EAST TENNESSEE STATE UNIVERSITY

ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES	
Responsible Official: **CHIEF INFORMATION OFFICER**	Responsible Office: **INFORMATION TECHNOLOGY SERVICES**

Policy Purpose

This policy describes the acceptable use of information technology resources and facilities at East Tennessee State University (ETSU or University).

Policy Statement

This policy provides a framework for the appropriate and respectful use of information technology resources. Failure to act responsibly can adversely impact the University. The policy is intended to prevent abuse of resources and to ensure that usage honors the public trust and supports the University's mission.

This policy applies to employees, students, guests, and third parties using, accessing, or integrating with ETSU technological resources, i.e., computing, accounts, and network systems. For example, this policy applies to individuals using ETSU computing devices, or individuals using personal devices connected to the ETSU network or other ETSU resources.

I. SYSTEM SPONSORS AND OPERATIONAL POLICIES.

A. The information technology resources at ETSU 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 information technology 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.

II. CYBER-CITIZENSHIP

A. Responsibility

1. Use of ETSU information technology resources must comply with ETSU policies, procedures, standards, and all applicable laws and not be used for any personal, for-profit, or 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 and maintain the latest version of ITS approved antivirus patterns and definitions.

B. 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 ITS 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.

III. UNIVERSITY RIGHTS

ETSU reserves the right to access, monitor, review, and release the contents and activity of an individual User's account(s) as well as that of personal Internet account(s) used for University business. The University reserves the right to access any University owned resources and any non-University owned resources on University property, connected to University networks and systems, or containing University data. This action may be taken to maintain the network's integrity and the rights of other authorized Users and to protect the infrastructure from spam, viruses, intrusions, malware, and other malicious content. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of University resources is suspected, or the University has a legitimate business need to review activity or data.

IV. PRIVACY

A. ETSU Privacy Notification

1. ETSU hereby notifies users that email communication and documents stored or transmitted using ETSU resources may be a public record and open to public inspection under the Tennessee Open Records Act. Therefore, pursuant to the Tennessee Public Records Act (T.C.A. § 10-7-501 et seq.), and subject to exemptions contained therein, all records generated or received by ETSU employees, all records owned or controlled by the State, or all records maintained using ETSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.
2. Users should have no expectation of privacy when using ETSU computing resources, computer accounts, and network resources.
3. The university does not routinely or without cause monitor individual use of these resources; however, the normal operation and maintenance of these resources require the backup and caching of data and communications, logging of activity, monitoring of general usage patterns, and other such activities.
4. Users should be aware that any activity on systems and networks, including documents created, stored, transmitted, or received on university computers and networks may be monitored, logged, and reviewed by university approved personnel or may be discovered in legal proceedings.
5. Users must respect the privacy and usage privileges of others, both on the ETSU campus and at all sites reachable via ETSU's external network connections.
6. 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.
7. Users will preserve and protect the privacy, dignity, well-being, and informed consent of all users of information technology systems.

V. SYSTEM SECURITY

A. Users must respect the integrity of computing systems and networks, both on the ETSU campus and at all sites reachable via ETSU's external network connections.
B. Users will not by any means attempt to gain access to a computing system or network without proper authorization, either on the ETSU campus or elsewhere.
C. Users will not attempt to damage or alter hardware or software components of a computing system or network, either on the ETSU campus or elsewhere.
D. 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 ETSU campus or elsewhere.
E. Users will use only supported and patched applications and operating systems on University-owned devices. Exceptions must be documented and approved by the Chief Information Officer or designee.

VI. ACCOUNT SECURITY

A. Users must protect the confidentiality of their assigned account credentials by not sharing passwords, PINs, tokens, or other authentication information with anyone, including friends, supervisors, ITS employees, or other employees.
B. Users must use only the accounts, passwords, and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose.
C. Users must report unauthorized account activity or suspected account compromises to the ITS Help Desk and change passwords immediately.
D. Users shall log out from computers, web pages, and other systems when they are not being actively used and not leave active sessions unattended.

VII. COPYRIGHTS AND LICENSES

A. Violation of copyright law or infringement is prohibited by University policy and state and federal law.
B. Software may not be copied, installed, or used on University resources except as permitted by the owner of the software and by law.
C. Users will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license.
D. All copyrighted information, such as text and images, retrieved from University resources or stored, transmitted, accessed, or maintained with University resources must be used in compliance with applicable University branding, copyright, and other laws.

VIII. USER RESPONSIBILITIES.

Access and use of ETSU IT resources are limited to purposes that are consistent with the instructional, research, and administrative goals and mission of the University. Users SHALL:

A. Respect and honor the rights of other individuals with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of University resources;
B. Use University provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license;
C. Only use University resources for which they have authorization;
D. Control and secure physical and network access to University resources; and
E. Comply with state and federal regulations concerning obscenity and child pornography, state prohibitions on gambling, and restrictions on gaming.

