Information Technology Resources	
Responsible Official:	Responsible Office:

Policy Purpose

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

Policy Statement

I. Applicability

This policy applies to employees, students, guests, and third parties using or accessing 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.

II. University Rights

The University 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.

III. 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 Open Record Act, Title 10, Chapter 7, 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 participants.

IV. System Security

8. 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.
9. 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.
10. 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.
11. 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.
12. 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.

V. Account Security

13. 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.
14. User must use only the accounts, passwords and privileges associated with their computer account(s) and use those account(s) only for their authorized purpose;
15. Users must report unauthorized account activity or suspected account compromises to the university helpdesk and change passwords immediately.
16. User shall log out from computers, web pages, and other system when they are not being actively used and not leave active sessions unattended.

VI. Copyrights and Licenses

17. Violation of copyright law or infringement is prohibited by University policy and state and federal law;
18. Software may not be copied, installed, or used on University resources except as permitted by the owner of the software and by law;
19. 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;
20. 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;

VII. User Responsibilities. (*This is not an inclusive list)*

User shall:

21. 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.
22. 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.
23. Only use University resources for which they have authorization.
24. Control and secure physical and network access to University resources.

Users shall NOT:

25. Use information technology resources in a manner that violates ETSU 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.
26. Use accounts, access codes, privileges or IT resources for which they are not authorized or obtain extra University resources or gain access to accounts for which they are not authorized.
27. 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.
28. 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.
29. 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.
30. Use any access not specifically assigned to the user.
31. Tamper, modify, or alter any restrictions or protections placed on their accounts, the University's system, or network facilities.
32. Physically damage or vandalize University resources.
33. Deliberately alter the account structure assigned to the user so as to increase system permissions without ITS authorization.
34. Attempt to render the system or equipment inoperative.
35. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any University resources.
36. Participate in activities that have the intent of monopolizing information technology resources.
37. Connect devices network devices such as switches, routers, hubs, and wireless access points) to the network without prior approval from ITS.

38. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan horses, or other malicious content.
39. Intercept other Users' transmissions;
40. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering;
41. Send email chain letters or mass mailings for purposes other than official University business;
42. Use University resources as an email relay between non-university email systems (routing email through university email systems between two non-university systems).
43. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth.
44. Include or request Sensitive Information be included in unprotected electronic communication (email, instant message, text message, etc.).
45. 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.
46. Commit offenses against others. For example:
    a. Harass another using information technology resources.
    b. Impersonate another.
    c. Take or alter another's work without permission.
    d. Assume credit for the work of another.
    e. Interfere in another's legitimate use of information technology resources.
    f. 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.
47. Abuse information technology resources. For example:
    a. Attempt to gain another user's password or to log on as another user.
    b. Permit unsupervised use of an assigned account by any other person.
    c. Use information technology resources for commercial activities except as authorized by the appropriate University administrative official or unauthorized not-for-profit business activities.
    d. 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.
    e. 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.
    f. 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.

<u>Employees shall NOT:</u>

The following additional requirements apply to University employees, contractors, temporary employees, student workers, external parties, and others accessing sensitive systems and data:

48. Access websites which are not directly related to the conduct of University business while accessing sensitive University system.
49. Install 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.
50. Install personal online storage applications, such as OneDrive, Google Drive, or storing University data on online storage.
    Note: This requirement does not apply to students and faculty using online storage for academic purposes only, i.e. teaching the use of online storage, or sharing class/educational material not containing sensitive/protected information
    Copy or store sensitive University data on personal storage, personal computing devices, mobile devices, or any other unapproved media.
51. Transmit, upload, download, or email, sensitive University data to non-University or unapproved systems.

VIII. 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. 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.

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, ETSU 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, and the Education and Copyright Harmonization (TEACH) Act.

3. Logos

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

IX. 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.

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, or 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 the 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.

X. 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 ETSU 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 ETSU employment.

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

Authority: Federal Copyright Law, Title 17 of the U.S. Code; Digital Millennium Copyright Act; Technology, Education and Copyright Harmonization Act; T.C.A. § 10-7-503; Family Educational Rights and Privacy Act

Definitions

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

B. Infrastructure Sponsor. Person responsible for the ETSU information technology resources infrastructure. The infrastructure sponsor is the 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.

Policy History

Effective Date: May 13, 2019
Revision Date:

Procedure (s)

Procedure History

Effective Date: May 13, 2019
Revision Date:

Related Form(s)

Scope and Applicability

Check those that apply to this policy and identify proposed sub-category.

	Governance	
	Academic	
	Students	
	Employment	
	Information Technology	
	Health and Safety	
	Business and Finance	
	Facilities and Operations	
	Advancement	

Policy and Procedure Differences

Policy	Procedure
Provides a guiding principle or rule for best practice; sets standard for functions of the university	Provides a consistent approach, sequential tasks or steps, for implementation of policy
Provides the rationale or why	Describes how, when, who, and what one needs to do
May be stated in general, broad terms	May be stated in specific, detailed terms
Frequent revision is unnecessary	Prone to change; continuous improvement
Final approval by Board of Trustees	Final approval by University staff

Policy Purpose: why there is a policy and desired effect or outcome; generally, 1-2 sentences.

Policy Statement: indicates specific regulations, requirements, or behavior; may express university culture, goals, or philosophy

Procedure: to define, describe, identify, provide, outline, establish

Definition of terms: to assist in understanding or interpreting policy; listed in alphabetical order.

Scope: who the policy affects