Computer and Network Usage Policy

DOCUMENT INFORMATION

Document Title	Computer and Network Usage Policy
Document Type	☐ Bylaws ☑ Policy Document ☐ Procedures ☐ Guidelines ☐ Form
Office/Unit	
Document Owner	
Contact Information	**Office** / **Name** / **Phone** / **Email**
Approval Date	
Approved by	
Effective Date	
Review Date/Schedule	
Revision History	Revised March, 2010 (President's Cabinet) Amended December, 2010 (President's Cabinet)

DOCUMENT CONTENT

Table of Contents

I. Introduction

Access to information technology is essential to the State University of New York's mission of providing the students, faculty and staff of the State University of New York at Fredonia 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 using computing systems and software, internal and external data and networks, as well as access to the World Wide Web, be made available to the SUNY community. The preservation of that privilege for the full community requires that each faculty and staff member, student, and other authorized user comply with institutional and external standards for appropriate use.

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

II. 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, mainframes, desktop and mobile computers, networks, and computer peripherals licensed, owned or operated by Fredonia.
Course list	Refers to special purpose list created (when requested) for communication between students enrolled in a specific course and section and the faculty member teaching the course.
Departmental (Majors) list	Refers to a list created (when requested) for a department to communicate with students in their major.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
e-Services	Fredonia terminology relating to electronic services such as e-mail, ANGEL learning management system, and electronic library resources.
Internet	All networks external to Fredonia.
Intranet	All networks internal to Fredonia.
List conduct	Refers to the behavior of a list subscriber in the context of the list as reflected by the subscriber's postings.
List content	Refers to the theme, topic, or purpose of the list as declared on the list application and/or the theme, topic, or purpose of list postings.
LISTSERV manager	The Information Technology Services' designated manager of the LISTSERV service.
List owner	Refers to a person (other than the LISTSERV manager) who has administrative rights to the list. This may or may not be the list sponsor.
List sponsor	The LISTSERV list applicant (the person who submits the application as designated in item 2) who assumes overall responsibility for and ownership of the list.
Managed	Software and anti-virus upgrades being controlled by a server and “pushed” to the desktop.
Remote Access	Any access to Fredonia's administrative network through a non-Fredonia controlled network, device, or medium.
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 computing facilities. Most users are students, faculty, and staff members of Fredonia. Some users are non-campus personnel authorized by the campus to make use of computing facilities, including volunteers for local non-profit agencies, scholars visiting from other SUNY institutions, and the like.
VPN	Virtual Private Network, a way to extend the corporate/production (trusted) network using authentication and encryption.

III. Authorization and Use

A. Authorized Activities

Fredonia computer facilities are a resource for members of the campus community (faculty, staff, students, and other affiliated individuals or organizations authorized by Fredonia) to be utilized for work consistent with the instructional, research, and administrative goals of the university as defined in the Fredonia “Missions and Goals” statement.

Use by nonaffiliated institutions and organizations shall be in accordance with SUNY Administrative Procedures Manual Policy 007-1: Use of Computer Equipment or Services by Non-affiliated Institutions and Organizations. All who use Fredonia computer facilities have the responsibility to do so in an effective, efficient, ethical, and legal manner, as outlined below.

B. User Accounts

The university grants access to particular computer systems with the assignment of specific user accounts based on educational and business need for access. Every computer user account issued by Fredonia is the responsibility of the person in whose name it is issued. University-recognized clubs and student organizations may be issued a user account. Faculty advisors shall designate a particular person or persons 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 university disciplinary procedures for misuse. The following include, but are not limited to, examples of theft of services, and subject to penalties described in Section IV.

1. Acquiring a username in another person’s name.
2. Using a username without the explicit permission of the owner and of Information Technology Services.
3. Allowing one’s username to be used by another person without explicit permission from Information Technology Services.

C. Password Security

It is mandatory that user accounts be kept secure by using strong passwords, keeping passwords secret, and changing the passwords often. Users must set a password which will protect their account from unauthorized use, and which will not be guessed easily. Avoid selecting easily guessable passwords, for example, nicknames, birthdates, and telephone numbers. Users must report to Information Technology Services any use of a user account without the explicit permissions of the owner and Information Technology Services.

D. User Privacy

Fredonia does not generally monitor or restrict material residing on state-owned or non-state owned electronic devices, whether or not such devices are connected to the campus networks. However, devices that are utilized in violation of Fredonia's policies are subject to investigation and disconnection without notice.

No user should view, copy, alter or destroy another's personal or state-owned electronic files without permission (unless authorized or required to do so by law or regulation). Fredonia computing and network resources are designed to protect user privacy; users shall not attempt to circumvent these protections.

