NAME:	**Acceptable Use Policy**
ISSUING DEPARTMENT	Campus Technologies
ISSUED DATE:	May, 1997
REVIEWED DATE:	
APPROVING AUTHORITY:	President
DATE REVISED:	August, 2019

DEFINITION

An acceptable use of technology policy defines the capabilities and limitations of the use of information technology resources to ensure that these resources are available to all approved users and that the use of technology complies with state and federal laws.

Information technology resources include, but are not limited to, all PASSHE/University owned or operated hardware, software, computing equipment, systems, networks, programs, personal data assistants, cellular phones, fax, telephone, storage devices, cable television, input/output, connecting devices via either a physical or wireless connection regardless of the ownership of the device connected to the network, and any electronic device issued by the System or Mansfield University.

Mansfield University encourages the responsible use of its information resources. The use of information resources is for Mansfield University academic activities, research, and public service. Access to Mansfield University's information resources is, however, a privilege. All users of the information resources should act responsibly to maintain the integrity of these resources.

PURPOSE

It is the intention of this policy to encourage the responsible use of information resources for all persons or entities who have access to the technological resources of the Pennsylvania State System of Higher Education (PASSHE) and Mansfield University. Nothing herein is intended to contradict or conflict with applicable federal and state laws or regulations.

Furthermore, all users must abide by all existing University codes of conduct, policies and guidelines as well as by local, state, and federal statutes. Mansfield University reserves the right to limit, restrict, or extend privileges and access to its resources.

SCOPE

This policy applies to all Mansfield University faculty, staff, students, contractors and guests who use the University's information resources.

FORMS

No forms are needed in the execution of this policy.

RESPONSIBILITY

The Campus Technologies Division (CT) is responsible for creation, modification, or deletion of this policy.

POLICY

Mansfield University computing and telecommunications resources provided to users for use in their work are the sole property of Mansfield University. These resources are not for personal use or gain.

Computing and telecommunications resources such as computer laboratories and classrooms, wired and wireless networks and software resources are available to all students, faculty and staff for responsible academic use.

The user community is expected to cooperate with the Campus Technologies Division of Mansfield University in its operation of computer systems and information networks, and in the investigation of misuse or abuse of the information resources. Should the security of a computer system or information network be threatened, suspect user files may be examined under the direction of the Chief Information Officer (or his/her designee) of Mansfield University.

While PASSHE and Mansfield University recognize the role of privacy in institutions of higher learning and will endeavor to honor that ideal, there is no expectation of privacy of information stored on or sent through PASSHE/University-owned IT resources, except as required by law. For example, the university may be required to provide information stored in its information technology resources to someone other than a user as a result of a court order, investigatory process, or in response to a request authorized under Pennsylvania's Right-To-Know statute (65 P.S. §67.101 et seq.). Information stored by the University may also be viewed by technical staff working to resolve technical issues, under the direction of the Chief Information Officer (or his/her designee).

These guidelines are subject to the terms and conditions of the various collective bargaining agreements that apply to faculty and staff.

This policy is established in an effort to help users understand what is expected of them. It sets guidelines regarding the issues of privacy and respect for property, ownership of data, system security, and misuse of the system. Each individual who obtains a computer/email account, or uses the computers and network resources made available by Mansfield University, must understand that he or she is accountable for the policies set forth in this document.

A Shared Resource

Computer and network services are available to all faculty, staff, students, contractors and guests of Mansfield University. To ensure access and service for all users, the following guidelines are provided:

The user must:

- Avoid wasting computing or network resources.
- Not use information resources for commercial purposes

- Use email responsibly to avoid congestion of the network. Do not send excessive email/attachments or messages locally or over the network such as chain letters, advertisements, or solicitations.

- Not engage in any act that may seriously impact the operation of computers, terminals, peripherals, or networks in a negative manner. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, blocking communication lines, or interfering with the operational readiness of a computer. Examples of such acts include, but are not limited to, the creation of unsanctioned personal web or ftp sites, the delivery of unauthorized streaming audio or video, high bandwidth gaming, or high bandwidth video conferencing without prior written approval from the Chief Information Officer (or his/her designee).

- Not operate a server on any Mansfield University network without prior written approval from the Chief Information Officer (or his/her designee). Examples of servers include, but are not limited to, WWW, FTP, SMTP, POP, NTTP, DNS, DHCP, TELNET, IRC, and bandwidth intensive media sharing programs or protocols (Kazaa, BitTorrent, etc.).

- Not host or operate a wireless network access point. The use of any type of wireless network equipment including, but not limited to, wireless switches and wireless routers on the university network is prohibited without prior written approval from the Chief Information Officer (or his/her designee).

Privacy
Technology should not be used in a manner that infringes upon an individual's expectation of privacy. The following restrictions are imposed to protect the privacy of our users.

Users are prohibited from:

- Gaining or attempting to gain unauthorized access to information or resources that are private or protected.

- Running programs that attempt to identify passwords, weaknesses in the university system, or other security codes.

- Circumventing or attempting to circumvent data protection schemes or exploiting security loopholes. Users should immediately report any breeches of system security to Campus Technologies. Do **NOT** demonstrate your ability to breech system security to anyone other than Campus Technologies personnel.

- Using another person's password or allowing others to use yours.

