Introduction

Access and use of computing and networking resources at Hofstra University are privileges extended to members of the Hofstra community. All holders of Hofstra University Network accounts are fully responsible for the actions performed on their accounts and their assigned machines.

Hofstra University's Office of Information Technology (IT) provides wired and wireless data network services for all organizations within the University. Hofstra University computer and network resources include, but are not limited to: the computing devices, printers, networks, online and offline storage media and related equipment, software and data files that are owned, managed, contracted for 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. (Collectively referred to as "Computing Resources").

Scope

This policy applies to students, faculty and other employees of the University and to all other persons accessing Hofstra University computer and network resources. As a condition to being granted use of or access to Hofstra University computer and network resources, each user (1) consents to the provisions of this policy and (2) agrees to comply with all of the terms and conditions detailed within this policy. Use of Hofstra Computing Resources, even when carried out on a privately-owned computing device that is not managed or maintained by Hofstra University, is governed by this policy.

Any use of Computing Resources in violation of this policy will subject the employee to appropriate disciplinary action up to and including termination as deemed appropriate by the University and in compliance with any applicable collective bargaining agreement. As set forth in the Guide to Pride, students are responsible for adhering to all acceptable use policy and student violations of this policy can result in loss of Hofstra University computing privileges, disconnection from the Hofstra network, and University sanctions as outlined in the Code of Community Standards. Any such violation by faculty, student, employee or other user may also lead to referral to local, state and federal law enforcement authorities. Without limiting its right to take action, the University reserves the right to, with no prior warning, (a) disable network access or (b) 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 and/or in response to violations of this or other University policies, laws or regulations.

Privacy

Hofstra University seeks to maintain its Computing Resources in a manner that respects individual privacy and promotes user trust. The use of Hofstra University's Computing Resources, however, is not completely private and users should have no reasonable expectation of privacy in their use of the Computing Resources.

The normal operation and maintenance of the University's Computing Resources, which includes the safeguarding of the security of these resources, require back up and caching of data and communications, logging of activity, monitoring of general usage patterns and other similar activities. These activities are necessary to protect the

integrity of University information resources and the rights of all users of the Computing Resources. When there is sufficient evidence of wrongdoing or when compelled by subpoena, court order or other legal demand for information, the University reserves the right to examine and impound any files, information or computer system(s) resident or attached to the Hofstra University network. The University may, with or without further notice to users, take such action as it deems necessary to preserve, protect, secure and promote the interests of the University in this regard.

Acceptable Use of Hofstra Computing Resources

Students, faculty and other employees of the University and all other persons accessing Hofstra Computing Resources, have the responsibility to use Computing Resources in an ethical and legal manner and agree to and acknowledge the following as a condition for the use of the Hofstra network:

- 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, employee 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 Hofstra's 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 network connected devices and my computer accounts and will adhere to this policy and other University policies. I will not use University Computing Resources in a manner that violates federal, state or local civil or criminal law.
- I will not attempt to monitor other individuals' computing devices 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.
- I must observe U.S. copyright laws, patent, trademark or other intellectual property rights.

- I must abide by applicable licensing restrictions in the receipt, transmission, use or destruction of software or data.
- 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 – whether provided by organizations within or outside the University – may be subject to additional norms of behavior or terms and conditions, such as those set forth in software licensing agreements or regulations specific to the resource, which I agree to follow.
- 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 policies and those of the ISP, the more restrictive policy shall be observed.
- 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 Computing Resources to solicit sales, personal commercial gain, conduct non-University 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 computing device.
- Incidental and non-recurring personal use of Computing Resources by faculty and other employees is tolerated as part of the daily learning and work of all members of the University community, provided however that such use does not otherwise violate this Policy or any other applicable law or regulation or University policy or procedure.
- Intentional access to, downloading of or dissemination of pornography by University employees is prohibited unless such use is for scholarly purposes. This provision applies to any electronic communication distributed or sent within University Computing Resources or to other networks while using University Computing Resources.
- I may not engage in activities that damage or disrupt communications, hardware devices or software applications, such as but not limited to, virus/malware/spyware propagation, circumventing system protection mechanisms, and/or overloading the network with excessive data.
- 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.

Compliance with Applicable Federal, State and Local Law

The University requires compliance with applicable federal, state and local laws, including copyright, export and re-export laws, as a condition to system use. Hofstra University respects the intellectual property rights of others. Intellectual labor and creativity is vital to academic discourse and enterprise. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of

privacy, unauthorized access, and trade secret and copyright violations, are violations of this policy. Moreover, except as expressly permitted, users shall not alter, delete or modify any attributions included within any hosted services.

Confidential and/or Sensitive Information

For the purposes of this policy, sensitive information is defined as information protected by all applicable laws, including, but not limited to, 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, as well as information that is considered confidential to the University's operations. Information contained on the Hofstra network may contain confidential or sensitive information. 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. Sensitive information should not be stored or saved on personal or home computers or on removable media such as flash drives or CD-ROMs, unless the media is sufficiently encrypted. In addition, sensitive information should not be stored, sent or saved using external storage vendors with whom the University does not have an agreement, e.g. you should not use personal accounts with outside vendors for this purpose. For assistance with appropriate ways to save, store or send sensitive University information in a secure and efficient manner, please contact the Help Desk. University employees must comply and be familiar with the University's Information Security Program, found on the IT department's web page.