Fredonia reserves the right to access all aspects of its computing and network resources, including individual usage to determine if a user is violating this policy or state or federal laws.

E. System Integrity and Denial of Service

Users shall respect the system integrity of campus computing facilities. For example, users shall not intentionally develop or use programs that infiltrate a computing system, or damage or alter the software components of a computing or network system.

F. Resource Accounting

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, e-mail, or print files that do not show the correct username of the user performing the operation.

G. Resource Usage

Office computer equipment is provided by the institution for academic and business use. All equipment is tagged with Fredonia asset tags and inventoried on a yearly basis. Any information stored, processed, or transmitted by this computer may be monitored, used, or disclosed by authorized personnel, including law enforcement.

Office and lab computing facilities must be used in a responsible and efficient manner. Users shall not develop or use procedures that obstruct authorized use by others. Users shall not interfere with computer setups which are intended to keep computer software current and legal, and shall not install personal software. Users shall not use applications that utilize an unusually high portion of the network bandwidth. Users shall avoid wasting computing resources by excessive game playing or other trivial applications; by sending chain letters or other frivolous or excessive messages locally or over the network; or by printing excessive copies of documents, files, images, or data. Campus printing must pertain to academic work, personal intellectual growth or administrative business.

H. Copyrights and Licenses

Users shall not violate the legal protection provided by copyrights and licenses held by Fredonia. Users shall not make copies of any licensed or copyrighted computer program found on any Fredonia computer or storage device without the written authorization of Information Technology Services. U.S. federal copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution, and integrity to their creations. Works of literature, photographs, music, software, film, and video works can all be copyrighted. Examples of probable violations of copyright laws include, but are not limited to: making unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio, and video recordings); distributing copyrighted materials over computer networks or through other means; resale of data or programs, or the use of them for non-education purposes or for financial gain; or public disclosure of information about programs (e.g., source code) without the owner’s authorization.

I. Restricted Access Systems

Access to selected administrative computers and programs is restricted on a ”need-to-know” basis conforming to SUNY policy guidelines. Unauthorized access or attempted access to these machines or data will constitute theft of services and will be subject to the penalties described in Section IV. Authorization for use of these systems is granted solely by Information Technology Services, on behalf of the institution, and reviewed by the campus Security Administrator.

J. Recreational Use

Recreational use of computing facilities, including computer games and social network communication, is allowed only when no other instructional, research, or administrative function requires the use of resources. Persons using a computer for recreational purposes are required to relinquish the computer immediately to someone needing it for academic or administrative purposes.

K. Termination of Access to Fredonia Computing Facilities

Intentional violation of policies contained in this document will result in immediate termination of access. Access will also be terminated for:

- Students who do not re-enroll for a subsequent semester.
- Graduating students - 90 days after graduation, with the exception of continued access to Google Apps for Education (FredApps).
- Faculty/staff, generally 90-120 days after termination of employment, with the exception of those employees granted emeritus status. Faculty and staff are encouraged to provide updated contact information to all contacts in advance of employment separation.

IV. Limitations on Users' Rights

The issuance of a password or other means of access is to assure appropriate confidentiality of Fredonia files and information and does not guarantee privacy for personal or improper use of university equipment or facilities.

Fredonia provides reasonable security against intrusion and damage to files stored on central facilities. Fredonia also provides some facilities for archiving and retrieving files specified by users and for recovering files after accidental loss of data. However, the university is not responsible for unauthorized access by other users or for loss due to power failure, fire, floods, etc. Fredonia makes no warranties with respect to Internet services, and it specifically assumes no responsibilities for the content of any advice or information received by a user through the use of Fredonia's computer network.

Users should be aware that Fredonia computer systems and networks may be subject to unauthorized access or tampering. In addition, computer records, including e-mail, are considered "records" which may be accessible to the public under the provisions of the New York State Freedom of Information Law.

V. Services

A. Academic/Administrative and Residential (ResNet) Network

1. Anti-virus Protection

Every computer connected to the campus network will be required to run current anti-virus protection software. Campus-provided “managed” anti-virus protection will be placed on the majority of campus-owned personal computers. The campus provides anti-virus protection software for students to utilize. ResNet students may utilize a “managed” or “unmanaged” mode, as owners prefer and as operating systems allow. Non-ResNet student anti-virus protection is un-managed.

It will be the responsibility of “un-managed” clients wishing to use campus network connectivity to keep anti-virus protection up-to-date. This “un-managed” client group would include:

- Campus-owned Macintosh, Linux, and UNIX-based machines
- Non-campus owned computers
- Student-owned computers for those not wishing to utilize the managed anti-virus protection provided by the campus.

