Policy Number: *1.9.001*
Title: **Information Technology Resources Acceptable Use Policy**

Purpose

Thaddeus Stevens College of Technology College's (the College) infrastructure supports the academic and administrative activities essential to fulfilling the College's mission. Access to these resources is a privilege that must be exercised responsibly, ethically, and lawfully. The purpose of this Information Technology Resources Acceptable Use Policy is to clearly define each user's role in protecting the College's information assets and to communicate the expectations for compliance.

Scope

This policy is for students, faculty, staff, student workers, and service providers and applies to all users of resources owned, managed, or provided by the College. It covers students, faculty, staff, student workers, and service providers who have access to the College's resources and facilities. Resources include College-owned or managed hardware and software, email, web domains, related services, and any use of the College's network—whether via physical or wireless connection—regardless of the ownership of the device used.

Privacy and Access to Information

The College strives to respect user privacy, but users do not have an expectation of privacy for communications transmitted or stored on the College's resources. The President, Vice-President of Finance and Administration, or Director of Technology may authorize designated College officials or agents to access, review, monitor, or disclose computer files related to an individual's account in response to legal requirements, College policy, or when deemed necessary to protect the College's interests. Such actions may include, but are not limited to, investigating violations of law or College policies or responding to health or safety emergencies.

Definitions

Classification - Process of organizing and identifying organizational information to relevant categories to be protected more efficiently, facilitate appropriate access, and maintaining regulatory compliance.

The College utilizes the following three categories.

a. Public: Information whose loss, corruption, or unauthorized disclosure would cause minimal or no personal, financial, or reputational harm to the College, College staff or the constituents/people we serve.
b. Private: Information whose loss, corruption, or unauthorized disclosure would likely cause limited personal, financial, or reputational harm to the College, College staff or the constituents/people we serve.
c. Restricted: Information whose loss, corruption, or unauthorized disclosure would cause severe personal, financial, or reputational harm to the College, College staff or the constituents/people we serve.

Denial-of-Service Methods - involve overwhelming a system, network, or service with excessive traffic to disrupt or block legitimate access, making it unavailable to users.

Intellectual Property - creations of the mind, such as inventions, designs, logos, names, artistic works, and trademarks, that are legally protected from unauthorized use. It allows creators to control and benefit from their work, and it includes patents, copyrights, trademarks, and trade secrets.

Malicious Activity - intentional actions that harm, disrupt, or compromise computer systems, networks, or data, such as spreading viruses, unauthorized access, or installing harmful software.

Personal Gain - any benefit, profit, or advantage an individual receives for their own use at the expense of others or an organization. This can include financial, material, social, or status-related benefits. For example, using work resources for personal business or financial profit, or exploiting a situation to increase one's own status, would be considered seeking personal gain.

Pirated Software - unauthorized copies of software that are distributed or used without the proper licensing or permission from the copyright holder. This includes software that is copied, downloaded, or shared illegally, often for free or at a reduced price.

Pyramid Scheme - a fraudulent system where participants earn money mainly by recruiting others, rather than through legitimate products or services. It collapses when recruitment slows.

SMS - Short Message Service, a text messaging service used for sending short messages (usually up to 160 characters) between mobile devices.

SPAM - unsolicited, often irrelevant, or inappropriate messages sent in bulk, usually for commercial or fraudulent purposes. It commonly occurs via email but can also appear in other forms like social media or instant messaging.

Spoofing - act of pretending to be someone or something else to deceive or gain unauthorized access. It can involve falsifying the origin of an email, IP address, or other data to make it appear as if it comes from a trusted source. Spoofing is commonly used in phishing attacks or to bypass security measures.

Trojan Horses - malicious programs that disguise themselves as legitimate software or files to trick users into installing them. Once activated, they can give attackers unauthorized access to a system, steal data, or cause other harm without the user's knowledge.

User Authentication - process of verifying the identity of a user attempting to access a system or network. It typically involves checking credentials, such as a username and password, biometric data, or security tokens, to ensure the person is authorized to use the system.

