Acceptable Use Policy

DOCUMENT INFORMATION

Document Title	Acceptable Use Policy
Document Type	☐ Bylaws ☑ Policy Document ☐ Procedures ☐ Guidelines ☐ Form
Office/Unit	Information Technology
Document Owner	
Contact Information	**Office** | **Name** | **Phone** | **Email** Stephen Rieks Associate Vice President of Information Technology / Chief Information Officer
Approval Date	11/9/2016
Approved by	President's Cabinet
Effective Date	11/9/2016
Review Date/Schedule	
Revision History	

DOCUMENT CONTENT

Reason for Policy

Access to information technology is essential to the mission of the State University of New York at Fredonia ("Fredonia") in providing Fredonia students, faculty and staff 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 Fredonia 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.

Policy Statement

To assist and ensure compliance with internal and external acceptable usage standards, Fredonia establishes the following policy which supplements all applicable Federal and State policies, including harassment, patent and copyright, student and employee disciplinary policies, and FERPA, as well as applicable federal and state laws.

Scope

The following document outlines Fredonia's policy on Fredonia-provided access to electronic information, services, computing facilities, and networks.

All creation, processing, communication, distribution, storage, and disposal of information by any combination of Fredonia resources and non-Fredonia resources are covered by this policy.

Technology resources covered by this policy include, without limitation:

- All Fredonia owned, operated, leased or contracted computing, networking, information resources, whether they are individually controlled, shared, standalone or networked,
- All information maintained in any form and in any medium within the Fredonia's computer resources, and Fredonia data networks
- All physical facilities, including all hardware, software, applications, databases, and storage media.

Definitions

Term	Definition
Authentication Credentials	Assigned UserID/Username and PIN/Password {changed by users) that, used in conjunction, authenticates users to privileged computing facilities and resources.
Computing Facilities	All software applications, desktop and mobile computers, networks, and computer peripherals licensed, owned or operated by Fredonia.
e-Services	Fredonia's terminology relating to electronic services such as e-mail, Learning Management System, and electronic library resources.
Internet	All networks external to Fredonia.
Intranet	All networks internal to Fredonia.
Managed	Software and antivirus upgrades being controlled by a server and "pushed" to the desktop or laptop.
Un-managed	A computing device that does not have anti-virus definitions or upgrades implemented automatically. The computer user installs all upgrades manually.
Users	Individuals who make use of Fredonia technology resources. This includes students, faculty and staff, authorized guests, and all persons authorized for access or use privileges by Fredonia including volunteers for local non-profit agencies, scholars visiting from other State University of New York institutions, and the like.

Policy Statement

Users of Fredonia's computing resources must comply with federal and state laws, Fredonia rules and policies, and the terms of applicable contracts including software licenses while using Fredonia 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 Fredonia's computing resources should contact the Chief Information Officer's office for more information.

Users are responsible for ascertaining what authorizations are necessary and such authorizations prior to using Fredonia 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, CPU time, or other limit applicable to all uses of Fredonia's computing resources, Fredonia 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 Fredonia community for any purpose other than those that are in direct support of the academic mission of Fredonia.

User Accounts

Use of Fredonia's computer systems and network requires that a user account be issued by Fredonia. Every computer user account issued by Fredonia is the responsibility of the person in whose name it is issued. Continued use of a previously assigned and previously enabled "@fredonia.edu" email account by an inactive or a transferred student is at the discretion of the Chief Information Office. Such accounts, if re-enabled will not be considered “the ft-of-service”. Fredonia 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 Fredonia's disciplinary procedures for misuse.

The following will be considered theft of services, and subject to penalties described below:

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

Resources

Fredonia's information technology resources are, by nature, finite. All members of the Fredonia community must recognize that certain uses of Fredonia's information technology resources may be limited for reasons related to the capacity or security of Fredonia's information technology systems, or as required for fulfilling Fredonia'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 Fredonia. 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 Fredonia. Appropriate incidental personal use of technology resources does not result in any measurable cost to Fredonia, and benefits Fredonia by allowing personnel to avoid needless inconvenience.

Incidental personal use must adhere to all applicable Fredonia policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's professional responsibilities, or adversely impact or conflict with activities supporting the mission of Fredonia. Examples of incidental personal use may include, sending a personal email or visiting a non-work-related web site.

Security & Privacy

Fredonia employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that Fredonia 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 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.

Fredonia computers and networks are designed to protect user personal privacy and as such, 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.

Computers are Fredonia owned state assets, as such Fredonia retains the inherent right to access these resources either directly or indirectly through remote access tools and techniques at any time.

While Fredonia does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the Fredonia's computing resources may 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. Fredonia may also specifically monitor or inspect the activity and accounts of individual users of Fredonia's computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to a webpage;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of Fredonia or other computing resources or to protect Fredonia 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.

Laws and Fredonia Policies

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

- Users shall comply with all 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 pornography unless written approval has been granted by the Vice President of Academic Affairs / Provost office to accommodate academic research. Research of this nature shall be conducted in an isolated environment approved by the Associate Vice President of Information Technology/ Chief Information Officer.

Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.

Occasional personal use of Fredonia's 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 Fredonia assigned 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 Fredonia's equipment.

Enforcement

Users who violate this policy may be denied access to Fredonia's computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through Fredonia's disciplinary procedures consistent with the terms and conditions of the governing labor agreements (if applicable).

Fredonia 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 Fredonia's or other computing resources or to protect Fredonia from liability.

Fredonia may also refer suspected violations of applicable law to appropriate law enforcement agencies.

When Information Technology Services becomes aware of a possible violation, Information Technology Services will initiate an investigation in conjunction with relevant campus offices including the President's Cabinet members, Human Resources, and University Police in accordance with collective bargaining rights for applicable unions. 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, Information Technology Services may suspend authorization for use of all computing facilities for the user(s) involved in the violation.

Related Documents, Forms, and Tools

1. Information Security Program (Word Doc)
2. Information Management and Cyber Security Policy (PDF)
3. Federal Policies
4. Gramm-Leach-Bliley Act
5. FERPA (Family Educational Rights and Privacy Act)
6. HIPPA (Health Insurance Portability and AccountabilityAct)
7. FISMA (Federal Information Security Management Act)

FAQ's	
Keywords	
Category(s)	☐ Academic Affairs ☐ Advancement ☐ Financial ☐ Governance ☑ ITS ☐ Operational ☐ Personnel ☐ School/College ☐ Student Life
Sub-Category(s)	