In addition, outbound ResNet e-mail will be filtered through a server that will scan and detect viruses.

Information Technology Services and ResNet have the authority to disconnect computers from the network that have been detected as infected. The computer will remain disconnected until the user demonstrates the following: that the machine has been cleaned of viruses/worms; that an appropriate anti-virus product has been licensed for the machine through at least the end of the current academic year; and that the product has been installed and set up to automatically check for and install virus detection updates.

Second and subsequent infractions which result from a lack of an installed, licensed anti-virus product may result in additional penalties.

2. Desktop Upgrades

Every state-owned computer connected to the campus network will have Windows or Macintosh operating systems upgraded or patched by a managed service as applicable.

It will be the responsibility of “un-managed” clients wishing to use the campus network connectivity to keep all operating systems up-to-date.

3. Network Use

Users shall not utilize the campus network to provide Internet access to any outside source, be it commercial or private.

All Resnet (residential) network users must sign off that they have read this Fredonia Computer and Network Usage Policy before they are permitted access to the network.

Actions detrimental or inappropriate when accessing the university and Internet resources include but are not limited to the following:

- Network naming conventions: All student users must use the username assigned by the university ("abcd1234") for the computer name that will be displayed on the network. The description field is required to be left blank.
- Shared connections: A network connection supplied by the university is solely for the use of the individual subscriber assigned to that connection. Connections may not be shared among multiple users. All network subscribers cannot use any mechanisms (either hardware or software) to provide network connectivity to non-subscribers. Users shall not utilize the campus network to provide Internet access to any outside source, be it commercial or private. Users are personally responsible for all use of their computers and network connections and will be held accountable for any violations that occur involving their computer or network connections.
- Network infrastructure: All adds, moves, and changes of network infrastructure electronics including but not limited to products such as repeaters, hubs, concentrators, bridges, routers, and switches must be coordinated and installed by university personnel. This includes all cabling that is patched into these devices that provide connectivity. Users are prohibited from connecting to any device such as a hub, router, switch, or wireless access point to the provided Ethernet jacks in the room to extend connectivity. For example, a user may not use a hub in their room or office to allow them to connect more than two devices to the network at a time.
- Assigned IP address: Alterations of any kind to the assigned IP address or related settings, including using an unauthorized IP address, is prohibited. ResNet IP addresses are assigned dynamically and users are not permitted to configure static IP addresses, DNS address, etc.
- File Sharing: Users are responsible for the security of the system. All student shared files must be password protected. If a user mis-configures the file sharing, others may be able to affect and alter the user's computer. Users are responsible for the content of files that they distribute. Current laws may permit users to be sued for libel, invasion of privacy, software piracy, pornography, and other such crimes. Fredonia is not responsible for any loss of data that may occur if users choose to activate file sharing.
- Copyright: Distribution of copyrighted materials such as computer software and music is normally prohibited, except where a portion of copyrighted material may be part of the public domain. In accordance with the Digital Millennium Copyright Act (DMCA) and with HR4137 "An Act to amend and extend the Higher Education Act of 1965 (HEOA), university policy forbids the copying, distribution, downloading, and uploading of copyrighted materials on any personal or College computer system or network. These materials include, but are not limited to, text (including emails and web information), graphics, art, photographs, music, film, and software. Violators of the Digital Millennium Copyright Act who have illegally shared copyrighted files are subject to civil penalties of between $750 and $150,000 per song. In the past, pre-litigation settlements offered by copyright owners have ranged from $3,000 to $4,000 and up. Additionally, a court may, in its discretion, grant the copyright owner reasonable attorney fees. 17 USC § 506 lays out criminal penalties for intentional copyright infringement which can include fines and jail time. Refer to http://www.fredonia.edu/its/DMCA.asp for Fredonia DMCA procedures.
- Monetary gain: Network access for monetary gain or for business activities of groups or organizations is prohibited. Re-sale of access or services is prohibited.
- Domain registration: The registration of commercial hostnames to a Network IP address is prohibited.
- Servers: Establishing a server or providing a service that over-utilizes the shared bandwidth is prohibited. FTP, Web servers, e-mail servers, and Peer-to-peer are examples of server programs.
- Port Scanning: Scanning for computers on any network using port scanners or network probing software including packet sniffers, is prohibited.

The university networks are monitored and violators of Fredonia policy will be denied service and referred to the proper authority, as noted in Section V of this policy.

4. Wireless Network

The wireless network is not meant as a replacement for the wired network and is not to be used as a primary network connection. The wireless network is meant to extend the wired network for simple uses in areas where wired network access is unavailable. Users are expected to avoid using applications that will use large amounts of network bandwidth. These include servers and file-sharing applications. Users should be aware that Fredonia does not utilize 802.11b/g/n encryption standards on the campus wireless network (i.e. WEP, WPA, WPA2).

