MERCER UNIVERSITY	**SECTION:**

Policies and Procedures Manual

SUBJECT: **INFORMATION TECHNOLOGY ACCESS AND USE POLICY**	**EFFECTIVE:** January 1, 2004

PURPOSE: To establish policies and procedures for the use of University-owned and -operated information technology resources.

Mercer University is dedicated to the missions of teaching, education, research, and public service. In support of these missions, Mercer University provides access to electronic information resources, including networks, software, and equipment, to its students, faculty, and staff.

The Mercer University Information Technology Policy (the "Policy") contains Mercer’s philosophy and requirements governing the use of its information technology resources by students, faculty, staff, and others who have been given authorization, either explicitly or implicitly, to access those resources. Mercer University expects each member of the community to use Mercer’s information technology resources, including connections to resources external to Mercer that are made possible by Mercer University's information technology resources, responsibly, ethically, and in compliance with the Policy, relevant laws, and all contractual obligations to third parties. The use of Mercer University's information technology resources is a privilege. If a member of the Mercer community fails to comply with this policy or relevant laws and contractual obligations, that member's privilege to access and use Mercer's information technology resources may be revoked. The use of Mercer University's information technology resources to send communications to Mercer or non-Mercer persons or entities typically identifies the sender as belonging to the Mercer University community. Each member of the community should, therefore, recognize that any such communication might reflect on how Mercer University is perceived by the Mercer community and the public at large.

By adopting the Policy, Mercer University recognizes that all members of the Mercer community are bound not only by the Policy, but also by local, state, and federal laws relating to electronic media, copyrights, privacy, and security. Other Mercer University policies that relate to this Policy and also apply to Mercer University students, faculty, and staff (collectively, the "community") can be found in the Mercer University Student, Faculty, and Employee Handbooks. Each member of the Mercer University community is expected to be familiar with this and all other relevant policies.

Freedom of Expression & Misconduct

Freedom of expression and an open environment within which to pursue scholarly inquiry and to share information are encouraged, supported, and protected at Mercer University. Censorship is not compatible with the goals of Mercer University. While Mercer may limit the use of some computers or resources to specific research or teaching missions, freedom of expression will generally be protected. While Mercer University rejects censorship, behavior that constitutes misconduct will not be protected. Such behavior includes, but is not limited to, the use of Mercer University's information technology resources in connection with child pornography, harassment of any kind, copyright infringement, theft, unauthorized access, and other violations of the law.

To comply with federal regulations governing tax-exempt organizations, Mercer University technology resources may not be used for mass and unsolicited communications used in connection with lobbying (except official Mercer University activities authorized by the Office of the President) or political campaigns. In addition, such resources should not be used for private business or commercial activities, except where such activities are otherwise permitted under applicable Mercer University policies. It must be understood that most software licenses purchased by the University stipulate that all use must be for educational or institutional administrative purposes only.

Privacy

Users should respect the rights of others to privacy and intellectual property rights and refrain from unauthorized access or copying. State and federal law and Mercer University policy prohibits unauthorized access to computer and telephone systems. No one should use aliases, nicknames, pointers, or other electronic means to capture information intended for others without permission of the intended recipient. Attempts to gain unauthorized access to machines or computer records, to decrypt encrypted materials, to monitor other individuals' computer or network use, to attempt to obtain their passwords, or to obtain privileges or information to which the user is not entitled are prohibited. Passwords are private, personal information, which should not be written down, posted or otherwise shared with others. Attempts to use another person’s password or to hack another person’s password are a violation of University Policy, and will be dealt with accordingly. Any attempt to make use of another person’s password or to access another person’s account or information may result in immediate termination of access to Mercer’s computer and network resources as well as judicial or criminal prosecution as defined by the appropriate existing law or policy.

If an account holder allows public access to files via file sharing, it is presumed that the account holder does not intend to keep those files private from other users. (See “Security” for warnings regarding file sharing.)

Information Technology systems support staff, systems operators, supervisors, and designated University officials may access information resources to locate and protect business information, maintain system and network resources, ensure system and network security, provide technical support, comply with legal requirements, or administer Mercer University policies. Information Technology personnel are not authorized to access or make use of any user's password-protected data without specific authorization from the user or direction from University Legal Counsel, Internal Audit, Human Resources, or Mercer Police. Attempts to do so will result in immediate termination of employment and could result in criminal prosecution.

Local area networks and local resources, including personal computers, workstations, file servers, printers, and similar devices shall be subject to the same rights to privacy and confidentiality afforded centralized computer systems regardless of whether those local resources are connected to any of Mercer University's central information technology networks.

Intellectual Property

Mercer University expects all members of the community to be aware of how intellectual property laws, regulations, and policies apply to the electronic environment and to respect the property of others. For further information, please see the Mercer University Copyright Policy, the Mercer University Policy and Guidelines on Copyrighted Materials, the Mercer University Patent Policy, the Mercer University Academic Honor Principle, and the Mercer University Faculty, Staff, and Student Handbooks.

No member of the community shall use another's content or property in a way that violates copyright law or infringes upon the rights held by others. The unauthorized duplication or use of any electronic material that is licensed or protected by copyright may constitute violations of civil and criminal law and is prohibited by this policy.

Members of the University community should recognize that placing individual work in the electronic public domain may result in widespread distribution of that work and could jeopardize their rights to that work. You should assume that works communicated through the network are subject to copyright unless there is a specific disclaimer to the contrary.

Internet Access

Mercer University maintains computer facilities and Internet access for its primary missions of teaching, education, research, and public service. Excessive use of the Internet for other purposes places an unreasonable burden on the Mercer network and interferes with access for legitimate use. Using the University network for occasional access to the Internet for personal purposes is not specifically prohibited. However, the Department of Information Technology is charged with the responsibility of ensuring recreational use does not interfere with legitimate educational and administrative access. When necessary, Information Technology staff will restrict activities as required to ensure all authorized users have adequate access to the Internet.

Violations of Internet use include, but are not limited to, accessing, downloading, uploading, saving, receiving, or sending material that includes sexually explicit content or other material using vulgar, sexist, racist, threatening, violent, or defamatory language.

Users should make economical and wise use of computer and network resources. Users should report suspected unauthorized use of resources to the Department of Information Technology. Theft, failure to observe copyright laws, and/or tampering with any computer system or network device will place violators in jeopardy of losing privileges as well as possible criminal prosecution. Each incident will be handled on a case-by-case basis and may be referred to University Legal Counsel or other appropriate authority.

Rights and Privileges

The names of students, faculty, and staff are entered into an electronic database of names along with associated items of information. An entry in the Mercer University Name Directory, administered by Information Technology, grants access to network services that originate at Mercer University and requires user authentication. Students have the right to request, through the Registrar's Office, that their information not be made available to anyone inside or outside the University. If a student has requested that their information not be published, their name and e-mail address will be published in Mercer's internal address books to facilitate communication; however, this information will not be accessible from off campus. Faculty and staff work contact information will be made available to Mercer and non-Mercer users except as required by law. Faculty and staff may request that their personal contact information not be published or made available.

Having an account is a privilege, not a right or entitlement. An individual is assigned an account for use while conducting activities related to the mission of Mercer University. The holder of an account may not share access information that would enable use of an account with anyone including colleagues at Mercer University, family members, or any other individual. Any account may be revoked temporarily or permanently if a user of University information technology resources violates public law or University policy.

Security

Personal computers and workstations are intended for use as "clients" that request computing services rather than "servers" that provide computing services. Providing services to other users, such as other Mercer network users or the Internet at large, potentially consumes excessive amounts of network bandwidth and compromises network security. Without explicit, written authorization from the Department of Information Technology, computers shall not be configured to operate as servers, including but not limited to: file, print, mail, web, chat, media streaming, name, time, directory, quote, network management, or proxy servers. Any computer ostensibly configured as a client but running special software that provides services to other users is regarded as being a server and deemed to be in violation of this policy. University information technology support personnel may restrict, limit, or disable specific application traffic to ensure that other mission-critical network traffic is not affected or disrupted in any way.

