

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY



Document Number: IT-POL-1
Audience: Students, Faculty and Staff
Effective Date: August 20, 2003
Revision Date: August 20, 2007
Author(s): Bob Wisler, Director of Information Technology
Contributors: See acknowledgements
Approved By: Northwood University Officers
Document Security: Public - www.northwood.edu/aup

SCOPE

This policy applies to all of the Northwood University community including students, faculty, administrators, staff, contract employees, and those who may be granted a guest computer account on a request basis. For purposes of this policy, Northwood systems include all computers and software owned by the University, any communications hardware and software provided by the University for the purpose of accessing its computers, and any computer network governed in part or whole by the University. Any member of the community who violates this policy is subject to disciplinary action as stated in this policy, and possible legal action under Federal Electronic Communication Acts. In addition, the **University community is bound by the Northwood [Code of Ethics](#) in the use of computer resources.**

DESCRIPTION

Northwood University's computing resources are provided for educational and academic purposes. Use of Northwood systems and all resources to which they are connected is a privilege, not a right. Northwood systems are a resource provided by the University as an educational tool to exchange information more efficiently. The Information Technology Department manages the resources for the mutual benefit of all. Computing resources include labs used for general computing, computer classrooms used for instructional purposes, facilities required to maintain operations, and any computer that is connected to the Northwood network. Access to these systems and resources is a privilege granted to the University community. Users must conduct computing activities in a responsible manner, respecting the rights of other computer users and respecting all copyright and computing license agreements. All computing and networking resources should be used in an efficient, ethical, and legal manner. This policy applies to all computer systems regardless of their operating system, manufacturer, or network connectivity.

Northwood University operates various network, academic, and administrative systems in support of its academic mission and business function. These systems are maintained and operationally controlled by the Northwood University Information Technology Department. As used in this policy, the term "user" refers to any person consuming technology resource. The term "Information Technology staff" refers to the full-time professional staff reporting to the corporate Director of Information Technology. The term "Northwood systems" refers to computing and associated systems or resources operated by Northwood University. Information in electronic format, whether stored on computers or removable media, is to be considered Northwood University property.

This policy provides a general description of what is expected of users. It is not intended to be an exhaustive list of all allowed/forbidden activities, but rather a guideline for the ethical use of the Northwood computing environment. Users should read the appropriate campus Computer Lab Rules & Procedures

ACCEPTABLE USE POLICY

- 2 -

posted in each computer lab for additional information and supplemental policies pertaining to the classroom or lab environment.

VIOLATIONS

Any violations of Northwood policies may result in disciplinary action up to and including termination or expulsion. If necessary, the University will advise appropriate legal officials of any illegal activities.

NETWORK, INTERNET AND E-MAIL

Access to the Northwood network, Internet and e-mail system is provided to students and employees for the benefit of the organization and its customers. To ensure that all students and employees are responsible Internet users and to protect the University's public image, the following guidelines have been established.

Acceptable Use

Students and employees accessing the Internet and e-mail through the Northwood system are representing the University. Both employees and students are responsible for seeing that the Internet is used in an effective, ethical and lawful manner.

Responsibilities include:

- The content of all text, audio, or images placed or sent over the Internet, e-mail and instant message programs.
- All messages communicated should have the user's name attached.
- No messages will be transmitted under an assumed name.
- Users may not attempt to obscure origin of any message.
- Information published on the Internet should not violate or infringe upon the rights of others.
- No abusive, profane or offensive language should be transmitted through the system.

Unacceptable Use

Students and employees must not use the Network, Internet or e-mail for purposes that are illegal, unethical or harmful to the University. Examples of unacceptable use are as follows:

- Personal gain or advancement of individual or political views.
- Solicitation of non-University business, or any use of the Internet for personal gain, is strictly prohibited.
- Privacy intrusions such as reading other user's e-mail, using accounts other than their own (including ID or password "cracking"), reading or deleting unprotected files, etc. Data stored in electronic format is to be considered real property.
- Network connections may not be used for the purposes of making unauthorized connections to, breaking into, or adversely affecting the performance of other systems on the network, whether these systems are University-owned or not.
- Users must not disrupt the operation of the University network or the networks of other users.
- Internet and e-mail use must not interfere with employee productivity.
- No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference will be transmitted.
- Access to, or distribution of, sexually explicit or defamatory content is strictly prohibited. In the event that these items are accessed at no fault of your own, or in the attempt to end future inappropriate communications or usage, accessing these items are not a violation of the Acceptable Use Policy.
- Spam, unsolicited bulk e-mail, including mass-mailings/forwarding, and chain letters. Use of Northwood University generated distribution lists is permitted only when explicitly authorized by

Information Technology. Access to these lists will be granted on a case-by-case basis.

