

INFORMATION TECHNOLOGY

Rights and Responsibilities for the Use of Central Network and Computing Resources at Northwestern University

Audience:

All members of the Northwestern Community and users of the University network.

Policy Statement:

Northwestern University Information Technology (NUIT) is the University organization that provides access to the network for Northwestern students, as well as for many Northwestern faculty and staff. The Northwestern computer network consists of a campus-wide backbone network, local area networks, and many shared computers as well as personal desktop computers. NUIT works to insure that network rights and responsibilities are not violated.

Background Issues:

Rights

Members of the Northwestern community can expect certain rights as they use the network and its services.

- **Intellectual Freedom:** The University is a free and open forum for the expression of ideas, including viewpoints that are strange, unorthodox, or unpopular. The University network is the same. Network administrators place no official sanctions upon the expression of personal opinion on the network. However, such opinions may not be represented as the views of Northwestern University.
- **Safety from Threats:** While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications should bring them to the attention of University Police. Electronic threats are taken as seriously as voiced or written threats, consistent with University policy.
- **Privacy:** Data files and messages traversing the University network are not private communications. The University reserves its right, as owner of the network and the computers in question, to examine, log, capture, archive, and otherwise preserve or inspect any messages transmitted over NUNet and any data files stored on University-owned computers. All members of the community must recognize that electronic communications are by no means secure, and that during the course of ordinary management of computing and networking services, network administrators may inadvertently view user files or messages. In addition, if a user is suspected of violations of the responsibilities as stated in this document, that user's privacy is superseded by the University's requirement to maintain the network's integrity, protect the rights of all network users, and promote respect for applicable laws and applicable license provisions. Should the security of a computer be threatened, user files and messages may be examined under the direction of the vice president & chief information officer, the associate vice president for cyber infrastructure, or a director of an IT division.

Responsibilities

There are also responsibilities that must be met as part of the privilege of network access. Network users are expected to live up to these responsibilities. If you knowingly violate a network responsibility, your network access will be suspended. Depending on the seriousness of the violation, you could be referred through the University disciplinary procedure process. Violations that also violate federal or state laws can also result in referral to the appropriate legal authority.

1. You are responsible for the use of your network ID (NetID) and all computer accounts that are assigned to you. You may not give anyone else access to your NetID or computer accounts. You must not use a NetID or a Northwestern University computer account that was not assigned to you. You may not try in any way to obtain a password for another user's NetID or computer account. The NetID and its associated password are the property of Northwestern University Information Technology. Applications and services that require their use must be approved by the Office of the Vice President for Information Technology or by a director within NUIT.

2. You may not misrepresent yourself or your data on the network.
3. You are responsible for the security of your passwords. This includes changing passwords on a regular basis and making sure no one else knows them.
4. You must not use NU's network resources to gain or attempt to gain unauthorized access to remote computers.
5. You must not deliberately perform an act that will seriously impair the operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
6. You must not run or install on any of NU's computer systems, or give to another, a program that could result in the eventual damage to a file or computer system and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
7. You must not attempt to circumvent data protection schemes or exploit security loopholes or interfere with standard technical measures that identify and protect the rights of copyright owners.
8. You must abide by the terms of all software licensing agreements and copyright laws. You must not make copies of or make available on the network copyrighted material, including without limitation, software programs, music files, video files, still and digital images, radio and television broadcasts, and written text works, unless permitted by a license, by the consent of the copyright owner, by a fair use limitation under copyright law, or by permitted copying under the Digital Millennium Copyright Act (DMCA) when made by a library or archive for preservation purposes or when incidental to computer maintenance and repair. Please see the more complete discussion of [software copyright protections \(/software.html\)](#) available on NUInfo, and the discussion of copyright law available on the [NU Office of General Counsel Web site \(/http://www.northwestern.edu/general-counsel/\)](http://www.northwestern.edu/general-counsel/).
9. You must not deliberately perform acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of other users. Any person operating a network-intensive application or a defective computer that overloads University networks will be notified and steps will be taken to protect the overall University network. This may include disconnecting the offending computer system from the University network until the problem is resolved. If the condition is an imminent hazard to the University network or disrupts the activities of others or violates applicable law, then the offending computer system or the subnet to which it is attached may be disconnected without prior notice.
10. You may not place on any University-owned computer system information or software that infringes on the rights of another person or gives unauthorized access to another computer account or system.
11. You must not attempt to monitor another user's data communications, nor may you read, copy, change, or delete another user's files or software, without permission of the owner.
12. Computing and networking resources are provided to support the mission of the University. These resources may not be used for commercial purposes.
13. Any network traffic exiting the University is subject to the acceptable use policies of the network through which it flows, as well as to the policies listed here.
14. All University computing and networking facilities are provided for use by faculty, staff, and students for relevant academic, research, or administrative pursuits. Like all other University facilities, private use must be approved in advance in keeping with policies expressed in the Northwestern University Employee Handbook and the Northwestern University Student Handbook.
15. Information servers - responsibility for content. The content of any information made available to others via the University's network is the sole responsibility of the person who created that information. It is that person's responsibility to become educated and aware of all applicable Federal laws, State laws and [University policies \(/index.html\)](#). See also discussion of copyright law on the [NU Office of General Counsel Web site \(/http://www.northwestern.edu/general-counsel/\)](http://www.northwestern.edu/general-counsel/). That person will be liable for any violations of Federal laws, State laws, or University policies.
16. Continued violations of system and network policies will be referred to the appropriate office for discipline. Sanctions may include fines, restitution of funds, termination of computer or network access, probation, suspension, separation, or exclusion from the University.

The NUIT Security Officer should be notified about violations of copyright laws and these NUIT policies, as well as about potential loopholes in the security of any computer systems and networks at Northwestern. Contact the NUIT Security Officer at [security@northwestern.edu \(/mailto:security@northwestern.edu\)](mailto:security@northwestern.edu).

Last Review Date:

December 2013

Original Issue Date:

June 2003



Revision Dates:

July 2012

June 2008

June 2003

Additional Information:

- [Northwestern University Staff Handbook](http://www.northwestern.edu/hr/forms/oncampus/handbook.pdf)  (<http://www.northwestern.edu/hr/forms/oncampus/handbook.pdf>)
- [Student Handbook](http://www.northwestern.edu/handbook/handbook.pdf)  (<http://www.northwestern.edu/handbook/handbook.pdf>)

Related Policies:

- [Use of Computers, Systems, and Networks \(/csn-use.html\)](#)
- [Use of Student Residence Networks \(/resnet.html\)](#)

Address**Information Technology**

1800 Sherman Ave
Evanston, IL 60201

Phone number

847-491-4357 (1-HELP)

Email Addressconsultant@northwestern.edu (<mailto:consultant@northwestern.edu>)[Share feedback about this page \(/../forms/feedback/comments.html\)](#)