COMPUTER NETWORKS ACCEPTABLE USE GUIDELINES

Responsibilities of All Hofstra Computer and Network Users
Access and use of computing and networking resources at Hofstra University are privileges extended to members of the Hofstra community. Access to Hofstra computing and networking resources is limited to authorized users and is for approved purposes only. "Authorized users" is defined as "any member of the Hofstra community who is issued a Hofstra ID card, and CCEPA faculty and students." "Approved purposes" are those consistent with the law, Hofstra policies, and the broad instructional, administrative and research mission of Hofstra University, and the user's relationship with the University. For the purposes of this policy, sensitive information is defined as all information protected by all applicable laws, including, but not limited to, FERPA, Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA), as well as information that is considered confidential to the University's operations.

Hofstra University computer and network resources include, but are not limited to: the computers, printers, networks, online and offline storage media and related equipment, software and data files that are owned, managed or maintained by Hofstra University, as well as all networks reached via this campus-wide network, such as the Internet. Also included are any specialized computer resources or services that other Hofstra schools have implemented for the use of their department and/or academic discipline.

Use of Hofstra computing resources, even when carried out on a privately owned computer that is not managed or maintained by Hofstra University, is governed by this policy.

Hofstra University's Computer Center provides data network services [known as the HOFSTRA NETWORK] for all organizations within the University. The Computer Center provides centralized computer-related services for instruction, administration and research. Other Hofstra schools may have specialized resources for the use of their department and/or academic discipline.

Each holder of a Hofstra Network account, or of any school or departmental account permitting network access, has the responsibility to use resources referred to above in an ethical and legal manner and agrees to the following as a condition for the use of the account:

- I understand that my access to Hofstra's computing resources and network is for the sole purpose of facilitating my work as a University student, staff member or faculty member.
- I will respect the privacy and reasonable preferences of other users (both at Hofstra and elsewhere on all connected networks), including the privacy of their accounts and data.
- I will respect the integrity and security of the systems and network, and will exercise care to maintain their security.
- I understand that computer accounts are for sole use by the account owner, and I will not share my account with other individuals or use an account assigned to another individual.

- I will take precautions to safeguard passwords and other privileged information to which I have been given access. Any passwords, verification codes or electronic signature codes assigned to me are for my individual use only. I will regard them as personal identifiers of my computer use, similar to my signature on a document.
- I understand that I am responsible for all actions performed from my computer account.
- I will not attempt to monitor other individuals' computer or network use, nor will I attempt to obtain their passwords or any other private information.
- I understand that, in the course of my work, I may be given or otherwise gain, access to confidential or privileged information relating to this or other institutions, or to Hofstra students, employees, or other individuals or groups. I will respect the confidentiality of all information to which I have access, neither divulging confidential information without appropriate consent nor seeking to obtain access to confidential information to which I am not entitled.
- I will not make unauthorized copies of software, or perform unauthorized installations of software or reconfigurations of systems. And any receipt, transmission, use or destruction of software or data must observe U.S. copyright laws, and license restrictions.
- I understand that accessing, altering or destroying any document, file or University records that I do not own or have rights to, is a violation of these policies.
- I understand that my use of computing resources accessed via the Hofstra Network – whether provided by organizations within or outside the University – may be subject to additional norms of behavior or regulations specific to the resource, which I agree to follow.
- I understand that my account is intended for the sole purpose of facilitating my research, educational, clinical, administrative, or other authorized goals. I may not use the Hofstra University computer resources to solicit sales, conduct business, download/share copyrighted materials, advertise or sell a service, or use the system for any illegal activities. This applies to the use or application of any University resources, such as, but not limited to, Internet access or e-mail through my personal computer.
- I understand that the Hofstra Computer Center must authorize connecting a personal computer or device to the Hofstra University Network.
- I may not engage in activities that damage or disrupt communications, hardware devices or software applications, such as but not limited to, virus creation and propagation, circumventing system protection mechanisms, playing games in the labs and/or overloading the network with excessive data.
- I understand that while I am a student, I have an advertisement-free Hofstra Gmail account with the use of Google Applications. I also understand that once I am no longer a student, I will retain my Hofstra Gmail account, and advertisements will be included in the service. I agree I will abide by these guidelines and any updates posted at www.hofstra.edu/SCS/aug.
- I will not perform unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing. I understand that performing such unauthorized distribution may subject me to civil and criminal liability.