There are other electronic devices that use the same 2.4GHz frequency as the Fredonia wireless network. Devices include 2.4GHz cordless phones, microwave ovens, X10 wireless cameras, Bluetooth devices, and other wireless LAN equipment. Devices using this technology can cause intermittent failure and loss of service.

The following policies are in addition to the Fredonia campus network usage policies. Actions detrimental or inappropriate when accessing the university and Internet resources include but are not limited to those listed below.

- Users may not extend or modify the network in any way. This includes adding access points and installing bridges, switches, hubs, or repeaters. The university reserves the right to remove or disable any unauthorized access points.
- Users will be responsible for all costs associated with purchase, installation, operation, and support of wireless adapters in client computers.
- Any attempt to break into or gain unauthorized access to any computers or systems from a wireless connection is prohibited.
- Running any unauthorized data packet collection programs on the wireless network is prohibited. Such practices are a violation of privacy and constitute the theft of user data.
- The institution has the right to limit bandwidth on a per connection basis on the wireless network, as necessary, to ensure network reliability and fair sharing of network resources for all wireless users.
- Any effort to circumvent the security systems designed to prevent unauthorized access to any Fredonia wireless network may result in the suspension of all access and an appearance before the appropriate disciplinary board.
- For more information regarding the campus wireless network including recommended computing habits and wireless coverage on campus please visit the following website: http://www.fredonia.edu/its/Networking/Wireless/

B. Electronic Mail

1. University Use of Electronic Mail

Electronic mail (e-mail) is a mechanism for official communication for Fredonia. The university expects that such communications will be received and read in a timely fashion.

2. Official University E-mail Accounts

An official university e-mail account is one in which the address ends with "fredonia.edu." All students, faculty, staff, and departments are assigned an e-mail address and account. The e-mail address is directory information. As with other directory information, in compliance with federal Family Education Rights and Privacy Act (FERPA) regulations, any student may request that his or her official e-mail address be restricted in its access. Departmental account forwarding to individuals or groups is the responsibiliity of each department.

3. Expectations For Use of E-mail

Students, faculty, and staff have the responsibility to use this e-mail in an efficient, effective, respectful, ethical and lawful manner. Students, faculty, and staff are expected to check their e-mail on a frequent and consistent basis in order to stay current with university-related communications. Unit heads that have exempted employees from the requirement of having an official e-mail account must make arrangements for alternative methods of access to official communications. Students have the responsibility to recognize that certain communications may be time-critical. “I didn’t check my e-mail”, error in forwarding mail, or e-mail returned to the university with “Mailbox Full” or “User Unknown,” are not acceptable excuses for missing official university communications via e-mail.

4. Redirecting of E-mail

If a student, faculty, or staff member wishes to redirect e-mail from their official @fredonia.edu address to another e-mail address (e.g., @aol.com, @hotmail.com), they may do so, but at their own initiative and risk. The university will not be responsible for the handling of e-mail by non-Fredonia providers. Redirecting e-mail does not absolve students, faculty, or staff from the responsibilities associated with official communication sent to their @fredonia.edu account.

5. Authentication for Confidential Information

It is a violation of university policies, including the Student Code of Conduct, for any user of official e-mail addresses to impersonate a university office, faculty/staff member, or student. To minimize this risk, some confidential information may be made available only through Your Connection which is password protected. In these cases, students will receive e-mail correspondence directing them to Your Connection, where they can access the confidential information by supplying their FredoniaID and PIN. The confidential information will not be available in the e-mail message.

6. Privacy

Users should exercise extreme caution in using e-mail to communicate confidential or sensitive matters, and should not assume that e-mail is private and confidential. It is especially important that users are careful to send messages only to the intended recipient(s). Particular care should be taken when using the “reply” command during e-mail correspondence.

7. Educational and Administrative Uses of E-mail

Faculty will determine how electronic forms of communication (e.g., e-mail, discussion boards, etc.) will be used in their classes, and will specify their requirements in the course syllabus. The official e-mail policy ensures that all students will be able to comply with e-mail-based course requirements specified by faculty. Faculty can therefore make the assumption that students’ official @fredonia.edu accounts are being accessed and faculty can use e-mail for their classes accordingly.

Administrative offices will determine how e-mail communications will be used for administrative purposes.

