910 Information Technology Resources

Approved by President

______________________________
Sidney A. McPhee, President

Effective Date: _____________, 2019

Responsible Division: Information Technology
Responsible Office: Information Technology
Responsible Officer: Vice President for Information Technology

I. Purpose

This policy identifies appropriate use of the information technology resources to support Middle Tennessee State University’s (MTSU or University) goals and objectives and informs all users of the policies set forth by MTSU, the laws of the State of Tennessee, and the federal government.

II. Objective

The objective of this policy is to ensure that the use of information technology resources is related to, or for the benefit of, MTSU and the State of Tennessee. The use of information technology resources is a privilege that imposes certain responsibilities and obligations on users and is subject to policy and applicable law. Acceptable use must be legal, ethical, reflect honesty, and show restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, the individual’s rights to privacy, and freedom from intimidation, harassment, and unwarranted annoyance.

III. Definitions

A. Information Technology Resources. Computing systems, networks, electronic storage, communication, and presentation resources provided by MTSU.

B. Infrastructure Sponsor. Person responsible for the MTSU information technology resources infrastructure. The infrastructure sponsor is the Vice President for Information Technology and Chief Information Officer (CIO). The infrastructure sponsor is authorized to determine which information technology resources will be acquired and utilized by the University.
C. System Sponsor. The individual(s) under whose authority a computing system, local network, or external network connection is funded. Individual computer systems and local networks may be sponsored by faculty members (i.e., using research grant funds), departments, colleges, or other units. In the latter case, the unit administrator is the system sponsor.

D. System Manager. The person(s) authorized by a system sponsor to grant, restrict, or deny user privileges, maintain the system files, inform users of all applicable policies, and generally ensure the effective operation of a system. In some cases, the system manager and the system sponsor may be the same individual(s).

E. Facility Staff. Individuals who are authorized to monitor, manage, or otherwise grant temporary access to computing facilities (such as microcomputer laboratories) in which one (1) or more systems are used by either specific populations of faculty, staff, and students, or the entire campus community.

F. User. Any individual who uses, logs in, attempts to use, or attempts to log in to a system (whether by direct connection or across one or more networks) or who attempts to connect to, or traverse, a network, whether via hardware, software, or both.

G. Account. A combination of username and password that provides an individual with access to an information technology resource.

H. Content. Any and all text, images, multimedia elements, coding, and other such items posted, transmitted, and/or used by information technology resources.

IV. Scope

MTSU maintains records to carry out its educational mission. Federal and state laws and regulations govern access to these records. This policy and related procedures are established to ensure compliance with these laws and regulations and to protect the integrity of University records and the privacy of individuals as it relates to usage of information technology resources. This policy applies to all individuals granted access to MTSU information technology assets.

V. Respect and Obligations

This policy is intended to provide a framework for users to practice respectful use of information technology resources. Failure to act responsibly can adversely affect the work of other users. The policy is intended to prevent abuse of resources and to ensure that usage honors the public trust and supports the University’s mission.

VI. Who May Request Accounts

The following persons may request an account at MTSU:
A. Any person needing access may request an account from the appropriate system sponsor. The Information Technology Department (ITD) will work with the appropriate system sponsor to determine if, and what type of access, the account will be granted.

B. Other persons may qualify for public service accounts on a particular system at the discretion of the Vice President for Information Technology and CIO.

VII. System Sponsors and Applicable Policy

A. The information technology resources at MTSU serve a diverse population. System sponsors are given discretion to establish reasonable and appropriate requirements applicable to the systems they oversee. For example, on some campus systems, playing of computer games or use of chat programs may be permitted or even encouraged. On other systems, game-playing and chatting may be discouraged or even prohibited.

B. System sponsors, and by the delegation, system managers, and facility staff, have discretion to set and revise reasonable usage priorities and operational policies (such as hours of operation, usage time limits, populations to be served, etc.). They may also take such routine steps (i.e., troubleshooting, updating systems, backing up systems, etc.) as may be reasonably necessary for the operation of their systems or facilities.

VIII. Cyber-Citizenship

A. Responsibility

1. Use of MTSU information technology resources must comply with MTSU policies, procedures, standards, and all applicable laws and not be used for any personal for-profit, or any unauthorized not-for-profit, purpose.

2. Users must expect variation in what constitutes acceptable use from system to system on campus and must make reasonable efforts to inform themselves about the particular requirements applicable to each system they use. In cases of doubt, it is the responsibility of the user to inquire concerning the permissibility of an action or use, prior to execution.

3. Users should protect systems from misuse and attack by being up to date on security patch installations, maintain the latest version of ITD approved antivirus pattern/definitions, and running only necessary services.