ACCEPTABLE USE OF THE HOFSTRA NETWORK

Use of Hofstra University computing resources by unauthorized individuals is strictly prohibited. Although the University does not as a matter of policy monitor the system for content, you should be aware that in special circumstances and for limited purposes, the University may examine certain files and archives. In addition, the University may be compelled to respond to subpoenas and other legal demands for information about system usage. Therefore, users should not have an expectation of complete privacy.

Please also be advised that the University requires compliance with applicable federal, state and local laws, including copyright, export and re-export laws, as a condition to system use. Except as expressly permitted, users shall not alter, delete or modify any attributions included within any hosted services. Users further agree not to engage in any activity that interferes with or disrupts the services, servers or networks provided. Google e-mail account users shall comply with the terms and conditions set forth by Google in connection with those e-mail services.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq

The programs you can access on the Hofstra network may contain CONFIDENTIAL information protected by various federal, state and local laws including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), the Financial Services Modernization Act of 1999 (Gramm Leach Bliley), Health Insurance Portability & Accountability Act (HIPAA), and the New York Education Laws. All users are cautioned to take appropriate measures to protect the privacy and integrity of this information and to refrain from engaging in any misuse or unauthorized disclosure of this information.

POLICY VIOLATIONS
Violators of the policies outlined in this document or in addenda at the *Hofstra University Acceptable Use for Computing Policy* Web site, www.hofstra.edu/scs/aug, may find their network access disabled, with no prior warning, until sufficient safeguards have been put in place to ensure that no further violations occur.

The University reserves the right to disconnect individual machines or sub-networks of the HOFSTRA NETWORK in order to preserve the smooth functioning and security of the network as a whole.

It is the responsibility of all network users to accept full responsibility for use of their accounts and machines. Users of the Hofstra Network agree to preserve their sole individual use of their accounts by not sharing them with other individuals, by maintaining secret passwords, by changing passwords frequently, and by selecting passwords that are difficult to guess or decrypt.

PROCEDURES FOR POLICY VIOLATIONS
Violations include, but are not limited to:
- Sharing network IDs and passwords (providing unauthorized use of network services)
- Chain e-mail or hoaxes
- Harassment of others using electronic communication systems (cyber bullying)
- Tapping phone or network transmissions
- Software piracy
- Privacy violations
- Sharing copyrighted materials
- E-mail bombing or spamming
- Commercial use of University resources
- Illegal activities as set forth in federal, state and local laws and statutes

Violations of the *Acceptable Use Guidelines* will be adjudicated, as appropriate, by Public Safety, Residential Programs, Student Computing Services or the Office of Community Standards.

Sanctions as a result of major violations may result in any or all of the following:
- Loss of Hofstra University computing privileges
- Disconnection from the HOFSTRA NETWORK
- University sanctions as outlined in the *Code of Community Standards*
- Monetary reimbursement or other appropriate fines
- Prosecution under applicable civil or criminal laws

Major violations include:
- Second offense of a minor violation (listed below)
- Hacking or attempting to circumvent security on another computer
- Cracking or attempting to violate security on copyrighted materials
- Intentional computer virus/worm propagation
- Distribution or soliciting copyrighted materials

- Electronic harassment of any kind, including but not limited to voice, email, electronic chats, instant messaging, Web pages, etc.
- Using network resources to solicit sales, conduct business or advertise a service
- Any violation of federal, state and/or local laws using Hofstra University computer network or telecommunication systems

Minor violations include:
- High bandwidth utilization
- Abuse of University bandwidth and resources
- Port scanning
- Unintentional virus/worm propagation
- Sending unsolicited e-mail
- Internally recognized file server

Disclaimer:
Hofstra University is not responsible for any loss of data or damage to hardware or software on your personal systems at home, in the residence halls or public access computer labs on campus.

Hofstra University believes in the user's rights to privacy; however, when there is sufficient evidence of wrongdoing, the University reserves the right to examine and impound any files, information or computer system(s) resident or attached to the Hofstra University network.