8. University Announcements

Approval and transmission of e-mail containing essential university announcements to students, faculty and staff must be obtained from the appropriate authority. Only the offices of vice presidents or the university president can authorize the sending of broadcast messages to a wide audience of students, faculty, and staff. Mass mailing communications to external Fredonia.edu audiences must be accomplished utilizing an appropriately identified third-party service to mitigate the placement of fredonia.edu e-mail servers on spam blacklists.

9. Ownership/Administration

Fredonia owns all e-mail accounts run on its domain. Under certain circumstances it may be necessary for the Information Technology Services staff or other appropriate university officials to access e-mail files to maintain the system, and to investigate security or abuse incidents or violations of other institutional policies. Such access will be on an as-needed basis and any e-mail accessed will be disclosed only to those individuals with a need to know or as required by law. While incidental non-business personal use of e-mail is acceptable, conducting business for profit using university resources is forbidden. Quota, maximum message size, message retention settings, time-out settings, maintenance times, and other e-mail guidelines will be set as appropriate for the anticipated volume and platform scaling. The need to revise settings will be monitored with recommended changes as appropriate. (See e-mail guidelines at http://www.fredonia.edu/its/servicecenter/email.)

10. Termination

E-mail accounts are provided to students and continued when they reach alumni status. Email accounts are provided to faculty and staff as a component of electronic services while employed. See Section III K. of this policy. In certain cases, employee e-mail accounts may be continued for a longer period or forwarded for appropriate business conclusions.

11. Violations/Abuses

Violation or abuse of the policy may result in restriction of access to Fredonia’s e-mail system and/or other appropriate disciplinary action.

C. LISTSERVs

1. Establishing a LISTSERV List

- List content must reasonably reflect the responsibilities, field of expertise, research, or study of the list sponsor as it relates to his/her function at the university.
- List sponsors and owners are expected to abide by all computing resource usage policies put forth by Fredonia.

2. List Sponsorship/Ownership

- Only permanent faculty/staff of the university may sponsor a list.
- List owners are responsible for adequately communicating to the list membership (usually in the form of a charter/welcome message sent to all new subscribers) the guidelines for list posting. Owners should also ensure that their subscribers are aware of certain important list configuration settings (e.g., who can post, who can subscribe, etc.).
- List owners are responsible for ensuring appropriate membership, as related to university functions.
- List owners are responsible for updating the subscriber list and removing or suspending invalid or problematic addresses.
- Institutional lists (i.e. announcements, news, proftalk) will be maintained by the Information Technology Services LISTSERV manager.

3. List Content and Copyright

- List subscribers, owners, and all others with list posting privileges are expected to observe all applicable copyright restrictions when posting any material that is not their own. The use of a mailing list to distribute any material (including binary files) in violation of copyright or licensing is strictly prohibited.

4. List Expiration and Renewal

- All lists, except for class lists, expire on a yearly basis at the end of each spring semester (the week after the end of final exams). Class lists expire at the end of each semester (the week after the end of final exams). Lists that are less than three (3) months old at the time of expiration will not expire until the end of following semester or academic year, whichever applies.
- All list owners will be notified by e-mail at least four weeks prior to the expiration date. In order to renew a list, the list owner must reply to the notification stating his/her intent to renew the list.
- If after two expiration notices the list owner has not declared intent to renew, the list will be deleted.

5. List Removal and Deletion

- A list may be deleted at any time by the LISTSERV manager at the request of the list sponsor.
- Information Technology Services reserves the right to delete lists that: (1) are misused; (2) do not comply with established policy; (3) pose a threat to system security or integrity. In such cases, the LISTSERV manager will attempt to notify the list sponsor and/or primary owner prior to the deletion of the list.

6. Information Technology Services' Rights

- Information Technology Services provides LISTSERV mailing lists as a service to the university community. As such, Information Technology Services reserves the right to make alterations in the service at any time for the sake of the common good of all users.
- The LISTSERV manager reserves the right to make changes to any list's configuration without notice in the following cases (not exhaustive): (1) to correct errors; (2) to make preferred changes or improvements; (3) where the list owner has been negligent or lax in conducting required list maintenance.

- The LISTSERV manager reserves the right to restrict or deny any user's access to or privileges on LISTSERV with due cause. The LISTSERV software may automatically and selectively deny service to users based on bounced or excessive e-mail or other detected problems.