Non-Northwood Owned Network Devices: Without specific authorization by the Network Administrator, users must not physically or electronically attach any foreign networking device to the Northwood University network. This includes, but may not be limited to routers, switches, hubs, wireless access points, and any device that may provide DHCP services. Violation of this policy may result in the immediate suspension of Northwood University network connectivity privileges.

Electronic Communications Policy

E-mail is the standard, and sometimes preferred, means of internal communication at the University. The University will consider employees and students to be duly informed and in receipt of notifications and correspondences sent by an administrator, staff, or faculty member delivered to an employee's or a student's Northwood e-mail account. It is recommended that employees and students frequently access their Northwood e-mail account for official information. All full-time and part-time faculty and staff, including active adjunct instructors, are expected to regularly check their Northwood e-mail account, and to acknowledge messages in a timely manner. Employees are expected to use the automated out-of-office notification functions in e-mail and voicemail when they are away from the office for an extended period.

ADMINISTRATIVE SYSTEMS

Northwood University, to provide services to its constituents, records a large amount of extremely confidential data, transmits the information over extensive networks, and stores the information on numerous computing systems. Any breach in the security of these systems or networks could disrupt the University and/or allow such confidential information to be transmitted quickly, silently and without geographic or constituency limits.

Recognizing these vulnerabilities and the need for institutions to limit access to such information, the Federal Government has passed numerous laws concerning personal information. As a result, the University must comply with a complex array of legislation including, but not limited to, FERPA. Failure to comply with legislation can have significant adverse consequences on the University.

The University is the ultimate owner of all Institutional Data (information relating to the administration of the University). All Institutional Data are considered confidential and are intended exclusively for purposes related to the University's programs. All Institutional Data and administrative systems should be used only for the legitimate business of the University and not for commercial, personal and/or political purposes.

Administrative Systems Accounts Management

Requests for access to Institutional Data, including maintenance and/or inquiry, should be given to the appropriate Module Leader who will determine the validity of the request. If a request for access crosses functional modules, the Module Leader for each respective module must authorize the request for its respective areas. System users are to be provided with the minimum access privileges required to perform permitted tasks.

Each systems user is responsible for the security, privacy and confidentiality of the Institutional Data to which he or she has access. Each system user is responsible for all transactions occurring during the use of his or her account. **Users must never share their passwords with others.** If a system user suspects that his or her password has been compromised, the password must be immediately changed. System users should log off or lock any administrative system when the user leaves his or her desk.

COPYRIGHT AND SOFTWARE LICENSES

The same standards of intellectual and academic honesty and plagiarism apply to software as to other

forms of published work.

Copyrighted materials belonging to entities other than Northwood may not be transmitted. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the University or legal action by the copyright owner.

Using Peer-to-Peer file sharing applications such as **Kazaa, Morpheus, Grokster, or similar applications** as a tool to download copyrighted music, videos and applications is a violation of Federal Copyright Law and the Northwood [Code of Ethics](#). Allowing other computers to gain access to copyrighted files on your system via the Northwood computer network is prohibited.

The license agreements for some pieces of software may specifically restrict the software to instructional use. This restriction, when applicable, is documented in the appropriate site software list, available from Information Technology. This document, or if necessary, Information Technology staff, should be consulted beforehand when planning the use of University-supplied third-party software for non-academic tasks in lieu of purchasing administrative licenses for this software.

Loading unauthorized applications or operating systems on any computer is prohibited. This applies to any program not explicitly licensed to the end-user or workstation by Information Technology, regardless of source (i.e., purchased by the user or obtained through public domain/shareware sources).

Deleting, copying, or altering programs without specific instructions from Information Technology is prohibited. Federal Copyright Law prohibits the use of unauthorized copies of computer software; this includes copying software belonging to the University for personal use. Northwood University does not condone illegal copying of software under any circumstances. Users are expected to strictly adhere to software license terms and the Northwood University Copyright Policy and Guidelines.