All persons accessing Hofstra University computing resources will be held accountable for their conduct. Conduct that involves the use of University resources in an inappropriate manner or that violates another person's rights may result in revocation of computing usage privileges and is subject to University disciplinary action as outlined in the University's policies and the *Code of Community Standards* as outlined in the *Guide to Pride*.

Such conduct may also be subject to criminal or civil legal action. Any abuse or violation of the rules outlined here (or of other rules and practices governing the use of computer networks to which Hofstra is attached) will lead to account suspension and immediate review, with the possibility of account revocation, further disciplinary action in accordance with Hofstra University rules and procedures, and referral to local, state and federal law enforcement authorities.

As a matter of routine, use of Hofstra computer systems and the Hofstra Network is monitored and recorded by authorized University staff members in order to safeguard the security and smooth operation of these resources. These privileges and further clarifications are continuously reviewed and amended. The latest updates to this document are available at www.hofstra.edu/scs/aug.

Network Account Specific Policies and Information
Network accounts are intended to provide members of the Hofstra University community of students, staff, and faculty with basic access to Hofstra University Network academic and

administrative software applications and Internet services, including electronic mail (Hofstra Gmail), Google Applications, the my.Hofstra.edu portal and other information services via World-Wide Web. Your account provides a set of the most popular software tools for these purposes, and Student Computing Services offers documentation, classes, and staff assistance to help you with their use.

Password
Each user of the system is assigned a unique login ID. We suggest that users change passwords every six months in order to maintain high security on the system. However, it is each account holder's responsibility to change the password and to not reveal it to other individuals. Passwords must conform to Hofstra University's strong password policy. For additional information visit http://www.hofstra.edu/scs/password/.

Limitations of the Hofstra Network Account
In order to provide the best possible service to the large community of Hofstra University Network users, the following limitations have been placed on the configuration and use of each Hofstra Network account:

- Network accounts are intended solely for the account holder's access to resources on the Hofstra University Network and their e-mail. Users of the network must therefore agree that, under no circumstance, will they allow other individuals to access these resources via their accounts. Furthermore, you will not provide to others Hofstra University Network access to information services via your computer system.
- A uniform quota of system disk space is allotted to each user to hold account configuration files, Web site files, personal files and electronic mail; individual disk quotas cannot be changed.
- Hofstra University's intention is to provide a uniform set of tools that are of interest to all users of the Hofstra University Network system. Users may not install additional application software or utilities in their Hofstra University Network disk space, whether for their own or others' use.
- Network accounts will be deactivated and removed upon graduation, or if an account holder's affiliation with Hofstra University ends.
- Hofstra Gmail and Google Application accounts will remain with the student once the student has graduated or is no longer a student. Once the student has graduated or leaves the University, their Hofstra Gmail account and Google Applications will receive the standard Google advertisements.
- Your Hofstra Network connection is for the use of the account holder or account holders in the case of roommates. Under no circumstance will you allow other individuals to access the HOFSTRA NETWORK via your account.
- Users are not to run any services (i.e., Web servers, HTTP servers, file servers, DNS servers, DHCP servers, FTP services, list servers, publish MP3/4s, publish files via generic file services, etc.) via this HOFSTRA NETWORK connection. This connection is not for commercial use (including, but not limited to nonprofit services that are not University sponsored).

WORLD WIDE WEB GUIDELINES AND PROCEDURES FOR ALL HOFSTRA UNIVERSITY COMPUTER AND NETWORK USERS

I. General Statement

The World Wide Web (WWW) offers the Hofstra University community rich resources for advancing teaching and research. Individuals can retrieve materials for use in their classes and scholarly activities as well as present materials for use by others. Hofstra supports the rights of students and faculty to create and receive educational information available through the Web, in keeping with its principles of academic and intellectual freedom. Access to the Web is made available to students, faculty and eligible staff of Hofstra as part of the educational computing and networking resources of Hofstra.

Use of these resources is a privilege extended to members of the Hofstra community, and must be exercised in conformity with all applicable Hofstra policies and procedures, and all applicable federal and state laws.

If anyone has any doubt as to the applicability of these guidelines and procedures, please contact the Office of Information Technology at **(516) 463- 6900** before taking any action. Anyone who does not want his or her Web activities restricted by the guidelines and procedures contained in this document is advised to contact commercial Internet service providers.