D. The University Website

1. The University Website and Use of the Web Servers

- The Fredonia website, which begins at the home page www.fredonia.edu is a volume of documents on several servers created by diverse authors which, as linked, represents the university as an official publication.
- All departmental or student group web pages are part of the official university website, and are screened, monitored, coordinated, supervised, and controlled by the university webmaster, who retains the right to edit the pages.
- All official university web pages must be designed to meet standards of technology or content set by the university webmaster or any overriding authority such as SUNY or New York State.
- All authorized users of the web servers (for official or personal pages) will be restricted to 7 megabytes of hard drive space per folder, and all space is to be dedicated to web page use only. The university may allow authorized individuals more than 7 megabytes of space if a legitimate academic need is described to the webmaster. No personal file storage or other file activity is permitted on the web servers.
- When notified that they are exceeding the 7-megabyte limit, authorized users must delete a necessary amount of material in a time period specified by the webmaster or risk deletion of all files.
- Except that access is gained by request, web server and website user responsibilities and access policies are the same as those under Sections III, IV, and VI of this document.
- All personal and official web pages will be free of content articulated in Sections I and II of this document, in addition to pornography, hate speech, and non-university sponsored e-commerce.
- Any official or personal web pages that employ technological features beyond HTML, Java, JavaScript, client-side VBScript and CSS must be submitted for review and approval to the university webmaster.
- Web pages using applications such as ASP must be submitted for review and approval by the university webmaster.
- World-wide write access is prohibited on any personal or official page.
- When a violation of these policies occurs, Fredonia reserves the right to remove any and all contents in any files or folders on the web server without advance notice or consultation, and to revoke server permissions to any authorized user.
- Incidences of violations found by the webmaster may be reported to appropriate university authorities.

All university-based groups (including student groups) who select external web developers will be responsible for overseeing and maintaining quality control procedures and meeting the standards of technology and content set by the university webmaster or any overriding authority such as SUNY or New York State. External developers, with no current, formal or direct affiliation with the university, will not be authorized to possess individual accounts on the university's web servers.

All departments or student groups who choose to have an external developer work on their web pages must contact the ITS Service Center prior to commencing work.

All web pages, images or files that are located on the university web servers must be maintained and updated to reflect current and accurate content. In no instances should the web servers be utilized for storage or archiving purposes. Files that are no longer active or current must be removed from the university web servers periodically, upon the request of the university webmaster, or risk removal as deemed appropriate by the webmaster. The webmaster will periodically remind the campus community to purge its web server directories of all inappropriate or out-of-date files.

Web publishers are responsible for the content of the pages they publish on the university web server and are expected to abide by the highest standards of quality and responsibility. Content must be relevant to the university. Web authors and publishers are required to comply with all Fredonia university policies, as well as all local, state, and federal laws concerning appropriate use of computers and the Internet. Departmental web pages must conform to the design standards set forth by the university. See Guidelines for Developing and Publishing New Web Pages located at: http://www.fredonia.edu/pr/web/guidelines.asp

The purpose of the web page is to provide information to students and colleagues and must contain the following as a minimum:

- All TITLE tags located within html files must use the following format to foster consistency, clear page identification, and increase rankings in search engines:

TITLE FORMAT: Page Title – Departmental Name, The State University of New York at Fredonia

Example: <TITLE>Electronic Journals, Daniel A. Reed Library, The State University of New York at

Fredonia</TITLE>

- All web pages must include the university name “The State University of New York at Fredonia.” Rationale: This will help identify the location if the user has entered the website without going through the home page.

- All pages must include a link back to the Fredonia home page (http://www.fredonia.edu).

In no instances should file names include spaces. Hyphens (-), underscores (_), alpha and numbers 0-9 are permissible.

Correct Examples: FileName.html Incorrect Example: File Name.html

File-Name.html

File_Name.html

All web pages must meet the minimum web accessibility requirements as set forth under Section 508 of the Rehabilitation Act, and mandated by the New York State Office for Technology Policy 99-3. This policy requires that all New York State agencies' websites provide universal accessibility to persons with disabilities.

All pages must include the following Meta tags for searching and identification purposes. If assistance is required, the following code example should be used (copy and paste the code below) and all underlined information replaced with keywords and a description that are specific to the web page being created.

<HEAD>

<META CONTENT="Include important keywords from your web page here (i.e., public, higher education, Fredonia, America's Best Colleges, Blue Devils, music, liberal arts, Chautauqua County)"><META CONTENT="Include a brief description of your web page here (i.e., Fredonia is a four-year comprehensive, public, liberal arts university in the Northern U.S., known for bachelor's degree programs in music and education, and named one of America's Best Colleges)">

</HEAD>

The university will host websites for non-university, non-profit organizations as long as their function is relevant to the overall university mission, and as long as there is an active member of the Fredonia campus community (faculty or staff holding a current appointment) who will serve as the sponsor for that website. Sponsors will be issued a special group account that may be used by the web developer, and sponsors will be responsible for maintaining and monitoring the organization's web pages. All new websites or web pages must be submitted by the sponsor for review and approval to the university webmaster prior to uploading to the university servers. Sponsors must also notify the university webmaster any time the content on any of the pages has been modified. These non-campus-hosted websites must comply with all the policies that are required of official university web pages. The university webmaster reserves the right to edit content and revoke server permissions to any authorized user who does not abide by the policies set forth by Fredonia.