Worms - self-replicating malicious software programs that spread across networks without needing human interaction. They can exploit vulnerabilities in a system to infect other devices, often causing damage, consuming bandwidth, or spreading malware.

Policy Detail

Activities supporting the College's mission take priority over personal or recreational computing use. Any activity that disrupts the College's mission is prohibited. All users of College resources must comply with the requirements outlined below, as well as other College Policies and Procedures and Code of Conduct.

I. Use of College Resources and Systems

College-provided IT resources, systems, and WiFi are primarily designated for instructional, research, work-related activity, departmental activity, or for administrative purposes. Employees and students may use these resources for personal purposes if that use does not interfere with the primary use and does not interfere with one's normal duties. Users must not use the College's information systems or data for commercial use or personal gain for their own use at the expense of others or an organization. If the non-business usages results in a direct cost to the College for any reason, it is the individual's responsibility to reimburse the College. For more information, please refer to the Conflict of Interest Policy.

A. Student and Employee Access
   1. College-Issued Email Address
      a. Your College-issued email address (example@stevenscollege.edu) is the primary platform for:
         i. important updates related to student life;
         ii. communications with your instructors;
         iii. sending essential announcements and reminders; and
         iv. providing access to most resources at the college.
      b. It is essential to activate your College email and check it regularly.
      c. Students can activate their email before classes start.
      d. Students and employees must register for Multi-Factor Authentication (MFA) within their accounts. MFA provides a second form of verification and is required for off-campus access.
      e. Recommended MFA Setup
         We recommend using the Microsoft Authenticator application on your phone via QR Code. To install the Authenticator on your iOS device:
         i. iOS link
         ii. Android link
         iii. Once installed and linked to your stevenscollege.edu account, it will automatically link to your Microsoft applications and most applications.
      f. A student and employee's email account is a Microsoft account that provides access to a student A5 license, which includes applications such as Excel, Word, Teams, OneDrive, and PowerPoint.

   2. Thad's Pad
   a. Thad's Pad is your "one-stop shop" online tool. It is a secure site that provides single sign-on access to Thaddeus Stevens College applications, including your College-issued email. It also offers a variety of customized information and resources to help you track your academic progress and make the most of your experience at the College.
   b. Network ID Usage
      Each individual may only use the network ID assigned to them, unless additional access has been authorized for that specific ID.

For Students:

1. While enrolled at the College, students will have access to cloud-based software to support their studies.
2. After graduation students' access to cloud-based software will remain active for one year.
3. If a student withdraws from the College, access will be immediately removed.

For Employees:

1. While at the College, employees will have access to cloud-based software to support their work.
2. Upon termination of employment or resignation, employees will no longer have access to any cloud-based software or internal programs affiliated with the College.

3. Social Media
   Social media and networking platforms are powerful communication tools that allow individuals to connect, share, and engage with a broad audience. The College supports students to participate in online communities as a means of communication, learning, and professional networking. However, students may be subject to disciplinary action if their personal use of social media violates College policies, including the Student Code of Conduct. Students should be aware that the content they post on social media may impact future opportunities. Employers increasingly review social media activities during the hiring process.

B. Fraudulent and Illegal Use
   The strictly prohibits the use of any College information system or network resources for fraudulent or illegal activities. Users must not engage in any activity that violates local, state, federal, or international law while using the College's information systems or network resources.

   1. Users must not:
      a. Violate the rights of individuals or organizations regarding information protected by copyright, trade secret, patent, other intellectual property, or similar laws, including, but not limited to, the installation or distribution of pirated software or software not licensed for use by the College.
      b. Use copyrighted material including, but not limited to, photographs, books, music, or software – without the College having the proper legal license.
      c. Abide by all software licensing agreements and copyright laws. Unauthorized copying of copyrighted software is prohibited, unless the College holds a site license that permits such copying.
      d. Copy site-licensed software or cloud-based software for distribution to individuals other than Thaddeus Stevens College faculty, staff, and students, or use site-licensed software outside the scope of the license agreement.
      e. Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
      f. Make fraudulent statements about warranties or offer false products, services, or items unless such actions are part of the normal duties.
   2. Reporting and Liability for Inappropriate Use

The Information Technology (IT) team must be notified of any potential security vulnerabilities or incidents involving misuse, abuse, or violations of laws, intellectual property rights, or copyrights. IT should also be kept informed during investigations of such issues.