II. Hofstra Guidelines Concerning Use of Computer Facilities

Hofstra is a nonprofit, educational institution, and the use of its facilities, including computer facilities, is limited to the educational and other nonprofit purposes of its students, faculty and eligible staff. Accordingly, Web pages may be created and posted only for the educational and research purposes of the Hofstra community. These Web pages may only be posted on Hofstra-sanctioned HTTP servers. No person may include in a Web page any advertising materials or other materials relating to business or commercial activities of such person or any third person.

The content of any Web page and its compliance with applicable policy and law is the sole responsibility of the author. At any point in time, there are likely to be various federal and state laws that impose civil and/or criminal liability for computer network transmission of certain types of materials or messages. Currently, such laws restrict or prohibit transmission of, among other things, obscene materials to minors and child pornography, and messages or materials that constitute libel or harassment.

III. Hofstra Guidelines Concerning Creation of Web Pages

Creation of Web pages for educational and research purposes may involve incorporation of original works of third parties (e.g., literature, photographs, music, software, film, and video works) that are covered by copyright laws. Web page authors must obtain all permissions that may be necessary to incorporate works of third parties in their Web page. These must be presented to the University administration upon request. Use of such works may be permitted by principles of fair use, consistent with copyright laws.

No person may use the name "Hofstra" or "Hofstra University," the name of any school of Hofstra University or any logo or trademark of Hofstra University without first obtaining written permission from Hofstra's Office of University Relations, except if University-developed templates are used. It is permissible, however, for a Web page author to identify himself or herself as a student, faculty or staff member of Hofstra, as appropriate.

The following policy applies to student organization Web sites and portal groups:

LEASE NOTE: Students requesting a student organization Web sites and portal group must complete the WEB SITE LINKING AGREEMENT (located at www.hofstra.edu/scs) prior to linking to the www.hofstra.edu web site.

The purpose of the organization's Web site is to promote the mission of the organization and to convey information about the organization's activities, honors, upcoming events, past events, announcements, governance, and other pertinent organizational materials, including pictures, audio and video. Hofstra does not monitor, edit or review the materials contained within the organizations' Web sites.

The organization's president and vice president are responsible for the content of the Web site, including but not limited to text, announcements, articles, graphics, photos, external links and files. The organizations' Web sites shall be governed by the *Computer Networks Acceptable Use Guidelines* at http://www.hofstra.edu/scs/aug and other provisions of the *Code of Community Standards* as outlined in the *Guide to Pride* at: hofstra.edu/CampusL_CampusL_Dean_of_Students_guidetopride.cfm.

Web pages must comply with all University policies, rules and regulations as well as all local, state and federal laws. A report of any violation of these policies may lead to disciplinary action in accordance with the *Code of Community Standards* and may also be subject to criminal or civil legal action. Hofstra University maintains the right at its sole discretion to remove the Web site or any content that violates this policy.

No organization's Web site may link to Hofstra University's Web site or use Hofstra University's name without written permission and pursuant to the terms of the *Web Site Linking Agreement.*

In accordance with the terms of the Web site linking agreement, the following disclaimer must be posted on the page containing the link to Hofstra's Web site: *This link is provided for convenience of reference only. The existence of this link is not to be construed as an endorsement by Hofstra of the content of this Web site or any external sites to which it links. Hofstra University makes no warranties, express or implied, with respect to the site's operation, or the information, content or materials included on this Web site. To the fullest extent permissible by applicable law, Hofstra hereby disclaims all warranties of merchantability and fitness for any particular purpose. Hofstra will not be liable for any damages of any kind arising from the use of or inability to use this site.*

IV. WEB SITE LINKING AGREEMENT

STUDENT ORGANIZATION WEB SITE / PORTAL GROUP PROCEDURE AND POLICY
PROCEDURE
To apply for a student organization Web site or portal group, the organization must be recognized and approved by the University. The following steps must be completed:

- Download and complete the *Web Site Linking Agreement* located at www.hofstra.edu/scs.
- The president or vice president of the student organization must complete the application and Web Site Linking Agreement.
- The Office of Student Leadership and Activities or the relevant academic dean must confirm the current status of the organization and confirm that the application and *Web Site Linking* Agreement are completed.
- Once completed, but no later than October 30, the president or vice president must submit the organization's completed application to Student Computing Services. The signed application and *Web Site Linking Agreement* shall be maintained by Student Computing Services.
- Student Computing Services will prepare a Web site account on a designated Hofstra University server for the organization and will notify the organization's president and vice president when the user IDs and passwords have been established.
- Each year on August 31, the organization's Web site is taken down. The organization can archive the site and the site can be reactivated once a new application is submitted and the organization's current status is approved.

