Information Technology Acceptable Use Policy

#1-021

GENESEO
THE STATE UNIVERSITY OF NEW YORK

Approved By: Cabinet
Effective Date: 08-01-1989
Revised Date: 10-21-2025

Category: General College
Policy Owner: Computing and Information Technology
Office Number: 585-245-5577

Scope

This policy applies to all individuals who access, use, or manage SUNY Geneseo's information technology (IT) resources, regardless of location, device ownership, or employment status. This includes, but is not limited to:

- Faculty, staff, and students.
- Retirees with extended access.
- Contractors, consultants, and vendors.
- Volunteers, affiliates, and visitors.
- Third-party service providers with access to Geneseo systems.

Covered IT resources include all college-owned or managed:

- Computing devices (e.g., desktops, laptops, tablets, mobile phones).
- Network infrastructure (e.g., wired and wireless networks, VPN).
- Software and applications (e.g., licensed software, cloud services, AI tools).
- Cloud storage platforms (e.g., Google Drive, Microsoft OneDrive, SharePoint).
- Learning Management Systems (e.g., Brightspace).
- Data and storage systems (e.g., institutional data, backups, shared drives).
- Communication platforms (e.g., email, messaging systems, listservs).

This policy applies to all use of Geneseo IT resources, whether on campus or remotely. All users are expected to comply with this policy and related institutional policies, procedures, and applicable laws.

Policy Statement

SUNY Geneseo provides information technology resources to support its academic, research, administrative, and outreach missions. These resources include computing systems, networks, software, data, and communication platforms that are essential to the daily operations of the college.

This policy establishes expectations for the responsible and ethical use of IT resources by all members of the campus community. It is designed to protect the integrity, security, and availability of institutional systems and data, ensure compliance with applicable laws and regulations, and promote a respectful and inclusive digital environment.

Users of Geneseo's IT resources are expected to:

- Use resources in a manner consistent with the college's mission and values.
- Respect the rights and privacy of others.
- Protect institutional data and systems from unauthorized access or misuse.
- Handle institutional data in accordance with Geneseo's Data Classification and Protection policy, which define levels of sensitivity and appropriate safeguards.

- Comply with all relevant policies, including those related to data classification, listserv management, and copyright.

This policy applies regardless of device ownership or location of access, including use of personal devices and remote connections.

Definitions

Computing Resources

Data Classification

FERPA

Mass Digital Communications

Multi-Factor Authentication (MFA)

Policy

Acceptable Use

Computing resources at SUNY Geneseo are provided for educational and business purposes. As a convenience to the Geneseo user community, limited incidental personal use of computing resources is permitted. Examples of acceptable incidental personal use include checking personal email, reading news, or briefly browsing non-work-related websites. Such use must not be illegal, interfere with job responsibilities, or compromise the integrity or availability of Geneseo IT systems. Faculty and staff are responsible for exercising good judgment about personal use in accordance with Geneseo and SUNY policies and ethical standards for state officers and employees. State officers and employees are expected to pursue a course of conduct that maintains public trust.

Use of AI tools (e.g., Copilot, Gemini) is permitted when aligned with institutional goals and data protection standards. These tools may be used for productivity, learning, or research, but must not be used to circumvent academic integrity or handle sensitive data.

Users may utilize cloud services such as Google Workspace and Microsoft 365 OneDrive and SharePoint provided their use complies with institutional guidelines and data protection policies.

All digital communications conducted through Geneseo IT resources must be respectful, professional, and consistent with SUNY Geneseo's mission and values.

Unacceptable Use

The following activities are prohibited when using SUNY Geneseo's computing resources. These examples represent violations of institutional policy, compromise security, or conflict with the college's mission and values.

Unauthorized Access and Sharing

- Accessing systems, accounts, or data without proper authorization.
- Sharing college-provided devices (e.g., laptops, desktops, tablets) with others, including family members or roommates.
- Using another person's Geneseo credentials or allowing others to use your own.
- Using former system privileges after your association with Geneseo has ended.

Confidential Data on Personal Devices

- Accessing or storing confidential institutional data on personally owned devices.
- Using personal cloud accounts or email services to transmit or store confidential college data.

Malicious or Illegal Activity

- Uploading, downloading, or distributing illegal content, including pirated software or media.
- Engaging in phishing, malware distribution, or other forms of cyberattack.

- Attempting to circumvent security controls or exploit system vulnerabilities.
- Using packet sniffers, keystroke loggers, or similar tools without authorization.

Harassment and Abuse

- Using IT resources to harass, threaten, impersonate, or deceive others.
- Sending messages or posting content that is discriminatory, abusive, or violates campus conduct policies.

Disruption of Services

- Running bots, scripts, or programs that interfere with normal system operations or monopolize shared resources.
- Intentionally or recklessly interfering with Geneseo's network infrastructure (e.g., wired, wireless, VPN) or transmitting unauthorized signals.
- Performing Denial of Service (DoS) attacks or similar actions intended to render services inaccessible to other authorized users.

Circumvention and Misrepresentation

- Falsifying identity or using aliases to avoid accountability.
- Attempting to bypass monitoring, logging, or usage restrictions.
- Sending messages or printing files that do not show the correct username of the user performing the operation.

Abuse of Incidental Personal Use

- Using Geneseo IT resources for personal financial gain or commercial ventures not affiliated with the college.
- Using IT resources for personal activities that are illegal, interfere with work responsibilities, result in measurable cost to the college, or conflict with Geneseo's nonprofit status.

Wasteful Use of Resources

- Excessive or non-essential printing of documents without a legitimate academic or business purpose.
- Excessive consumption of computing capacity for non-institutional purposes, such as cryptocurrency mining or running endless/repetitive computations.
- Excessive consumption of storage capacity for non-institutional purposes, such as bulk personal data or photo storage.
- Monopolizing shared resources, such as holding public computers or shared devices for extended periods when others are waiting.

Mass Digital Communications

Mass digital communications at Geneseo —such as email listservs, bulk messaging platforms, or shared distribution lists— are intended solely to communicate important information regarding academic, college, and student business to students, faculty, and staff. These communications should be relevant to the intended audience, respectful in tone, and consistent with SUNY Geneseo's mission and values.

Unsolicited mass communications are not permitted. This policy must not be circumvented by sending multiple messages to smaller populations. Opt-in mailing lists for projects, student organizations, or external groups can use Google Workspace @ Geneseo. Centrally managed Geneseo mailing lists are restricted to messages that meet their purpose.

All use of listservs must follow the Listserv Management Policy, which outlines approval processes, audience targeting, and appropriate content standards.

Use of AI and Emerging Technologies

SUNY Geneseo recognizes the growing role of artificial intelligence (AI) and emerging technologies in education, research, and administrative work.

Permitted Use

- AI tools (e.g., Copilot, Gemini, ChatGPT) may be used for tasks such as drafting content, summarizing information, generating ideas, or automating routine processes.
- Use must align with institutional goals and comply with applicable laws, policies, and ethical standards.
- Users must be aware of potential bias in AI-generated content and exercise critical judgment when using these tools for decision-making or communication.

Prohibited or Restricted Use

- AI tools must not be used to process, store, or transmit institutional data classified as Sensitive or Confidential unless explicitly approved and protected under enterprise agreements.
- Use of AI to circumvent academic integrity, impersonate individuals, or generate misleading or harmful content is strictly prohibited. Users should follow academic integrity guidelines as outlined by their instructors and the Teaching and Learning Center's guidance on generative AI.

User Responsibilities

- Users must verify the accuracy of AI-generated content before relying on it for official or academic purposes.
- Users are responsible for ensuring that AI use complies with copyright, licensing, and data protection requirements.
- SUNY Geneseo provides access to enterprise AI tools such as Microsoft Copilot, which include enhanced data protection and integrations with other supported services. Users are encouraged to use institutionally provisioned tools when available and avoid using commercial platforms that may not meet institutional data protection standards. Questions about appropriate use of AI tools should be directed to the Office of the CIO.

Security, Privacy, and Monitoring

SUNY Geneseo retains ownership of all institutional computing resources and reserves the right to monitor, access, or inspect their use when necessary. While the College does not routinely monitor individual usage, users should not expect privacy when using Geneseo IT systems.

Monitoring or inspection may occur under the following circumstances:

- To maintain system integrity, security, or performance.
- To investigate suspected policy violations or illegal activity.
- To comply with legal obligations, including subpoenas, FOIL requests, or litigation.
- When an account exhibits unusual, excessive, or malicious activity.
- When a user has voluntarily made content publicly accessible.

The College may also monitor or inspect the activity of individual users of college computing resources, including individual login sessions and the content of individual communications, or delete user content that is not required to be kept by retention policy without notice or permission. Retention requirements are governed by SUNY's Records Retention Schedule.

Routine IT operations may involve:

- Backups of data and communications.
- Logging of activity and usage patterns.
- System diagnostics and performance monitoring.

Users must respect the privacy of others. Unauthorized access to another user's files, email, or account is prohibited. Any attempt to circumvent security controls or exploit vulnerabilities to gain access to private information is a violation of this policy.

Roles and Security Responsibilities

Effective implementation of this policy requires shared responsibility across the campus community. All users and designated roles must follow secure computing practices and comply with institutional policies and applicable laws.

End Users

All individuals who access Geneseo IT resources are responsible for:

- Using resources in accordance with this policy and related institutional policies.
- Protecting their credentials and devices.
- Enabling Multi-Factor Authentication (MFA) and using strong passphrases.
- Reporting suspected security incidents or policy violations using the Security Incident Report Form.
- Respecting the privacy and rights of others.
- Complying with applicable local, state, and federal laws, including copyright, data protection, FERPA, HIPAA, and Payment Card Industry regulations.

Supervisors and Department Heads

Responsible for:

- Ensuring their teams understand and comply with this policy.
- Supporting secure practices within their departments.
- Coordinating with CIT on access needs and incident response.

Account Managers

Designated individuals responsible for managing generic accounts (e.g., departmental, club, or initiative accounts) must:

- Ensure accounts are used appropriately and securely.
- Maintain accountability for all activity under the account.
- Update access permissions as roles change.
- Ensure compliance with institutional security standards.

Computing & Information Technology (CIT)

Responsible for:

- Maintaining and securing Geneseo's IT infrastructure and systems.
- Monitoring performance, usage, and security across institutional platforms.
- Investigating incidents, enforcing policy violations, and coordinating response efforts.
- Developing and maintaining IT and security policies, standards, and procedures.
- Advising on data protection, compliance, and risk mitigation strategies.
- Supporting users with secure computing practices and technology guidance.

Data Stewards

Individuals responsible for specific institutional data sets must:

- Classify and protect data in accordance with the Data Classification and Protection policy, ensuring appropriate safeguards based on sensitivity level.
- Ensure appropriate access controls are in place.
- Collaborate with CIT on data governance.

Policy Violations and Enforcement

Violations of this policy include any activities outlined in the "Unacceptable Use" section, as well as other actions that compromise the integrity, security, or availability of Geneseo's IT resources. Reports of suspected violations may be submitted through a supervisor, the Office of the CIO, the CIT Help Desk, or via the Security Incident Report Form.

Users who violate this policy may be denied access to college computing resources and may be subject to disciplinary action, including expulsion or dismissal. Alleged violations will be handled through applicable college disciplinary procedures.

CIT may suspend, block, or restrict access to accounts when necessary to protect system integrity or prevent further unauthorized activity. Suspected violations of law may be referred to law enforcement.

Users are expected to cooperate fully in investigations. CIT may coordinate with campus offices such as the Dean of Students, Human Resources, and University Police. During investigations, CIT may suspend access to computing facilities for involved users.

Frequency of Review and Update

This policy will be reviewed every 3 years by CIT, in consultation with relevant campus stakeholders. Interim updates may be made as needed to reflect changes in technology, legal requirements, or institutional priorities.

Periodic Review Completed:10-21-2025

Approval

Signed By Paul Jackson

10-21-2025

Paul Jackson
CIO and Director, CIT

Date of Approval