the information carrier.

- b. An environment free of illegal or malicious acts. The user agrees never to use a University technology resource to perform an illegal or malicious act. Any attempt to increase a user’s authorized level of access or deprive other authorized users of resources or access to any University system shall be regarded as malicious and may be treated as an illegal act.
- c. A secure environment. Any user who finds a possible security lapse on any system is obliged to report it to the system administrators including Information Technology Services.

Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.