SUPPORT SERVICES
Portal Groups
The Help Desk will provide training and strategies for making successful and effective portal groups. The approved application form shall be forwarded to the Computer Center Help Desk to complete the portal group implementation. Training and consultation is provided to the student group PRIOR to the group going online.

Organization Web Sites
Student Computing Services provides group training classes on Web site development and design. Training in Dreamweaver and HTML are provided each semester. Custom classes are provided to organizations upon request.

V. Other Guidelines
In addition to the guidelines set forth in this document, each person using Hofstra's computer and network facilities shall also comply with the policies contained in *Responsibilities of All Hofstra University Computer and Network Users*, the *Faculty Handbook*, and the *University Policies and Procedures* and the *Code of Community Standards* set forth in the *Guide to Pride* at Hofstra. Hofstra receives its Internet access from an Internet Service Provider (ISP), and any network activity that leaves Hofstra's network destined for the Internet, including all Web pages, is bound by any policies of this ISP. In the

event of an inconsistency between Hofstra's policy and those of the ISP, the more restrictive policy shall be observed.

Hofstra does not routinely monitor or edit the content of faculty, staff or student Web pages. However, in the event that Hofstra becomes aware of a violation of University policy or law that involves a Web page, Hofstra reserves the right to remove the Web page, restrict access to such page or take other action as deemed appropriate by Hofstra University. Any such violation may also lead to disciplinary action in accordance with Hofstra rules and procedures, and referral to local, state and federal law enforcement authorities.

THIS DOCUMENT DOES NOT DISCUSS ALL APPLICABLE LAWS NOR SHOULD IT BE INTERPRETED AS PROVIDING LEGAL ADVICE. EACH WEB PAGE AUTHOR IS RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS WITH RESPECT TO HIS OR HER WEB PAGE.

For more information about creating personal Web pages, contact Student Computing Services at (516) 463-7777. Any questions concerning these guidelines should be directed to the Office of Information Technology at (516) 463-6900.

VI. NETWORK OPERATIONAL PRINCIPLES

The following statements express many of the fundamental principles governing the day-to-day operation and configuration of the HOFSTRA NETWORK as managed by the Hofstra University Computer Center. These principles are followed so as to maintain the smooth and reliable operation of the HOFSTRA NETWORK through careful adherence to widely recognized industry-standard approaches.

Network configuration and management at the school or departmental level must be performed in conformance with these principles. If a topic of interest is not mentioned explicitly below, the Computer Center must be consulted.

Network Analysis and Scanning

The Computer Center is the only group that may run any type of network analysis or network scanning equipment or software on the HOFSTRA NETWORK at large, unless express permission is granted. Such devices can be used to manipulate the network, impact connectivity at large and damage individual machines. Any such activity detected on the HOFSTRA NETWORK will be considered a security breach warranting investigation and possible revocation of network privileges during the investigation.

Network Discovery

Software that uses SNMP or ICMP to automatically "discover" or identify entities on a network generally can have a negative impact on the network at large. As such, network discovery is prohibited. Such software scans the entire network, flooding it and its intended target agents with an overwhelming amount of SNMP traffic. The end result is reduced bandwidth to the local networks and diminished router performance.

Network Naming and Addressing

External hostnames or domain names may not be registered with Internet Service Providers (ISPs) or the InterNIC against Hofstra DNS name space, address space or name servers.

Additional IP and Domain Guidelines
- Private IP address space is NOT available.
- No computer can use the Hofstra sub domain name.
- An individual or group may not register a domain name with Hofstra's IP address.
- An individual or group may not register a domain name that contains Hofstra or Hofstra University, as these are trademark names.

