Acceptable Use Policy

Scope

This is the SUNY Geneseo policy on college-provided access to electronic information, services, computing facilities, and networks. This policy applies to all persons accessing or using college technology resources. This includes students, faculty and staff, authorized guests, and all persons authorized for access or use privileges by the college, hereafter referred to as users.

Summary

Access to information technology is essential to the state university mission of providing the students, faculty and staff of SUNY Geneseo with educational services of the highest quality. The pursuit and achievement of the SUNY mission of education, research, and public service require that the privilege of the use of computing systems and software, internal and external data networks, as well as access to the Internet, be made available to all those of the SUNY community. The preservation of that privilege for the full community requires that each faculty member, staff member, student, and other authorized user comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

Technology resources covered by this policy include, without limitation:

1. all college owned, operated, leased or contracted computing, networking, telephone and information resources, whether they are individually controlled, shared, standalone or networked,
2. all information maintained in any form and in any medium within the college's computer resources, and
3. all college voice and data networks, telephone systems, telecommunications infrastructure, communications systems and services, and physical facilities, including all hardware, software, applications, databases, and storage media.

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.

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.

Policy

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 as to how the various laws, rules and resolutions may apply to a particular use of college computing resources should contact the CIO's Office for more information.

Users are responsible for ascertaining what authorizations are necessary and for obtaining them before using college computing resources. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident.

Although there is no set bandwidth, disk space, CPU time, or other limit 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 unnecessarily holding public computers for long periods of time when others are waiting for the same resources.

Users must not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.

Network services and wiring may not be tampered with or extended beyond the area of their intended use. 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.

User Accounts

Use of SUNY Geneseo's computer systems and network requires that a user account be issued by the College. Every computer user account issued by SUNY Geneseo is the responsibility of the person in whose name it is issued. College recognized clubs and student organizations may be issued a user account. Faculty advisors shall designate a particular person(s) 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 following will be considered theft of services, and subject to penalties described below.

- Acquiring a username in another person's name;
- Using a username without the explicit permission of the owner and of Computing & Information Technology;
- Allowing one's username to be used by another person without explicit permission of Computing & Information Technology;
- Using former system and access privileges after association with Geneseo has ended.

Resources

The College's information technology resources are, by nature, finite. All members of the college community must recognize that certain 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.

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 resource available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality, and can 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.

Users shall limit incidental personal use. Incidental personal use is an accepted and appropriate benefit of being associated with Geneseo. Appropriate incidental personal use of technology resources does not result in any measurable cost to the college, and benefits the college by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable college policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's college responsibilities, or adversely impact or conflict with activities supporting the mission of the college. Examples of incidental personal use may include, sending a personal email or visiting a non-work-related web site.

Security & Privacy

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 by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users should also be aware that their uses of college computing resources are not private vis-à-vis the college. 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 the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The college may also specifically monitor or inspect the activity and accounts 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:

- The user has voluntarily made them accessible to the public, as by posting to a web page;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of college or other computing resources or to protect the college from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy or any other law or policy;
- An account appears to be engaged in unusual or unusually excessive activity;
- 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 users' files, access or attempt to access other users' email, or modify other users' passwords without their permission. Geneseo computers and networks are designed to protect user privacy; users shall not attempt to circumvent these protections.

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 means of an alias, and may not send messages, mail, or print files that do not show the correct username of the user performing the operation.

Users shall not circumvent or attempt to circumvent security mechanisms or the intent of a system.

Laws and College Policies

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

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

Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain. Occasional personal use of college computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other college responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of college equipment.

Enforcement

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 do so in order 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 in conjunction with the campus Security Administrator and/or relevant campus offices including the Dean of Students, Human Resources, and University Police. Users are expected to cooperate fully in such investigations when requested.

In order to prevent further unauthorized activity during the course of such an investigation, Computing & Information Technology may suspend authorization for 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. Geneseo Student Code of Conduct http://www.geneseo.edu/handbook/policies_procedures#studentcodeofconduct
4. Cyber Citizenship http://www.cybercitizenship.org/index.html
5. New York State Laws and Notices http://www.its.ny.gov/tables/technologypolicyindex.htm
6. New York State Information Technology Policy IT Best Practice Guideline: Acceptable Use of Information Technology (IT) Resources
7. The Digital Millennium Copyright Act http://lcweb.loc.gov/copyright/legislation/dmca.pdf
8. US Code Title 17 http://www4.law.cornell.edu/uscode/17
9. Electronic Frontier Foundation http://www.eff.org/share
10. Respect Copyrights http://www.respectcopyrights.org

Contact

Sue Chichester
CIO and Director, CIT
sue@geneseo.edu

Effective Date: August 1989
Last Updated: December 2019