

3. Users are responsible for all use of information systems conducted under their user ID(s), and are expected to take all precautions including password security and file protection measures to prevent use of their accounts and files by unauthorized persons. Sharing of passwords is prohibited.
4. Users may not offer, provide, lend, rent, or sell access to University information systems. Users may not provide access to individuals outside the University community. Expansion or redistribution of Northeastern's networking and cable television services are not permitted. Personal, private, or departmental switches, routers, wireless access points, or DHCP-serving devices may not be connected to centrally managed network segments, except only as may be agreed to in writing between the device owner and Information Services. For security reasons, dial-up modems may not be in use on computers while they are connected to the University network, except only as may be required for bona fide academic or administrative purposes, and where appropriate security measures are in place.
5. Use of University information systems for hosting non-University activities must have the explicit written authorization of the senior vice president for Administration and Finance prior to the use.
6. While the University attempts to protect electronic communication and files from unauthorized access, this cannot be guaranteed. Users may not access, copy, or move files including, but not limited to programs, data, and electronic mail that belong to another account, without prior authorization from the account holder. Files may not be moved to other computer sites without permission from the holder of the account under which the files reside.
7. Users may not use remote resources such as printer and file systems, regardless of location on or off the Northeastern network, unless the administrator of the remote resource has first granted permission to do so.
8. Northeastern information systems may be used for lawful purposes only. Users must not use their accounts or Northeastern information systems for unlawful purposes, including, but not limited to, the installation of fraudulently or illegally obtained software, illegal dissemination of licensed software, sharing of content where the disseminator does not hold lawful intellectual property rights, or propagating chain letters, pyramid, Ponzi, other unlawful or deceptive schemes, or for any purpose contrary to local, state, and federal law or University policy.
9. Use of University information systems must comply with the provisions of copyright law and fair use. Copyright law limits the right of a user to decrypt, copy, edit, transmit, or retransmit another's intellectual property, including written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is in compliance with Fair Use or TEACH Act provisions.
10. Printed materials, computer equipment, and storage media containing sensitive and/or protected information, shall be handled in accordance with Information Disposal Guidelines, Asset Disposition procedures, and hazardous materials regulations.
11. Users are responsible for the timeliness, accuracy, and content/consequences of their Web pages and other electronic writings. Posting of personal, family, or other identifying information is at the sole discretion of the user, and is a discouraged practice.
12. The electronic privacy rights of others shall be respected at all times. Use of audio, video, cell phone, "Web cam," or related technologies for the purpose of capturing images and/or recording speech in locations or circumstances where a reasonable expectation of privacy exists, is prohibited without the consent of the subject(s) depicted and/or recorded. This provision shall not apply to lawful surveillance conducted by appropriate law enforcement agencies. The University reserves the right to impose additional restrictions on the use of electronic recording devices, in its sole discretion. Questions about the applicability of this provision to a particular situation should be referred to the Office of University Counsel or the director of Information Security and Identity Services.
13. University information systems may not be used for commercial purposes except only as permitted with explicit prior written approval of University Counsel and the senior vice president for Administration and Finance.

14. Internet use must comply with the Terms of Service stipulated by our Internet service provider(s). These policies are incorporated by reference. In addition, the acceptable use, Terms of Service and/or other policies of the system(s) also bind users of the Internet connection and resources to which they connect. At the time of this writing, the Internet service providers for Northeastern University are Level3 Communications (www.level3.com), Sprint (www.sprint.com), Northern Crossroads (www.nox.org), and Abilene Network/Internet2 (abilene.internet2.edu).
15. Users may not use information systems irresponsibly, wastefully, or in a manner that adversely affects the work or equipment of others at Northeastern or on the Internet.
16. Exports of computing equipment and information technologies from the University must be in compliance with U.S. Export Control Regulations.
17. Electronic messages pertaining to the official business of the University, including all academic and administrative matters, shall be sent from University-owned or University-recognized messaging systems. For example, student inquiries must be sent from myNEU or other University-recognized e-mail account. Replies from faculty or staff must be sent to the same accounts. In cases where unrecognized third-party messaging systems are used to originate a message, and/or where a party chooses to forward messages from a University-owned or University-recognized system to a third-party unrecognized system, individuals using these systems shall be solely responsible for all consequences arising from such use.
18. Speakers are expected to make clear when they are not representing the University in their electronic communications.
19. The University's information systems, and the messages, e-mail, files, attachments, graphics, and Internet traffic generated through or within these systems, are property of the University. They are not the private property of any University employee, faculty, staff, contractor, student or any other person. No user of University systems should have an expectation of privacy in their electronic communications. All electronic communications, files and content presented to and/or passed on the Northeastern network, including those to, from or through Internet connection(s), may be monitored, examined, saved, read, transcribed, stored, or retransmitted by an authorized employee or agent of the University, in its sole discretion, with or without prior notice to the user. The University reserves and intends to exercise the right to do so. Electronic communications and content may also be examined by automated means.

Northeastern reserves the right to reject from the network or block electronic communications and content deemed not in compliance with policies governing use of information systems at the University. The University may make appropriate disclosures of written and/or electronic information or data from the University's information systems, including with respect to an investigation of alleged misconduct or wrongdoing and/or to law enforcement, pursuant to lawful inquiries and/or legal process. By accessing Northeastern information systems, users give Northeastern permission to conduct each of the operations described above.
20. The confidentiality of any message or material should not be assumed. Even when a message or material is deleted, it may still be possible to retrieve and read that message or material. Further, the use of passwords for security does not guarantee confidentiality. Messages read in HTML may identify the reader to the sender. Aside from the right of the University to retrieve and read any electronic communications or content, such messages or materials should be treated as confidential by other students or employees and accessed only by the intended recipient. Without prior authorization, students and employees are not permitted to retrieve or read electronic mail messages not sent to them.
21. Notwithstanding the University's right to audit or monitor its information systems, all users are required to observe the confidentiality and privacy of others' information accessed through Northeastern information systems, including information pertaining to University programs, students, faculty, staff, and affiliates. Without proper authorization, University system users are not permitted to retrieve or read electronic mail messages not sent to them. With proper University authorization, the contents of electronic mail or Internet messages or materials may be accessed, monitored, read, or disclosed to others within the University or otherwise.