2. Personal Web Pages

Users may create their own homepages. Faculty and students will have FTP (File Transfer Protocol) access to a personal directory on the university server where they can maintain their own homepage files. Under no circumstances should personal space and/or files be shared with other users. In designing a personal homepage, persons should keep in mind that homepages may not be used for personal profit, nor to violate copyright, pornography or any other state or federal laws. The university reserves the right to monitor all work on the server and remove any personal homepage or files it determines have violated any of the policies. In addition, failure to comply with computing policies could, in some cases, lead to disciplinary action or criminal prosecution.

3. Blog and Forum Standards on Fredonia's website

Fredonia Website Services provides server space and forum and web log or blog services in support of scholarly, academic, extra-curricular and professional communications conducted by members of the university community who have network accounts. Standards for posting behavior:

- Content should be free of vulgar, racist, sexist, homophobic, or otherwise objectionable matter, including personal attacks against named individuals.
- Posts should stay on-topic and be faithful to the theme or purpose of the blog or forum.
- The following statement must appear on all blog and forum pages: “The views and opinions expressed in this page are strictly those of the page author(s). The contents of this page have not been reviewed or approved by the State University of New York at Fredonia.”
- Fredonia reserves the right to require blog and forum administrators to use university-approved templates for all hosted pages.
- When blog and forum content violates university website policy or local, state, or federal law, Fredonia reserves the right to remove such content or the blog or forum module itself. Fredonia also reserves the right to do the same at its sole discretion when it is judged appropriate to do so.

4. Additional Web Design Standards for Official Fredonia websites

In addition to accessibility requirements and all other web policies from Sections V.D.1, V.D.2, and V.D.3 of this document, all official Fredonia web sites, i.e., colleges, schools, academic and administrative departments, are also subject to the following layout standards intended to maintain site-wide navigation and design consistency:

a. All official Fredonia web sites must use an approved web design template.

The source code for approved web templates is available at: http://www.fredonia.edu/templates/global_files.zip (900KB) A sample template site is available at: http://www.fredonia.edu/templates/global_files/sample_site/

b. The global top navigation bar must appear at the top of all official Fredonia web pages. The source code for the global top nav bar is available at: http://www.fredonia.edu/templates/global_files/topnavbar/topnavbar_inc.asp

The global top nav bar also requires an accompanying CSS file:

http://www.fredonia.edu/templates/global_files/topnavbar/topnavbar.css As a best practice, the topnavbar.css CSS and topnavbar_inc.asp files should be linked dynamically to every web page. Using an ASP virtual #include function, the topnavbar_inc.asp file is linked within the <BODY> block of every web page, prior to other elements: <!-- #include virtual="/templates/global_files/topnavbar/topnavbar_inc.asp" --> The CSS file is linked within the <HEAD> block of every web page: <link href="http://www.fredonia.edu/templates/global_files/topnavbar/topnavbar.css" rel="stylesheet"> When the top navigation bar is included this way then any changes made to the top navigation bar's code will be reflected immediately on every page of the web site.

Requests for Exemptions:

Academic or administrative departments requesting exemptions to the above design and navigation standards for official Fredonia web sites are asked to mail or email their request to: Chair, Web Steering Committee c/o Webmaster, Foundation House, 272 Central Ave., Fredonia, NY 14063, ph.716-673-3323 webcontent@fredonia.edu The Web Steering Committee will review the request and forward its recommendations to ITAB for review and consideration. At minimum, the global top navigation bar (see Section V.D.4.b of this document) is required for all official university pages, unless technical issues prevent its inclusion.

