



INFORMATION TECHNOLOGY POLICIES

Section 800: Information Security	Policy Number: 803.0 Acceptable Use Policy
New: _____ Revised: <u> X </u>	Effective Date: 01/01/2004 Last Revised:
Scope: Information Technology	Authority: Executive Director of ITS

803.0 Title **Acceptable Use Policy**

803.1 Philosophy Technology resources provided by Otterbein University are made available to students, faculty, staff and approved guests primarily as tools for enhancing and facilitating teaching, learning, and scholarly research.

803.2 Statement

Resources and Primary Uses

- Resources include, but are not limited to, hardware and software either owned or leased by the University, and consulting time and expertise of Otterbein University employees. Additionally, owners of personal equipment that is connected to the data or telecommunications infrastructure of the University are also subject to these policies.
- Use of the resources for instructional and administrative activities directly related to the mission of the University shall have priority over personal or recreational use of resources.
- Many of the technology resources of the University are shared among the entire University community. Activities involving these resources must be in accord with the University policies found in faculty and staff handbooks, the Campus Life Handbook; all relevant local, state, federal laws and international agreements; and all contracts and licenses.

Ethical Use

- It is the intent of the University to maintain a campus environment that facilitates access and sharing of information without fear that an individual's work will be violated by misrepresentation, tampering, destruction and/or theft.
- The privilege of using these resources carries with it the responsibility for ethical behavior. Unethical behavior will not be tolerated and includes, but is not limited to:
 - activities that obstruct usage or deny access to others
 - activities that compromise privacy
 - activities that could be considered harassment or libelous



- attempts to gain unauthorized access to local or remote information resources
- activities that violate copyright laws (this includes unauthorized copying and distribution of commercial software, text, graphic images, audio and video recordings)
- activities that violate University policies and standards of conduct
- destruction or alteration of data or information belonging to others
- activities that violate local, state, or federal laws
- unauthorized use of computer accounts or impersonating other individuals
- creating, using or distributing programs intended to damage data files, application programs, system operations, or network operations
- attempts to capture or crack passwords or break encryption protocols
- allowing anyone else to use your account(s)
- extensive use of resources for private or personal use
- use of resources for commercial and/or financial gain
- violation of licensing agreements for information resources
- knowing or reckless distribution of unwanted mail or other messages, specifically "chain letters" and other schemes that may cause excessive network traffic or computing load
- unauthorized extension or retransmission of Otterbein network services

Privacy

The University places a high value on privacy and recognizes its critical importance in an academic setting. Nevertheless, computer users should be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and such activities that are necessary for the rendition of service. Computer users should be aware that information may appear on system backups, and even the deletion of messages or files may not eliminate them from the system. Further, where it appears that the integrity, security or functionality of the University's computer or network resources are at risk; or to protect the University from liability; or in instances of abuse of University policies, codes, or local, state or federal laws, Otterbein University reserves the right to take whatever actions it considers necessary (including, but not limited to monitoring activity and viewing files) to investigate and resolve the situation. Any such individual monitoring, other than as required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the Director of Information Technology or the Director's designees. In such instances, a written report of the findings will be forwarded to the appropriate University officials or civil authorities (see the Violations of Policy section, below). In order to assure



continuity for academic and administrative departments, similar procedures may be used after an employee is separated from Otterbein or is no longer able to perform the required duties.

Violations of Policy

Student violations of this policy, such as computer time/theft/abuse (as included in the [Campus Life Handbook](#) located on the student conduct page), will be addressed through the Student Affairs Office. Employee violations of this policy are addressed in the Policies and Procedures Manual for Salaried and Hourly Staff or in the Union Contract. Violations of this policy by administrative staff, non-exempt staff and union employees are handled through the Office of Human Resources. Faculty violations are handled through the Academic Dean's Office. Violations of local, state or federal laws will be reported to the appropriate authorities. The University may temporarily suspend or block access to an account or remove files, when reasonably necessary to do so in order to protect the integrity, security or functionality of University or other computing resources or to protect the University from liability. Any such suspension or blocking of access to an account, other than as required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the Director of Information Technology or the Director's designees.

Copyright

Otterbein University is committed to complying with [U.S. copyright law](#) and expects all users of the University's technology resources to do the same.

Amendment of Policy

Otterbein University reserves the right to amend this policy at any time with 90 days notice.

- | | | |
|--------------|-------------------------|------|
| 803.4 | Attachments | None |
| 803.5 | Related Policies | None |