22. The University strives to maintain the security and privacy of electronic communications. All use, dissemination, and disclosures of information must comply with the provisions of applicable law, regulation, and University policy, described in the following table:

Handling of this type of information	Must be in compliance with this law, regulation, or policy...	Which can be read at this location...
Student information	Family Educational Rights and Privacy Act (FERPA) of 1974	http://www.osccr.neu.edu
Protected health information (PHI)	Health Insurance Portability and Accountability Act (HIPAA) of 1996	http://www.neu.edu/adminm/HIPAA_Privacy_Practices.pdf
Social Security Number (SSN)	NU Policy on Collection, Handling, and Use of the Social Security Number	http://infoservices.neu.edu/get_help/virus_and_security_information.html

23. The University reserves its right to use manual and/or automated means to assess materials submitted as academic work submitted electronically for signs of plagiarism or other form(s) of academic dishonesty.
24. The University reserves the right at any time, without prior notice or permission from the user or users of a computer or other Northeastern-owned computing device, to seize such devices and/or copy or have copied, any and all information from the data storage mechanisms of such devices as may be required in the sole discretion of the University in connection with investigations of possible wrongdoing.
25. By accessing and/or using any Northeastern information or telecommunication system, including its network, e-mail, or Internet services, the user agrees and expressly consents to the terms of this policy, and gives Northeastern permission to conduct each of the operations, monitoring, or oversight practices described in this policy, including but not limited to those in sections 18 through 22.
26. The Appropriate Use Policy specifically prohibits the use of Northeastern University information systems or facilities to:
- Harass, threaten, defame, slander, or intimidate any individual or group;
 - Generate and/or spread intolerant or hateful material, which in the sole judgment of the University is directed against any individual or group, based on race, religion, national origin, ethnicity, age, gender, marital status, sexual orientation, veteran status, genetic makeup, or disability;
 - Transmit or make accessible material, which in the sole judgment of the University is offensive, violent, pornographic, annoying, or harassing, including use of Northeastern information systems to access and/or distribute obscene or sexually explicit material unrelated to University sanctioned work or bona fide scholarship;
 - Generate unsolicited electronic mail such as chain letters, unsolicited job applications, or commercial announcements;
 - Generate falsely identified messages or message content, including use of forged content of any description;
 - Transmit or make accessible password information;
 - Attempt to access and/or access information systems and/or resources for which authority has not been granted by the system owner(s);
 - Capture, decipher, or record user IDs, passwords, or keystrokes;

- Intercept electronic communications not intended for the recipient;
- Probe by any means the security mechanisms of any resource on the Northeastern network, or on any other network through a connection to the Northeastern network;
- Disclose or publish by any means the means to defeat or disable the security mechanisms of any component of a Northeastern University Information System or network;
- Alter, degrade, damage, or destroy data;
- Transmit computer viruses or malicious/destructive code of any description;
- Conduct illegal, deceptive, or fraudulent activity;
- Obtain, use, or retransmit copyrighted information without permission of the copyright holder;
- Place bets, wagers, or operate games of chance; or
- Tax, overload, impede, interfere with, damage, or degrade the normal functionality, performance or integrity of any device, service or function of Northeastern information systems, content, components, or the resources of any other electronic system, network, service, or property of another party, corporation, institution or organization.

The above enumeration is not all-inclusive. If there is a question as to whether a specific use is appropriate or acceptable under this policy, the University's sole determination shall prevail.

27. Use of Northeastern University information systems must comply with all applicable local, state, and federal laws, including, but not limited to, the following which are incorporated herein by reference:

- Massachusetts General Laws Chapter 266, Sections 33(a) and 120(f), which imposes sanctions for, among other acts, destroying electronically processed and stored data or gaining unauthorized access to a database or computer system.
- United States Code, Title 18, Sec. 1030 et seq., Computer Fraud and Abuse Act, which imposes sanctions for, among other acts, knowingly accessing a computer without authorization or in excess of authorized access, knowingly causing damage to protected computers, or trafficking in password information.
- United States Code, Title 18, Sec. 2510 et seq., Electronic Communications Privacy Act, which imposes sanctions for, among other acts, interception of wire, oral, or electronic communications.
- United States Code, Title 18, Sec. 2701 et seq., Stored Wire and Electronic Communications and Transactional Records Act, which imposes sanctions for, among other acts, intentionally accessing without authorization, a facility through which electronic communication service is provided, or intentionally exceeding authorization to access a facility, and thereby obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage.
- United States Code, Title 47, Sec. 223 (H)(1) et seq., Communications Act of 1934 (Amended), which imposes sanctions for, among other acts, use of any device or software that can be used to originate telecommunications or other types of communications that are transmitted in whole or in part by the Internet, without disclosing the sender's identity, and with intent to annoy, abuse, threaten, or harass any person who receives the communications.

NOTICE OF RIGHT TO CHANGE APPROPRIATE USE POLICY

The University reserves the right to change this policy or any portion of the policy, at any time, without prior notice. Changes to this policy are effective upon posting at <http://www.infoservices.neu.edu>, where the most current version resides.