B. Privacy and Privilege

1. Users must respect the privacy and usage privileges of others, both on the MTSU campus and at all sites reachable via MTSU’s external network connections.
2. Users will not intentionally seek information on passwords. Unauthorized users will not modify files, data, or passwords belonging to other users. Users will not develop or retain programs for these purposes.

3. Users will preserve and protect the privacy, dignity, well-being, and informed consent of all participants.

C. System Integrity

1. Users must respect the integrity of computing systems and networks, both on the MTSU campus and at all sites reachable via MTSU’s external network connections.

2. Users will not by any means attempt to gain access to a computing system or network without proper authorization, either on the MTSU campus or elsewhere.

3. Users will not attempt to damage or alter hardware or software components of a computing system or network, either on the MTSU campus or elsewhere.

4. Users will not attempt to disable any hardware or software components of a computing system or network via network attacks and/or scans, either on the MTSU campus or elsewhere.

D. Resource Management

1. To effectively manage information technology resources, priority is given to applications that support the University mission. The system sponsor has the responsibility to manage resources so as to make them available for mission related applications.

2. Users are expected to comply fully with the instructions of facility staff, system managers, system sponsors, and the infrastructure sponsor. In particular, users will vacate facility workstations and will surrender other resources promptly when asked to do so.

IX. Examples of What Users are Not Permitted to do with MTSU Information Technology Resources (Not an Inclusive List)

A. Violate laws or policies. For example:

1. Use information technology resources in a manner that violates MTSU policy and/or other applicable policy and laws. Users will comply with state and federal regulations concerning obscenity and child pornography, state prohibitions on gambling, and restrictions on gaming.
2. Transfer or use copyrighted materials without the explicit consent of the owner.
   
a. The unauthorized downloading, copying, or distribution of materials (i.e., proprietary music, video, software, or database information) via information technology resources is prohibited.

b. Student Users should be aware that course instructors have primary responsibility for the maintenance of academic integrity. Cases involving academic dishonesty (i.e., plagiarism, cheating, etc. and/or facilitating such an act) should be reported to the Coordinator for Academic Misconduct.

B. Commit offenses against others. For example:

   1. Harass another using information technology resources.
   2. Impersonate another.
   3. Take or alter another’s work without permission.
   4. Assume credit for the work of another.
   5. Interfere in another’s legitimate use of information technology resources.
   6. Display obscene material in a public area. Note: Any direct attachment, linkage, or anchoring of such materials to documents viewable by the public is prohibited.

C. Abuse information technology resources. For example:

   1. Attempt to gain another user’s password or to log on as another user.

   2. Permit unsupervised use of an assigned account by any other person.

      a. Use information technology resources for commercial activities except as authorized by the appropriate University administrative official or unauthorized not-for-profit business activities.

      b. Use MTSU web pages for commercial, private, or personal for-profit activities. Examples include the use of web pages advertising services for personal marketing or business transactions, private advertising of products or services, and any activity meant to foster personal gain.

      c. Use commercial logos/icons unless that owner provides a University service, such as dining services. Those pages must contain a notice that the owner provides the service under contract to the University.

      d. Use MTSU web pages for unauthorized not-for-profit business activities. This includes the conducting of any non-University related fundraising or public relations activities, such as solicitation for religious or political causes.
3. Use information technology resources in support of agencies or groups outside the University when such use is not in compliance with the mission of the University.

4. Use information technology resources for activities unrelated to the mission of the University when such use prevents or seriously restricts resource usage by persons fulfilling the mission.

5. Use information technology resources to give access to persons who have not and/or could not obtain access to University resources through official MTSU channels.

6. Use any access not specifically assigned to the user.

7. Deliberately alter the account structure assigned to the user so as to increase system permissions without ITD authorization.

8. Attempt to render the system or equipment inoperative.

9. Participate in activities that have the intent of monopolizing information technology resources.

10. Install wireless network transmitters/routers without ITD authorization.

X. Digital Content Provisions

A. Default Access

The default access to information technology resources (such as files) is to be set to allow the owner read, write, delete, and execute access and to give access to no other person. If the owner of such resources modifies this access to grant others access, such access by another, in itself, is not considered an ethical infraction. However, it is prohibited to use such access to copy another’s work and assume credit for it, modify the file of another without explicit verbal or written permission to do so, and/or publicizing its contents without authorization or by modifying the file’s contents in a manner unauthorized by the file’s owner.