If a user's inappropriate use of College resources results in liability for the College, the user agrees to indemnify and hold the College harmless in the event the College needs to defend itself legally against the user's actions.

C. Malicious Activity

The College strictly prohibits the use of information systems for any malicious activity that targets other users, the college's information systems or the information assets of external parties.

1. Denial of Service
    a. Users must not:
        i. Disrupt the College information systems or network communications through denial-of-service methods.
        ii. Introduce malicious programs such as viruses, bitminers, worms, or Trojan horses into any information system.
        iii. Develop or use programs to infiltrate, damage, or alter a computer, WiFi components, high-speed backbone network, communication lines, system, or network.

    Exceptions may be granted for approved academic purposes.
2. Confidentiality
    a. Users must not:
        i. Cause or enable security breaches, including attempting to bypass data protection measures, uncover security vulnerabilities, access data or accounts without permission.
        ii. Share their password or login credentials with anyone, including other users, family members, or friends.
        iii. Attempt to access files or resources they have not been authorized to view, including obtaining or using another user's password.
        iv. Make copies of another user's files without their knowledge and consent.
3. Impersonation
    a. Users must not:
        i. Bypass user authentication or security measures of any information system.
        ii. Modify network headers or use forged information to impersonate someone else ("spoofing").
        iii. Create or use proxy servers not authorized by Thaddeus Stevens College or redirect network traffic outside normal routing.
        iv. Use technologies designed to hide or alter their identity or activities electronically.

D. Objectionable Content

The College strictly prohibits the use of its administrative information systems to access or distribute content that may be deemed objectionable by other users.

This includes posting, uploading, downloading, or displaying any of the following materials:

1. Political
2. Racist
3. Sexually Explicit
4. Violent or Promoting Violence

E. Hardware and Software

Users are prohibited from installing, attaching, connecting, removing, or disconnecting any hardware—including wireless access points, storage devices, and peripherals—on any College information system without prior approval from Computer and Networking Services (IT). The College strictly prohibits the use of hardware or software for administrative or academic purposes unless it has been purchased, installed, configured, tracked, and managed by the College.

1. Users must not:
    a. Install, attach, connect, remove, or disconnect any hardware, including wireless access points, storage devices, and peripherals, without Information Technology's permission.
    b. Download, install, disable, remove, or uninstall software (including patches) on any College information system without the approval of IT
    c. Use personal flash drives or other USB storage devices without prior manager approval.
    d. Remove College equipment from campus without prior authorization.

F. Messaging

The College provides a communication platform to support its mission. No individual may engage in activities that deliberately waste computer and network resources or unfairly monopolize them to the exclusion of others, such as:

1. Users must not:
    a. Send unsolicited electronic messages, including "junk mail" or other advertising, to individuals who have not requested such material (SPAM).
    b. Solicit electronic messages for any digital identifier (e.g., email, social handle) other than their own, with the intent to harass or collect responses.
    c. Create or forward mass mailings or chain letters, including those promoting 'pyramid' schemes; generate unnecessary jobs or processes; obtain excessive output; upload large files like music and videos; print excessively; or create unnecessary network traffic.
2. Students must not:
    a. Automatically forward electronic messages of any kind using client message handling rules or other mechanisms.

G. Network Discovery

1. Users must not:
    a. Use port scanning tools on the college network or any external network, unless this activity is part of their job duties, such as conducting vulnerability scans as a member of Computer and Networking Services (IT) or using tools in a controlled environment for faculty purposes.

b. Use network monitoring tools or engage in any form of network monitoring that intercepts data not intended for them unless this is part of their job responsibilities.