- Attempting to monitor another user's data communications or network traffic, except as necessary by Campus Technologies when properly authorized.

User Responsibilities:

- Respect for the rights of others is imperative. Civil discussion is at the heart of a university community and based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, bear in mind that it is the user's responsibility to do so in a way that actually advances the cause of learning and mutual understanding.

- The following type of information or software cannot be placed on any University-owned computer system or network:

    - That which infringes upon the rights of another person

    - That which may injure someone else and/or lead to a lawsuit or criminal charges; this includes, but is not limited to, pirated software, copyrighted software or media that the user is not entitled to distribute, destructive software, pornographic materials, or libelous statements.

    - Users must not run or install on any of the computer systems, or give to another, a program that could reproduce itself or result in the eventual damage to a file, computer system, or network. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.

    - Users must not mask or attempt to mask the identity of the account or computer that they are using. For example, pointing a non mansfield.edu domain name at a host within Mansfield University's address space.

    - Users are responsible for the security of their passwords. This includes changing passwords on a regular basis and properly securing them.

Users are expected to:

- Check email often and delete unnecessary messages from the server immediately. If email is not attended to regularly, the system administrator reserves the right to remove messages to maintain system integrity.

- Report unauthorized use of his/her account.

- Frequently make backup copies of his/her work and store them securely to ensure against loss.

- Be sensitive to the public nature of the shared computing facilities and take care to refrain from transmitting to others in any location inappropriate images, sounds, or messages which might reasonably be considered harassing, threatening, defamatory, or fraudulent.

- Clearly label works and opinions as his/her own before they are widely distributed.

- Abide by the terms of all software licensing agreements and copyright laws.

Privately owned computers
Faculty, staff, students, contractors and guests of Mansfield University who provide their own computer and equipment but connect to the University's network must still abide by all aspects of the Acceptable Use Policy. In addition, there are several special areas for these users to keep in mind:

Domain names: A non mansfield.edu domain name may not point at a host within Mansfield University's address space, unless that domain is being used by a recognized university organization, and is approved by the Campus Technologies Division. Mansfield University's address space consists of all IP addresses starting with 157.62. Users connecting to Mansfield University's network are assigned an IP within our address space for their academic use. Users may not alternately register their IP address with any name other than Mansfield University's official registered names. For example, user XYZ, given IP address 157.62.99.99, may not identify that IP as xyz.com or funtimes.net, etc.

Responsibility for content: The content of any files or services made available to others over the network is the sole responsibility of the person with ownership of and/or administrative authority over the computer providing the service. It is this person's responsibility to be aware of all applicable federal and state laws, as well as university and PASSHE policies and guidelines. This person will be liable for any violations of these laws and policies.

Network-intensive applications: Any person operating a network-intensive application or a defective computer, which causes network overload, will be notified and steps will be taken to protect other users and the university network overall. This may include disconnecting the offending computer system from the network until the problem is resolved. If the condition is an imminent hazard to the university network or disrupts the activities of others, then the offending computer system or the subnet to which it is attached may be disabled without notice. This latter course of action may affect other users connected to the network.

Responsibility for security: Any person attaching a computer to Mansfield University's network is responsible for the security of the computer system and for any intentional or unintentional activities from or to those network connections.

Wireless Equipment: The use of any type of wireless network equipment including but not limited to wireless switches, wireless printers, wireless routers and gaming systems on the university network is prohibited without prior written approval from the Chief Information Officer (or his/her designee). Only wireless access points installed and managed by Mansfield University Campus Technologies division will be allowed in use

on the university's network. Campus Technologies will maintain a current list of wireless access points available on the network.

Ethernet Network: Network services and wiring may not be modified or extended by users for any reason. This applies to all network wiring, hardware, and data jacks. Ethernet switching equipment and hubs other than those provided by the university are prohibited for use on any Mansfield University network without prior written approval from the Chief Information Officer (or his/her designee).

Authority
Violations of this policy can result in loss of access to Mansfield University's information resources and adjudication through Mansfield University's judicial or discipline processes, which may result in discipline up to and including termination of employment or suspension/expulsion from the University. Offenders may also be subject to prosecution under local, state, or federal law. It is the user's responsibility to be aware of all applicable federal and state laws, as well as university policies, including the University's Copyright Policy

Examples of illegal acts include, but are not limited to: (i) accessing, altering, or damaging any computer system, network, software or data base, or any part thereof, with the intent to interrupt the normal functioning of an organization; (ii) disclosing a password to a computer system or network, knowingly and without authorization; and (iii) the intentional and unauthorized access to a computer, interference with the operation of a computer network, or modification of computer software.

The Campus Technologies Division of Mansfield University may access other's files for the maintenance of networks, computers, and storage systems. In all cases, the individual's expectation of privacy will be respected to the greatest degree possible. Campus Technologies has the responsibility to protect the rights of users as well as protecting the integrity of our information resources. Campus Technologies reserves the right to limit or refuse access in the event of a safety/security issue. In this regard, Campus Technologies will make a reasonable effort to notify users affected by any such decisions. If offenses are serious enough to warrant disciplinary action, they shall be referred to the appropriate office of the University.

DISTRIBUTION
This policy will be distributed through the web and maintained by the staff of Campus Technologies.