Section 800: Information Security	Policy Number: 803.0 Acceptable Use Policy
New: _____ Revised: __X_	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 84 4pBys. Additing

- o attempts to gain unauthorized access to local or remote information resources
- o activities that violate copyright laws (this includes unauthorized copying and distribution of commercial software, text, graphic images, audio and video recordings)
- o activities that violate University policies and standards of conduct
- o destruction or alteration of data or information belonging to others
- o activities that violate local, state, or federal laws
- o unauthorized use of computer accounts or impersonating other individuals
- o creating, using or distributing programs intended to damage data files, application programs, system operations, or network operations
- o attempts to capture or crack passwords or break encryption protocols
- o allowing anyone else to use your account(s)
- o extensive use of resources for private or personal use
- o use of resources for commercial and/or financial gain
- o violation of licensing agreements for information resources
- o 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
- o 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

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 of files may not eliminate them from the system. Further, where it appears that the integrity, security or func
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

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