No user shall attempt to access any service or resource to which they have not been explicitly authorized access by the appropriate University authority. All network access ports are provided for use with a single computer system. No router, wireless access point, hub, or other network device may be installed in any Mercer facility without prior review and written approval from the Department of Information Technology. Users of the University network shall not perform any activity which disrupts network or server resources, impedes or prevents network or server access by others, or attempts to access private data of others. Examples include, but are not limited to, port scanning software, packet sniffers, mail bombing, ping flooding, SMURF attacks, and/or SYN flooding. Users found to be in violation of this policy will be denied access without prior notice.

Any user of the University network who disrupts or obstructs, whether intentionally or inadvertently, teaching, research, administration, or other University activities will be subject to disciplinary sanctions as outlined in existing University policy.

In order to ensure the security of Mercer's networks and the systems attached to those networks, Information Technology has implemented a security system which will ensure that all student, faculty, and staff systems are adequately protected. This system will scan each user's computer for viruses, worms, and exploits and will also ensure that each computer has up-to-date virus/worm protection and that all patches required to ensure the security of the system have been applied. All system checks must be completed successfully before access to the University network will be allowed. Compromised or insecure systems will be directed to a web site which will assist the user with the process of ensuring that their system is adequately protected. This security system does not search for or collect any user's personal information contained on any computer.

E-mail

In general, use of University electronic mail services is governed by policies that apply to the use of all University facilities. In particular, the use of University electronic mail services is encouraged subject to the following conditions:

> **Purpose** - Electronic mail services are to be provided by University organizational units in support of the teaching, research, and public service mission of the University, and the administrative functions that support this mission.
> **Users** - Users of University electronic mail services are to be limited primarily to University students, faculty, and staff for purposes that support the mission of the University.
> **Non-Competition** - University electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside the University.
> **Restrictions** - University electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of the University; personal financial gain (see applicable academic & personnel policies); or uses that violate other University policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment.
> **Representation** - Electronic mail users shall not give the impression they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University unless appropriately authorized to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing the University. An appropriate disclaimer is: "These statements are my own, not those of Mercer University."

Mercer University prohibits the use of University's electronic communications resources for any purpose that could unnecessarily strain or compromise these resources. Mercer University also prohibits electronic communications that interfere with the use of these resources by other employees. Toward this end, University resources may not be used to:

> **Perpetuate chain e-mail letters or their equivalents** - This includes letters that require the recipient to forward an e-mail to a specified number of addresses in order to achieve some monetary, philosophical, political, superstitious, or other goal. E-mails that are part of a multilevel marketing or pyramid-selling scheme, sometimes known as "Ponzi schemes," are generally illegal and are specifically forbidden under this policy.
>
> **Create and/or send "spam"** - Spam is defined as any unsolicited electronic communication that is sent to any number of recipients who did not specifically request or express an interest in the material advertised in the communication.
>
> **Send or encourage "letter bombs"** - Letter bombs are extremely large or numerous e-mail messages that are intended to annoy, interfere with, or deny e-mail use by one or more recipients.
>
> **Practice any activity designed to deny the availability of electronic communications resources** - Also called "denial of service attacks," these activities deny or limit services through mail bombing, malicious executables such as viruses, threatening a virus, or opening a large number of mail connections to a mail host or SMTP relay without authorization or permission.

Wireless Network Access & Usage

Mercer University’s wireless network infrastructure has been installed to support the mission of the University. The University must maintain administrative control of the radio frequency spectrum that wireless devices use as their base transport mechanism. Other devices exist that also use the same frequency band and can cause interference on the wireless network. These devices include, but are not limited to, other wireless networking devices, cordless telephones, cameras, keyboards, mice, audio speakers, ad-hoc (peer-to-peer) networks and computers or other devices equipped with a wireless card and software to act as an access point. Information Technology staff will work with the campus community to determine if use of such devices can be accommodated without causing interference to the wireless network.

Wireless network usage is bound by the same policies governing the use of Mercer University’s wired network. Access to Mercer’s wireless network is restricted to currently enrolled students and current employees only. In order to ensure adequate security, all systems and devices intended for use on the University’s wireless network must be registered with the Department of Information Technology. Wireless access points and wireless devices which are not registered will not be allowed access to the network.