Users shall NOT:

A. Use information technology resources in a manner that violates ETSU policy and/or other applicable policy and laws;
B. Use accounts, access codes, privileges or ITS resources for which they are not authorized or obtain extra University resources or gain access to accounts for which they are not authorized;
C. 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;
D. 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;
E. Use information technology resources to give access to persons who have not and/or could not obtain access to University resources through official ETSU channels;
F. Use any access not specifically assigned to the user;
G. Tamper, modify, or alter any restrictions or protections placed on their accounts, the University's system, or network facilities;
H. Physically damage or vandalize University resources;
I. Deliberately alter the account structure assigned to the user so as to increase system permissions without ITS authorization;
J. Attempt to render the system or equipment inoperative;
K. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any University resources;
L. Participate in activities that have the intent of monopolizing information technology resources;
M. Connect network devices such as switches, routers, hubs, and wireless access points to the network without prior approval from ITS;
N. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious content;
O. Intercept other Users' transmissions;
P. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering;
Q. Send email chain letters or mass mailings for purposes other than official University business;
R. Use University resources as an email relay between non-university email systems (routing email through university email systems between two non-university systems);
S. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth;
T. Include or request Sensitive Information be included in unprotected electronic communication (email, instant message, text message, etc.);
U. Transfer or use copyrighted materials without the explicit consent of the owner. The unauthorized downloading, copying, or distribution of materials (i.e., proprietary music, video, software, or database information) via information technology resources is

prohibited;

V. Commit offenses against others including but not limited to:

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; or

W. Abuse information technology resources including but not limited to:

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.
3. Use information technology resources for commercial activities except as authorized by the appropriate University administrative official or unauthorized not-for-profit business activities.
4. Use ETSU 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.
5. 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.
6. Use ETSU 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.

University employees, contractors, temporary employees, student workers, external parties, and others accessing sensitive systems and data shall NOT:

A. Access websites which are not directly related to the conduct of University business while accessing any University system containing sensitive/protected data.
B. Install or use online chat applications, computer games, peer-to-peer file sharing software or other software which is not directly related to the conduct of University business.
C. Transmit, upload, download, or email, sensitive University data to non-University or unapproved systems.

IX. 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 – ETSU 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. 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 – Regarding intellectual property, ETSU reserves the right to protect copyrights, patents, trademarks, trade secrets, and other legally obtained rights 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. 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, and the Education and Copyright Harmonization (TEACH) Act.

D. Logos – The use of the ETSU logo is acceptable on University hosted web pages.

X. PRIVILEGE

Access to ETSU 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.

XI. RIGHTS TO PRIVACY

A. While ETSU 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 ETSU information technology resources. ETSU expects all users to obey all applicable policies and laws in the use of information technology resources.

B. Pursuant to state public records law, T.C.A. § 10-7-503 and subject to the exemptions contained therein, electronic files (including email correspondence) which are maintained using ETSU resources may be subject to public inspection upon request by a citizen of the State of Tennessee.

C. The University abides by the Family Educational Rights and Privacy Act (FERPA), which requires

the University to protect the confidentiality of student education records.

D. 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-ETSU entities will be reviewed by the Office of University Counsel prior to release.

E. 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.

F. 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

Violations 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. Revocation of the user's computing privileges at ETSU. There will be no refund of any technology access fees.

C. Recommendation users go through the regular disciplinary processes and procedures of the University for the appropriate student, staff, administrator, and faculty category.

D. Recommendation of termination of employment from ETSU for faculty, staff, and

students.

E. Recommendation the violation be turned over to appropriate law enforcement agencies in the case of suspected law violations for criminal and/or civil action.

Authority: The Focus Act § 49-8-203 et. seq; Federal Copyright Law, Title 17 of the U.S. Code; Digital Millennium Copyright Act; Technology, Education and Copyright Harmonization Act; T.C.A. § 10-7-501 et seq; Family Educational Rights and Privacy Act

Previous Policy:

Defined Terms

A defined term has a special meaning within the context of this policy.

ACCOUNT	A combination of username and password that provides an individual with access to an information technology resource.
CONTENT	Any and all text, images, multimedia elements, coding, and other such items posted, transmitted, and/or used by information technology resources.
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.
INFRASTRUCTURE SPONSOR	Person responsible for the ETSU information technology resources infrastructure and who is authorized to determine which information technology resources will be acquired and utilized by the University. (Chief Information Officer (CIO)
INFORMATION TECHNOLOGY RESOURCES	Computing systems, networks, electronic storage, communication, and presentation resources provided by ETSU

SENSITIVE UNIVERSITY DATA	Any information that is protected against disclosure, including all data that may contain personal information, protected health information, student education records, customer record information, card holder data, or other confidential information.
SENSITIVE UNIVERSITY SYSTEMS	Any University owned electronic systems that contain Sensitive University Data.
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).
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.

Policy History

Effective Date

Initial: 06/12/23

Revised:

Procedure

N/A

Procedure History

Effective Date

Initial: 06/12/23

Revised:

Related Form(s)

Scope and Applicability

Primary:

Secondary: