Information Technology Acceptable Use Policy

Created by Laurie Fox, last modified by Sue Chichester on Sep 06, 2022

Scope

This policy defines guidelines on the acceptable use of computing resources owned, operated, and managed by SUNY Geneseo. This policy applies to all persons accessing or using Geneseo's technology resources, including all faculty, staff, students, affiliates, volunteers, or visitors at the College, hereafter referred to as users.

Policy Statement

This policy is intended to promote excellent information and network security posture for SUNY Geneseo and to specify acceptable and unacceptable activities involving SUNY Geneseo's computing resources.

The purpose of this policy is to outline the acceptable use of computing resources and any information maintained in any form and any medium within the College's computing resources and explain violations of acceptable use. Additionally, all creation, processing, communication, distribution, storage, and disposal of information by any combination of college resources and non-college resources are covered by this policy.

Access to information technology is essential to the college's mission. The privilege to use computing resources requires that each faculty member, staff member, student, and other user comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

To assist and ensure such compliance, SUNY Geneseo establishes the following policy, which supplements all applicable SUNY and College policies, including harassment, patent and copyright, student and employee disciplinary policies, and FERPA, as well as applicable federal and state laws.

SUNY Geneseo values the privacy rights of all individuals using its computing resources. As a usual business practice, Geneseo does not routinely monitor individual usage of its computing resources. Nonetheless, users should be aware that all computing resources are the property of Geneseo. As such, the college may access and monitor computing resources and any information stored on or transmitted through those computing resources, but only in accordance with applicable laws, for legitimate business purposes including, but not limited to, system monitoring and maintenance, complying with legal requirements, police investigations, investigating security incidents, and administering this or other Geneseo policies. Further, to protect systems on the Geneseo network, the college may, without prior notice if deemed necessary, remove compromised devices from the network, block malicious traffic from entering the network, and prohibit devices within Geneseo's network from connecting to known malicious outside entities.

Definitions

Computing resources – Computing resources refer to computing technology owned, leased, operated, and managed by the College, including but not limited to software, electronic mail systems, web hosting, applications, storage media, databases, and Internet connectivity. Also included are physical resources such as College-owned, -leased, -operated, or -managed computers, network cabling, wireless access points, computer workstations, kiosks, card swipes, printers/copiers, audio-visual equipment, telephone/fax equipment, classroom equipment, or wiring closets. Further, computing resources encompass all college voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities.

FERPA

Mass digital communications - Messages sent, unsolicited, to large segments of the college population using email, text messaging, or voice telephony.

MFA (Multi-Factor Authentication) Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Source: csrc.nist.gov/glossary/term/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. 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. In general, State officers and employees are charged to pursue a course of conduct that will not raise suspicion among the public that they are likely to be engaged in acts in violation of the public trust. Examples of incidental personal use may include sending an occasional personal email or visiting a non-work-related website. Incidental personal use must comply with the following:

1. It cannot be illegal.
2. It cannot interfere with a Geneseo employee's job responsibilities.
3. It cannot adversely affect the availability, integrity, or reliability of Geneseo IT systems or cause harm to the activities of others using the IT systems.
4. It cannot be inconsistent with the College's status as a state entity and its non-profit, tax-exempt status.

College-provided devices (i.e., laptops, desktops, tablets) shall not be shared with or used by anyone other than the primary user.

College employees should use separate non-Geneseo accounts, email addresses, and devices for personal activities. Personally owned devices should not be used to access sensitive Geneseo data (e.g., FERPA or HIPAA protected information).

Resources

The College's information technology resources are, by nature, finite. All members of the college community must recognize that specific uses of college information technology resources may be limited for reasons related to the capacity or security of the college's information technology systems or as required for fulfilling the College's mission.

Although there is no set bandwidth, disk space, CPU time, or other limits applicable to all uses of college computing resources, the college may require users of those resources to limit or refrain from specific uses if, in the opinion of the system administrator, such use interferes with the efficient operations of the system. Users are also expected to refrain from deliberately wasteful practices such as printing unnecessary large documents, performing endless unnecessary computations, or holding public computers for long periods when others are waiting for the same resources.

User Accounts

Users are responsible for ascertaining what authorizations are necessary and obtaining them before using college computing resources. The use of SUNY Geneseo's computer systems and network requires that the College issue a user account. Every computer user account issued by SUNY Geneseo is the responsibility of the person whose name it is issued. Users are responsible for any activity originating from their accounts that which they can reasonably be expected to control. Under any circumstances, accounts and passwords may not be used by persons other than those to whom the account administrator has assigned them. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident.

College recognized clubs and student organizations may be issued a user account. Faculty advisors shall designate a particular person(s) (e.g., club president) authorized to act on behalf of the club or organization. This person(s) is responsible for all activity on the account and will be subject to College disciplinary procedures for misuse.

The college employs various measures to protect the security of its computing resources and its user's accounts. Users

should be aware, however, that the college cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices using long complex passphrases, employing Multi-Factor Authentication, and guarding their passwords and MFA methods.

Laws and College Policies

Users of college computing resources must comply with federal and state laws, college rules and policies, and the terms of applicable contracts, including software licenses, while using college computing resources. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies of those other systems and networks. Users with questions about how the various laws, rules and resolutions may apply to a particular use of college computing resources should contact the Office of the CIO for more information.

Users must use computing resources consistent with local, state and federal laws and policies and college policies. Examples include but are not limited to:

1. Users shall comply with federal copyright law.
2. Users shall not download, use or distribute illegally obtained media (e.g., software, music, movies).
3. Users shall not upload, download, distribute or possess child pornography.

Mass digital communications

Mass digital communications at Geneseo are intended solely to communicate important information regarding academic, college, and student business to students, faculty, and staff.

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.

Security & Privacy

Users should be aware that their college computing resources' use is not private. The college always retains ownership of its computing resources. Such ownership provides the college with an inherent right of access. While the college does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the college's computing resources require backup of data and communications, logging of activity, monitoring general usage patterns, and other activities necessary for the provision of service. 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 when:

1. The user has voluntarily made them accessible to the public by posting to a web page.
2. It reasonably appears necessary to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability.
3. There is reasonable cause to believe that the user has violated or is violating this policy or any other law or policy.
4. An account appears to be engaged in malicious, unusual, or excessive activity.
5. Accessing the account is otherwise required or permitted by law, including but not limited to freedom of information laws, laws governing the conduct of parties engaged in or anticipating litigation, and laws governing criminal investigations.

Users shall respect the privacy of others. Users shall not intentionally view information of other users, modify or obtain copies of other user's files, access or attempt to access other users' email, or modify other users' passwords without their permission. Unless the information is specifically made public or accessible to you, you should assume anything on the network is private. Just because you may have the ability, through a loophole, someone's carelessness, etc., to access files, directories, or information that does not belong to you, you do not have the right to do so. Any attempt to circumvent computer, network, or file security or to take advantage of security lapses is prohibited.

Violations of Acceptable Use

Violations of this Policy include, but are not limited to:

1. Illegal Use - Using computing resources to upload, download, transmit, post, or store any material or data that, intentionally or unintentionally, violates any applicable local, state, national or international law, or violates the rules, policies, or procedures of the College or any college department is prohibited. Transmitting, uploading, downloading, or storing any material that infringes upon an existing copyright, trademark, patent, trade secret, or other legal right using computing resources is also prohibited.
2. Threats or Harassment - Using computing resources to transmit material or data that causes or encourages physical or intellectual abuse, damage, or destruction of property, or that causes or encourages harassment, explicit or implied, is prohibited.
3. Forgery or Impersonation - Falsifying or removing identifying information on computing resources with intent to deceive, defraud, or misguide is prohibited. Impersonation of other persons or groups with the intent to harm is prohibited.
4. Malicious Content - Use of Geneseo computing and messaging systems to transmit any material which contains malicious content, such as malware or phishing scams, or any other content that may damage computer systems or collect or misuse personal information is prohibited.
5. Fraudulent Activity - Using computing resources to transmit material or communications to promote a financial scam or wrongdoing is prohibited.
6. Unauthorized Access or Penetration Attempts (i.e., “hacking”) - Unauthorized access or penetration attempts of Geneseo computing resources, or a remote entity using SUNY Geneseo computing resources, are prohibited. Users must not use computing resources to impair or damage the operations of any computers, networks, terminals, or peripherals.
7. Intercepting Communications - Using packet sniffers, password capture applications, keystroke loggers, and other tools that perform similar behavior or any form of network wiretapping on Computing Resources is prohibited. Using such tools to diagnose, analyze, or mitigate ongoing service issues or security violations may be permitted when conducted by authorized personnel.
8. Reselling Services - Computing resources are not to be used for personal commercial purposes or personal financial or other gains.
9. Service Interruptions - Using computing resources to permit or promote activity that adversely affects the integrity or performance of computing resources is prohibited. Denial of service attacks, forged packet transmission, and similar actions may be permitted when conducted by authorized College personnel.
10. Physical Security - Unauthorized access to, destruction, extension, or alteration of, theft, damage, or tampering of any physical computing resources, including computer workstations, kiosks, card swipes, printers, audio-visual equipment, telephone/fax equipment, classroom equipment, or wiring closets is prohibited. This applies to all network wiring, hardware, and in-room jacks. Users shall not use the residential network to provide Internet access to anyone outside of the College community for any purpose other than those that are in direct support of the academic mission of the College.
11. Transferring of Use - Permission to use computing resources is granted to individuals and may not be transferred to others. Sharing of a username/password assigned to an individual is expressly prohibited. Use of another user's ID or seeking to access another user's account is prohibited. Similarly, individuals may not use their user credentials to provide access to Geneseo's wireless network to other individuals. The following will be considered theft of services.
    a. Acquiring a username in another person's name.
    b. Using a username without the explicit permission of the owner and Computing & Information Technology.
    c. Allowing one's username to be used by another person without the explicit permission of Computing & Information Technology.
    d. Using former system and access privileges after association with Geneseo has ended.
12. Interference with or Transmission of Wireless Signals - Interfering with Geneseo's wireless networks or attaching a device to transmit a Geneseo network is strictly prohibited.
13. Circumvention of controls – Deliberately circumventing security controls or exploiting vulnerabilities at Geneseo or any other network from Geneseo equipment or network is prohibited. Gaining access by exceeding the limits of assigned authorization is likewise prohibited. Users shall not develop or use procedures to alter or avoid the accounting and monitoring of the use of computing facilities. For example, users may not utilize facilities anonymously or by using an alias. They may not send messages, mail, or print files that do not show the correct username of the user performing the operation.
14. Excessive or Unreasonable Use - Users shall not use information technology resources to excess. Excessive use of information technology resources by a particular user or for a particular activity reduces the amount of resources available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality and result

in significant costs to the college. Some examples of excess use may include writing a program or script or using an Internet bot to perform a repetitive task such as attempting to register for a class or purchasing concert tickets online.

15. Abuse of incidental personal use - Incidental personal use must not:
    a. Be illegal.
    b. Interfere with a Geneseo employee's job responsibilities/work.
    c. Interfere with the legitimate education and business purposes of Geneseo.
    d. Result in any measurable cost to the College.
    e. Adversely affect the availability, integrity, or reliability of Geneseo IT systems or cause harm to the activities of others using the IT systems.
    f. Violate this policy or other College or SUNY policies.
    g. Be inconsistent with the College's status as a state entity and its non-profit, tax-exempt status.
    h. Be for personal gain.

Reporting & Enforcement

Violations of this Policy may be reported through one's supervisor, Office of the CIO, the CIT HelpDesk, or the Information Security Incident Report Form, or as otherwise permitted through College policy.

Users who violate this policy may be denied access to college computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through the college disciplinary procedures applicable to the user. The college may suspend, block, or restrict access to an account, independent of such procedures, when it reasonably appears necessary to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability. The college may also refer suspected violations of applicable law to appropriate law enforcement agencies.

When Computing & Information Technology becomes aware of a possible violation, we will initiate an investigation with relevant campus offices, such as the Dean of Students, Human Resources, and University Police. Users are expected to cooperate fully in such investigations when requested.

To prevent further unauthorized activity during such an investigation, Computing & Information Technology may suspend authorization for the use of all computing facilities for the user(s) involved in the violation.

Related Links

1. Geneseo Password Controls Policy
2. Geneseo Laptop Encryption Policy
3. Remote and VPN Access to Campus Systems for Contractors and Vendors Policy
4. Information Security Incident Report Form
5. Geneseo Student Code of Conduct
6. New York State Laws and Notices
7. New York State Information Technology Policy IT Best Practice Guideline: Acceptable Use of Information Technology (IT) Resources
8. 18 US Code § 1030 https://www.law.cornell.edu/uscode/text/18/1030
9. The Digital Millennium Copyright Act http://lcweb.loc.gov/copyright/legislation/dmca.pdf
10. US Code Title 17 http://www4.law.cornell.edu/uscode/17
11. Electronic Frontier Foundation http://www.eff.org/share
12. Respect Copyrights http://www.respectcopyrights.org

Effective Date

August 1989

Revision Date

September 2022

Frequency of review and update: Every three years.

Signature, title, and date of approval:

Sue Chichester
CIO and Director, CIT
sue@geneseo.edu
Last Updated: September 2022

Effective Date: August 1989
Last Updated: September 2022

cit policy