VII. NETWORK SERVICES

Non-routable protocols: The HOFSTRA NETWORK, being a multiprotocol routed network, supports IP, IPX and DecNET protocols; however, non-routable protocols such as NetBEUI (used by Windows NT/95/98 for Microsoft Networking) pose significant scalability problems by not properly functioning on a routed network. Hence they are not supported for communications across the HOFSTRA NETWORK.

Domain Name Service: The HOFSTRA NETWORK supports the IETF/Internet host-naming scheme called the Domain Name Service (DNS). Due to significant incompatibilities with this standard, the Microsoft naming scheme, WINS, is not supported.

Name and Boot servers: The Computer Center runs redundant BOOTP, DHCP and DNS servers on behalf of the HOFSTRA NETWORK. These servers ensure the uninterrupted and reliable assignment and registration of IP addresses for all hosts on the HOFSTRA NETWORK. Individual departments may not run such servers of their own. The Computer Center sets the standards for all network services in DNS services and servers.

WWW proxy server: The Computer Center runs an HTTP proxy server on behalf of the University. Such devices can consume a large amount of bandwidth on the network, and pose a security risk to the HOFSTRA NETWORK unless extremely carefully managed. As a result, no other HTTP proxy servers may be run on the network.

FTP and Web server appropriate use: FTP or Web servers for the intention of distributing copyrighted or pirated software on the HOFSTRA NETWORK or the Internet are illegal and not permitted on the HOFSTRA NETWORK. Any group wishing to establish an FTP or Web server for distribution of large amounts of data should contact the Computer Center for guidance. Such activity impacts traffic flows on the network and has a direct impact on performance of the HOFSTRA NETWORK at large.

High-bandwidth network applications: High-bandwidth projects or activities, including streaming video and videoconferencing, should also be conducted in coordination with the Computer Center.

Local Area Networks and Servers: Backup of computers over the HOFSTRA NETWORK is not currently supported, due to the bandwidth requirements of such activities. Individuals may use the network to back up machines local to their LAN, but such traffic traversing the

HOFSTRA NETWORK backbone can negatively impact the connectivity of others on the HOFSTRA NETWORK.

VIII. SERVING COPYRIGHTED MATERIAL

Hofstra provides Web and FTP servers for use by students, staff and faculty as well as central Web site. Consequently, many opportunities exist for individuals or departments to "publish" information for global consumption.

Unfortunately, this provides a means to redistribute non-original material (e.g., commercial music, commercial software, documents) that is protected by copyright, without permission of the copyright owner, using Hofstra's systems and network.

Peer-to-peer (P2P) file-sharing technology allows users to make files available for other users to download and use. File sharers store files on their computers and the file-sharing software enables other users to download the files onto their computers. Examples of P2P file sharing networks include BitTorrent, Gnutella, and LimeWire, among others.

If you have P2P file-sharing applications installed on your computer, you may be sharing copyrighted works without even realizing it. Even if you do not intend to engage in infringing activity, installing P2P software on a computer can easily result in you unintentionally sharing files (copyrighted music or even sensitive documents) with other P2P users, and you may then be personally responsible for the legal and financial consequences.

Distributing copyrighted works without permission of the copyright holder is both contrary to Hofstra's policy on appropriate-use, and is a violation of federal law governing copyright.

If you are serving any data, in any medium, that is not your own intellectual property, and is protected by copyright, you must either obtain the permission of the owner of the material or remove the copyrighted material from distribution immediately.

RESTRICTIONS ON USE OF BANDWIDTH

In order to ensure the HOFSTRA NETWORK availability is sufficient for Hofstra work, the University has been forced to take steps to restrict traffic related to an outside service that enables distribution of music files, streaming video, or audio over the Internet. This is in violation of the policy prohibiting the installation of servers on the HOFSTRA NETWORK. See section titled *Limitations of the Hofstra Network Account.* Any file sharing and file scanning software (e.g., P-2-P software) creates significant risks of compromise to your computer and your privacy, as well as to other computers on the HOFSTRA NETWORK. There is no way to tell what malicious functions may be performed by the software you automatically download or what modifications may have been made to the files themselves. By choosing to be an authorized user of the Hofstra University network [HOFSTRA NETWORK], you have agreed to these limitations in addition to those updated at www.hofstra.edu/scs/aug.