II. Confidentiality and Security

A. Confidential Information

The College has both ethical and legal responsibilities to protect confidential information classified as “Restricted” or “Private.” To meet these obligations, the College has established the following guidelines:

1. Transmission of confidential information via unauthorized messaging technologies (e.g., personal email, instant messaging, SMS, chat) is prohibited.
2. Writing or storing confidential information on mobile devices (e.g., phones, tablets, USB drives) or removable media is prohibited.
3. Recording devices (e.g., photographic, video, audio) are prohibited in designated secure areas.

B. Incident Reporting

The College is committed to addressing security incidents involving personnel, college-owned information, or assets.

As part of this policy:

1. Any loss, theft, or misuse of College access credentials (e.g., passwords, key cards, security tokens) or other information must be immediately reported to IT.
2. No student shall prevent another individual from reporting a security incident.

C. Provisions for Private Devices Connected to the College Network

The following guidelines apply to anyone connecting a private device (e.g., computer and cell phone) to the College network:

1. The device owner is responsible for the actions of all users and all network traffic to and from the devices, whether they are aware of it.
2. A private device may not be used to provide network access to unauthorized individuals or function as a router or bridge between the College network and external networks (e.g., Internet Service Provider).
3. If Information Technology staff suspect inappropriate use of a private device connected to the College network, network traffic may be monitored. If necessary, the system will be disconnected, and further action may be taken.
4. Students with authorized network accounts may use the College network under the following conditions:
    a. The use does not violate any law, regulation, or policy.
    b. It does not cause excessive use of College resources or interfere with network performance.
    c. It does not violate any part of this policy.
5. Users are responsible for their device’s security and integrity. If a device is compromised, the user must immediately shut it down and disconnect it from the network to prevent further damage or spread of the attack. For assistance, enter a ticket and email staffcns@stevenscollege.edu.
6. Personal servers, Wi-Fi network, rogue connections or entities, or network equipment may not be connected to the College network without prior authorization from Information Technology Services.

III. Roles and Responsibilities

The College reserves the right to protect, repair, and maintain its computing equipment and network integrity. In accomplishing this goal, the College's Information Technology personnel or their authorized partner will make every effort to protect user privacy, including the content of personal files and Internet activities. Any information obtained by Information Technology personnel about a user through routine maintenance of the College's computing systems should remain confidential, unless it pertains to activities that violate the acceptable use of the College's resources.

IV. Enforcement

Enforcement of this policy is the responsibility of the College's President or designee. Users who violate this policy may be denied access to the College's resources and may face disciplinary action, both within and outside of the College. The College may temporarily suspend or block access to an account if necessary to protect the integrity, security, or functionality of the College resources or to mitigate liability. Users are also subject to disciplinary rules outlined in policies and procedures governing acceptable workplace behavior.

V. Exceptions

Exceptions to this policy may be granted by the President or Vice President of Finance and Administration. All exceptions must be reviewed annually.

VI. Indemnification/Liability Statement

A. Thaddeus Stevens College of Technology makes no warranties, either express or implied, regarding the Internet services it provides. The College is not responsible for any damages suffered by users, including, but not limited to, data loss due to delays, non-deliveries, user errors, or service interruptions.

B. The College is not liable for the accuracy or quality of information obtained through its Internet services, including email. Users assume responsibility for any damages resulting from information obtained through these sources.

C. The user agrees to indemnify and hold harmless Thaddeus Stevens College of Technology, its Board of Directors, and its employees from any claim, lawsuit, cause of action, damages, judgment, loss, expense, or liability arising out of the use of the College's hardware, software, and network facilities. This indemnification includes, but is not limited to, claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

References

The Gramm-Leach Bliley Act (GLBA)
Family Educational Rights and Privacy Act (FERPA)
Pennsylvania's Breach of Personal Information Notification Act
NIST 800-53
FIPS-199
PCI DSS 3.1
Code of Ethics of the American Library Association

Audience	*All College*
Effective Date	*01/22/2018*
Date Revised	*01/08/2026*
Date Reviewed	*01/08/2026*
Owner	*Director of Information Technology*
Policy Title	*The policy title was previously "Computer Resources: Acceptable Use Policy" before 2025. On 2/21/25, the title was changed to "Information Technology Resources Acceptable Use Policy" to better reflect that IT encompasses all information technology, not just computer resources.*