TERRA STATE COMMUNITY COLLEGE

ACCEPTABLE USE POLICY

Division: Information Technology

Policy Statement

This policy provides specific requirements for the use of computing and network resources at Terra State Community College. All college computing resources are provided for the exclusive use of Terra students, staff, and other users authorized by the college and staff. College computing resources include all college-owned or managed hardware, software, network resources, data, information, email, and college assigned user accounts, and use of the college network via wired, wireless, or remote connections regardless of the ownership of the device connected to the network.

It is the responsibility of every computer user to know and understand this policy and conduct their activities accordingly. All users consent to this policy by logging onto, or utilizing any Terra State Community College computing resources. All users must read, acknowledge and accept an "acceptable use" statement if presented onscreen when accessing college computing resources.

Policy Details

All users covered by this policy must adhere to the following acceptable use guidelines:

1. Utilize computing resources for purposes authorized by the college according to individual job descriptions or as directed by supervisors or the leadership of the college.
2. Only access computing resources for which they have been granted authorized access.
3. Be considerate of others when utilizing shared computing resources and refrain from overloading networks with excessive data, degrading services, or wasting printer paper and toner, disk space, or other shared resources.
4. Only utilize legal versions of copyrighted software in accordance with vendor licensing requirements.
5. Protect sensitive and confidential information in accordance with applicable Federal laws, including but not limited to FERPA, State, and Local laws.
6. Protect all authentication and authorization mechanisms from unauthorized use, including, but not limited to, user ids, passwords, and digital signatures.
7. Immediately update passwords when there is a suspected compromise of those credentials.
8. Report any suspected or identified security incidents immediately to the Information Technology Help Desk at 419-559-2309.
9. Report any theft or vandalism of college computing resources immediately to the Information Technology Help Desk.
10. Ensure that any personal devices connected to the college network is running a supported and updated operating system, and is also running current and updated malware protection software.
11. Be cognizant of phishing techniques and carefully examine all emails before responding to requests or opening attachments, particularly when the email is unexpected.
    - When unsure of an email's validity, contact the IT help desk for guidance.
    - When an email is suspicious use the Spam Reporting tool with the email client to report the suspect email to the IT help desk.
12. Report any issues with computing resources immediately to the IT help desk.
    - In particular, users need to be aware of a slow, or otherwise poorly performing, computer and report it immediately as this could be a symptom of malware infecting the device.
13. Be responsible for the content of their electronic communications, including but not limited to emails and instant messaging, and may be subject to personal liability as a result of that use.

The following activities and/or uses of computing resources are prohibited and will not be tolerated by the college in any form. This list of prohibited activities below is by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing TSCC resources.

1. Accessing, downloading, storing, transmitting, sharing or otherwise making use of violent, pornographic, obscene, lewd, or otherwise offensive materials of any kind over the network or internet.
2. Engaging in any form of harassment or intimidation activity over the network or internet.
3. Accessing, downloading, storing, transmitting, sharing or otherwise making use of "hate-group" or other materials of any kind that may cause discomfort to any racial or ethnic group.
4. Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
5. Engage in activities that cause an invasion of privacy.
6. Engage in acts of terrorism, cybercrime, extortion, or identity theft.
7. Illegal duplication or transmission of copyrighted or otherwise protected software.
8. Knowingly download or install any software which have not been approved by the Information Technology Department.
9. Destruction or theft of computer hardware, software, files or data.
10. Attempting to gain access or use another person's system, files, or data without permission.
11. Sharing or otherwise revealing your log in credentials or other authentication and authorization means to any other individual.
12. Attempting to circumvent or subvert any system or network security measures, or assisting others in such actions.
13. Executing any form of network monitoring to intercept data unless as part of the employee's normal job or duties.
14. Engaging in any activity that is intended to harm systems or stored information including creating or propagating malware, disruption of services, inflicting damage to files, port scanning, or any other unauthorized modifications to college data and systems.
15. Using the college's systems for any commercial purposes not authorized by the college.
16. Violation of any applicable laws, regulations or college policies and procedures governing the use of IT resources.
17. Using the college's computing resources to transmit commercial or personal solicitations or advertisements unrelated to college business.
18. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
19. Creating or forwarding "chain letters" or "pyramid" schemes of any type
20. Storing sensitive or confidential data, including but not limited to student's personally identifiable information (PII) data, on flash drives or other portable or external media unless specifically authorized by the Information Technology Department.
21. Unauthorized use, or forging, of email header information.
22. Storing of personal data or information on college computing resources.
23. Transmitting sensitive or confidential information without making reasonable accommodations to ensure the security of the information.

All users of college computing resources are responsible for practicing basic cyber security safety practices. It is up to each user to safeguard the personal information of themselves and others. All faculty, staff, and students are required to utilize and comply with specific security controls including, but not limited to multi-factor

authentication, and any future security protocols instituted by the college to assist in the protection of college assets, data, and information.

Terra State Community College reserves the right to audit users, networks, systems, and connected devices on a periodic basis to ensure compliance with this policy. By using any college computing resource, all users accept that activities may be monitored, logged, and reviewed by college-approved personnel, or may be discovered in legal proceedings.

Any user's account that is suspected to be compromised will be immediately locked down by the IT department until remediation actions can be taken to secure the compromised account.

Violations of this policy may result in, but not limited to, immediate restriction or forfeiture of computer access privileges, disciplinary action, which may include suspension of privileges, restriction of access, or more severe penalties up to and including suspension or expulsion (students), or termination of employment (staff). Where illegal activities or theft of college property (physical or intellectual) are suspected, the college may report such activities to the applicable authorities.

All user accounts are the property of Terra State Community College and are subject to termination upon a student's graduation or withdrawal, or an employee's resignation or termination. The college is under no obligation to allow a departed user access to their closed account to retrieve personal files or email communications, nor is the college responsible for the loss of any user's personal files.

The Information Technology department will monitor and revise this Acceptable Use Policy document on an as-needed basis to keep up with the changing needs of the technology in use at the college.

Procedures

Any violations of this policy are to be reported to the Chief Information Officer or emailed to abuse@terra.edu.

Information Technology personnel will immediately disable access to any user account that is suspected of being compromised until remediation actions can be taken.

Resources

Documentation

Electronic Communications Privacy Act – https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Computer Fraud and Abuse Act – https://www.energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings
Internet	A worldwide system of computer networks
Personally Identifiable Information (PII)	Any data element that can be used to unequivocally identify a person such as, but not limited to, Social Security Number, Driver's License Number, face, credit card number, digital identity.
Phishing	A fraudulent practice of sending messages purporting to be from reputable companies for the purpose of misleading individuals into revealing personal or financial information or login credentials.

Network	Two or more computers linked together to share resources, exchange files or data, or to allow electronic communication.
Email Header	An area of an email that contains important information such as sender and receiver details, subject, date, return path, and reply-to field. The header will also contain technical details such as who sent the message, software used, message ID, and email servers that the message has passed through.

Approval History

Date	Policy/Procedure or Entire Document	Notes (Types of Actions)	**Approved by
11/17/2004	Policy	Issued	
12/15/2017	Policy	Revised	
12/19/2022	Entire Document	Edited – Updated to new form	Wayne Yerdon
12/22/2023	Policy	Annual Review & Update	Wayne Yerdon

**Full name of CASA Committee Chair, signatory, or designee

Effective Date: 2/02/2023

Next Review Date: 1/9/2025