Copyright

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. See also Hofstra's Policy regarding Reporting Copyright Infringements for more information about the Digital Millennium Copyright Act and penalties thereunder.

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.

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. Moreover, 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 automatically downloaded or what modifications may have been made to the files themselves.

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.

Please note that 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.

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.

Network Account Specific Policies and Information

Network accounts are intended to provide members of the Hofstra University community with basic access to Hofstra University Network academic and administrative software applications and Internet services, including electronic mail, Google Applications, the my.Hofstra.edu portal and other information services via World-Wide Web. Users agree not to engage in any activity that interferes with or disrupts the services, servers or networks provided.

Password

Each user of the system is assigned a unique login ID. The system automatically prompts users to change their passwords every six months to maintain high security on the system. It is the account holders' responsibility to maintain the secrecy of their passwords. Passwords must conform to Hofstra University's strong password policy. For additional information visit Password Help Guidelines.

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 related services. 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.

- For students, network accounts will be deactivated and removed upon graduation, or if affiliation with Hofstra University ends. For employees, access to the employee network and email accounts will be revoked upon termination.
- A residential student's wired Hofstra Network connection is to be used only by the individuals residing in the room where the port is located. Under no circumstance may students allow other individuals to access the HOFSTRA NETWORK through the wired network connection in their rooms.
- Users are not to run any type of unauthorized server (i.e., Web/ HTTP servers, file servers, DNS servers, DHCP servers, FTP servers, list servers, media sharing server, 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).
- Users may not use wireless routers or Wi-Fi access points on the Hofstra University campus as these devices interfere with Hofstra-provided wireless network services and potentially allow unauthorized access to Hofstra's network.
- Software that uses SNMP or ICMP to automatically "discover" or identify entities on a network is prohibited.
- Only IT may run any type of network analysis or network scanning equipment or software on the HOFSTRA NETWORK at large. 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.
- Only IT may run redundant BOOTP, DHCP and DNS servers on behalf of the HOFSTRA NETWORK. Individual departments may not run such servers of their own. IT sets the standards for all network services in DNS services and servers.
- IT runs an HTTP proxy server on behalf of the University and no other HTTP proxy servers may be run on the network.

Restrictions on use of Bandwidth

In order to ensure that the Hofstra network availability is sufficient for academic work and Hofstra business, the University has taken steps to restrict traffic related to unauthorized outside services that enable distribution of music files, streaming video, or audio over the Internet.

High-bandwidth projects or activities, including streaming video and videoconferencing, should also be conducted in coordination with IT.

Electronic Mail

Faculty, Administrators and Staff

Hofstra provides email services for legitimate University-related activities and personal use should remain incidental. University email accounts, as Computing Resources, are subject to the provisions of this Acceptable Use Policy. As with all Computing Resources, email accounts are not completely private, and users should have no

reasonable expectation of privacy in their use of email services.

Access to Accounts of Terminated or Otherwise Unavailable Employees

It is not a standard practice to provide access to the email accounts of former or otherwise unavailable employees. In general and subject to the provisions of this Acceptable Use Policy, access to employee email accounts should be with employee's consent. When employees are not available to provide such consent, for example, when an employee is on leave; unexpectedly goes on a prolonged absence; is terminated for cause; or is otherwise incapacitated; no access will be granted to their email accounts without the prior written approval of the Chief Human Resources Officer or her designee for nonfaculty employees and, for faculty, of the Provost or her designee. Any requests for access directed to the IT Help Desk will be redirected to the Human Resources department or Provost's Office, as appropriate.

Deceased Employees

University email accounts are for legitimate University-related activities and are digital assets belonging to the University and not to the employees. Upon notice of an employee's death, the University's IT department will coordinate with the Human Resources department to disable the deceased employee's network account, including email accounts. No direct access to the University email accounts of deceased employees will be provided to third parties. Timely requests for access to email accounts of deceased employees by the employees' former department for University business shall be subject to the same approval process set forth above.

Student Email

Hofstra University students are provided with a Hofstra Gmail account sponsored by Google. While a student at Hofstra, student use of the Hofstra Gmail account is subject to this Acceptable Use Policy. The Hofstra Gmail account will remain with the student once the student has graduated or is no longer a Hofstra student, and is then subject to the terms and conditions set forth by Google.

Upon a student's death, the University's IT department disables a student's University Google/Gmail account and deletes the account and its contents 30 days later. Any rights to the deceased student's University Gmail account are subject to this limited retention, to the terms and conditions of the Google account, and to applicable law.

No Warranties or Assurances:

The University makes no warranties of any kind, whether express or implied, with respect to the Computing Resources it provides. Hofstra University is not responsible for any damage resulting from use of Computing Resources, including service interruptions, 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.