E. ANGEL Learning Management System

- ANGEL policy will address items not already covered by another policy or regulation.
- Access defaults should mirror Banner data accessibility rules:
  - Faculty can see profile data (address, phone number) for students in their classes.
  - Students can see profile data for faculty.
  - Directory information will be available to authenticated users.
  - Students who request confidentiality of directory information via the Registrar will be granted confidentiality in ANGEL and indicated as confidential to faculty.
  - Banner data determines ANGEL course enrollments with a nightly add/drop. Accounts and Roster entries are added nightly. Drops and withdrawals are marked as “disabled” in the ANGEL course roster. There will be no self-enrollment for students in courses. Faculty may allow access to others at their discretion. Courses are searchable and accessible to students upon creation.
  - Undergraduate students are not authorized to access the ANGEL gradebook. This item is currently under review and will be audited until a final decision is made.
  - Students will be allowed the role of Group Leader and will be able to request a group be made for online collaboration from any Fredonia employee who agrees to sponsor their online group. Student Group Leaders can add members to the group if they know the Fredonia e-mail address of the potential member. They will not be able to list ANGEL accounts or educational records. They will only see directory information.
  - Librarians will have access to courses for those who request reserve materials. Reserve readings will be published to ANGEL courses regardless of whether the instructor uses ANGEL for the class. Permission is granted to library staff by the instructor via the reserve request form.
  - Campus members may submit public items (news, events, forums, polls, surveys) to the ANGEL Administrator to post in Public Areas of ANGEL. Items will be selected based on their academic nature and relevance to a general student audience. Policy for increased access to public components is being developed.
  - Fredonia ID photos will be added to ANGEL to allow instructors to view photos of students enrolled in their classes. Target: Spring 2007
  - Campus members may request guest ANGEL accounts by e-mailing the ANGEL Administrator. This item is being reviewed by the Electronic Services Group.
  - At this time, there are no plans to delete ANGEL accounts. When students graduate, their accounts will be disabled and categorized as ALUMNI. These accounts may be activated as part of the Eportfolio implementation. Employees who leave and students who don’t return will also be disabled and categorized as EX.
  - Groups will automatically be created for Departments and Advisors based on Banner data. (Target: Spring 2007)
  - Data purge policies are under development.

F. Virtual Private Network (VPN)

Fredonia Information Technology Services provides a Virtual Private Network (VPN) primarily for Information Technology Services staff to remotely and securely monitor and administer systems as necessary. The following standards are designed to minimize the potential exposure to Fredonia from damages, which may result from unauthorized use of Fredonia resources. Damages include the loss of sensitive or university confidential data, intellectual property, damage to public image, damage to critical Fredonia internal systems, etc.

Limited VPN use is provided for employee administrative access to confidential databases when remote work-related business is absolutely necessary, and when the employee has Cabinet- level approval for such access. Employees with VPN privileges understand and agree to the following:

- It is their responsibility to select, coordinate installation of, and pay associated fees for high-speed connectivity (DSL) through an Internet Service Provider (ISP).
- It is their responsibility to ensure that unauthorized users are not allowed access to Fredonia internal networks via their VPN.
- VPN use is controlled using password authentication.
- VPN gateways will be set up and managed by Fredonia ITS, and only ITS-approved VPN clients may be used.
- By using VPN technology with personal equipment, users understand that their machines are a de facto extension of Fredonia's network, and as such are subject to the same rules and regulations that apply to Fredonia-owned equipment, i.e., their machines must be configured to comply with all Fredonia Security Policies, including the latest operation system security patches and anti-virus software definitions.
- Desktop support and connectivity issues related to VPN access are provided by Information Technology Services on state-owned equipment only.

VI. Unauthorized Use

Violation of these regulations is unethical and may constitute a criminal offense.

Offenses will be dealt with according to any or all of the following: applicable federal laws, Chapters 156 and 165.15 of the New York State Penal Law; the Fredonia "Student Rights and Responsibilities;" other laws, regulations, and policies of the campus, the State University of New York, the State of New York and the United States of America. Offenses may result in the suspension or permanent closing of usernames, campus disciplinary action, legal action and/or other action.

When Information Technology Services or the Residential Network (ResNet) Office becomes aware of a possible violation, the university will initiate an investigation in conjunction with the campus Security Administrator and/or relevant campus offices including the Office of Student Affairs, Human Resources Office, 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, Information Technology Services may suspend authorization for use of all computing facilities for the user(s) involved in the violation. ResNet reserves the right to temporarily suspend a user’s Internet connection pending the outcome of any required Administrative Sanction Hearing.

The following include, but are not limited to, examples of unauthorized use.

A. Academic Dishonesty

Practicing any form of dishonesty through use of computing facilities (for example, cheating, plagiarism, or fraud) is prohibited.

B. Harassment

Using computers or networks to harass, abuse or intimidate another person is prohibited. Users shall not develop or use programs that harass other users. Users shall be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages that could create an atmosphere of discomfort or harassment for others.

C. Obscenity

Obscene language in electronic mail, messages, process names, file names, file data, and other publicly visible forms is prohibited.

D. Child Pornography

Federal Child Pornography Law makes it illegal to create, possess, or distribute graphic depiction of minors engaged in sexual activity, including computer graphics. Computers storing such information can be seized as evidence.

E. Pornography

Pornography in electronic mail, file data, web sites, and other publicly visible forms, is prohibited.

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