B. Software

1. MTSU utilizes a wide variety of software, with an equally wide range of license and copyright provisions. Users are responsible for informing themselves of, and complying with, the license and copyright provisions of the software that they use.
2. No software copy is to be made by any user without a prior, good faith determination that such copying is in fact permissible. All users must respect the legal protection provided by copyright and license to programs and data.


C. Content

1. With regard to intellectual property, MTSU reserves the right to protect copyrights, patents, trademarks, trade secrets, and other rights obtained legally that prohibit copying, trading, displaying, or using without permission. Many of these items may be found by searching networks including the internet, but their presence on these networks does not imply that they are free to use without permission.

2. All content must comply with copyright laws, policies, and regulations detailed in the Federal Copyright Law (Title 17 of the United States Code), and Digital Millennium Copyright Act (DMCA), the Technology, Education and Copyright Harmonization (TEACH) Act, the Ethics Guidelines for Faculty in the MTSU Faculty Handbook, and Policy 540 Student Conduct.

3. Logos

   a. The use of the MTSU logo is acceptable on University hosted web pages.

   b. Authorization to use the MTSU Blue Raider logo is granted only by the MTSU Athletic Department.

XI. Privilege

Access to MTSU information technology resources is granted contingent on that access not being misused. If that access is misused, it can be withdrawn at any time. Further disciplinary action may be taken as a result of serious offenses.

Rights to Privacy

A. Privacy of information is the subject of Policy 121 Privacy of Information that gives considerable guidance on privacy. Other laws, policies, and regulations from MTSU, the State of Tennessee, and the federal government address privacy issues also.

B. While MTSU recognizes the role of privacy in an institution of higher learning and every attempt will be made to honor that principle, there should be no expectation of privacy in any message, file, image or data created, stored, sent, retrieved, or received by use of MTSU information technology resources. MTSU expects all users to obey all applicable policies and laws in the use of information technology resources.
C. Pursuant to state public records law, T.C.A. § 10-7-503, and Policy 120 Public Records – Inspecting and Copying, and subject to the exemptions contained therein, electronic files (including email correspondence) which are maintained using MTSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.

D. The University abides by the Family Educational Rights and Privacy Act, or FERPA, which requires the University to protect the confidentiality of student education records.

E. When sources outside the University request an inspection and/or examination of any University owned or operated information technology resource, and/or files or information contained therein, the University will review the request pursuant to state law and institutional policy, and will release the information when any one or more of the following conditions exist:

1. When approved by the appropriate University official(s) or the head of the department to which the request is directed;

2. When authorized by the owner(s) of the information;

3. When required by federal, state, or local law; or,

4. When required by a valid subpoena or court order.

Note: When notice is required by law, court order, or subpoena, computer users will receive notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure). In all cases, a request for access to any University information resource by non-MTSU entities will be reviewed by the Office of the University Counsel prior to release.

F. Data on University computing systems may be copied to backup media periodically. The University makes reasonable efforts to maintain the confidentiality of the data contained in the backup.

G. The contents of a user’s files will typically not be accessed or disclosed except when (1) the owner has set the file permissions to grant others access in accordance with the restrictions noted in this policy, or (2) in the event of any situation listed below.

1. The system sponsor in charge of a system may require personnel to investigate the system suspected of being used by someone other than its rightful owner.

2. The system sponsor in charge of a system may require personnel to investigate the system suspected of being used in a manner that violates University policy or federal, state, or local law.
3. Information traversing the data networks may be intercepted and/or analyzed in conjunction with investigations.

XII. Violation of this Policy

Violation of this policy may result in one or more of the following:

A. Immediate suspension of any or all of the following: the user’s account, network access, and internet access followed by timely review of the charges by the appropriate person or persons.

B. The user’s computing privileges at MTSU may be permanently and totally removed. There will be no refund of any technology access fees.

C. Use of the regular disciplinary processes and procedures of the University for students, staff, administrators, and faculty.

D. Faculty, staff, and students may be recommended for termination from MTSU employment.

E. Referral to appropriate law enforcement agencies in the case of suspected law violations for criminal and/or civil action.

XIII. Related Acceptable Use Policies

Policy 121 Privacy of Information

Forms: none.

Revisions: June 5, 2017 (original); ____, 2019.

Last Reviewed: __________, 2019.

References: Federal Copyright Law, Title 17 of the U.S. Code; Digital Millennium Copyright Act; Technology, Education and Copyright Harmonization Act; Ethics Guidelines for Faculty in the MTSU Faculty Handbook; T.C.A. § 10-7-503; Family Educational Rights and Privacy Act; Policies 120 Public Records-Inspection-Copying Public Records; 121 Privacy of Information; 140 Intellectual Property; 540 Student Conduct; 950 Computer Software.