Software Downloads

To prevent computer viruses from being transmitted through the system there will be no unauthorized downloading of any software to University computer systems. In the event that software needs to be downloaded and installed on individual staff workstations, contact the Help Desk to have an Information Technology staff member coordinate the installation.

SYSTEM MONITORING

All messages created, sent or retrieved over the Internet are the property of the University and should be considered public information. The University reserves the right to access and monitor all messages and files on any computer system as deemed necessary and appropriate. Internet messages are public communication and are not private. No user should have any expectation of privacy as to his or her Internet usage. Information Technology staff members have the responsibility to report any violations of University policy, or state and federal laws to the Human Resources department or Dean of Students whenever such violations come to their attention. Monitoring specifics include:

- In the normal course of examining and repairing system problems, and when investigating instances of improper use of Northwood systems, the Information Technology staff may need to examine users' files, electronic mail, and printer listings.
- Investigations that discover improper use may cause the Information Technology staff to: limit the access of those found using facilities or services improperly; disclose information found during the investigation to University or law enforcement authorities; initiate disciplinary actions as prescribed by Northwood University policies and procedures.
- In order to protect against hardware and software failures, backups of data stored on Northwood University administrative and server systems are made on a regular basis. (Backups do **not** include personal computers.) The Information Technology staff has the right to examine the

contents of these backups to gather sufficient information to diagnose and correct problems with system software, or to investigate instances of improper use of University facilities.

- Information Technology staff may alter the priority or terminate the execution of any process that is consuming excessive system resources or objectionably degrading system or network response time, with or without prior notification.
- Information Technology staff may remove or compress disk files that are not related to the University missions or which are consuming large amounts of disk space, with or without prior notification.
- Information Technology staff may terminate login sessions that have been idle (unused) for long periods of time, in order to free resources.
- Information Technology staff has the responsibility to maintain confidentiality.

HARASSMENT

Harassing or defamatory material may not be sent via e-mail, instant message programs or posted to electronic bulletin boards, news groups or web pages. No messages with derogatory or inflammatory remarks about an individual or group's age, gender, race, religion, national origin, physical attributes, or sexual preference will be transmitted.

Harassment should be reported immediately to Information Technology, Human Resources, Security, or the Dean of Students.

SECURITY

It is Northwood University's policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

Access Codes and Passwords

The confidentiality and integrity of data stored on Northwood University's systems must be protected by access controls to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each user.

Information Technology may refuse or restrict access to any person or group that has violated the policies set forth in this document or any supplemental ones.

User Responsibilities

- To enable Information Technology to accurately maintain user information about each account, each user is responsible for supplying current information to the appropriate staff member including campus or department affiliation, degree program (undergraduate or graduate), expected graduation date or termination date, and University position (faculty, staff, or student).
- Students must provide proof of their student number and a photo ID at the time of account creation.
- Providing false or misleading information for the purpose of obtaining access to Northwood systems is a violation of University policy.
- Users are responsible for selecting a secure password for their account(s) and for keeping that password(s) secret at all times. Passwords are required to be changed every ninety days.
- Passwords should not be written down, stored on personal computer drives, or given to others.

- Passwords should not be given out to someone claiming to be an Information Technology staff member; authorized Information Technology members have full access privileges and do not need to know individual users' passwords.
- Use passwords containing both alpha and numeric characters.
- Users should log out when leaving his/her workstation.
- Users are responsible for reporting any system security violation, or suspected system security violation, to the Information Technology staff immediately.
- A user may not permit any other person, including other authorized users, to access University system resources through his/her account. Each user is responsible for any and all activity initiated in or on University systems by his/her account.
- Various contracts prohibit unauthorized users from using Northwood University equipment; thus, no unauthorized party may use Northwood University computer hardware or software. This includes, but is not limited to, family members and friends of employees.

Supervisor's Responsibilities

Managers and supervisors should notify Information Technology promptly whenever an employee leaves the University or transfers to another department so that his/her access can be revoked or changed as needed. Involuntary terminations must be reported concurrent with the termination.

GENERAL TOPICS

- Information Technology is responsible for all equipment purchases, installations, disconnections, modifications, and relocations. Employees are **not** to perform these activities.
- Any computer hardware or software purchased by Northwood University is the property of the University and is expected to be used on University premises, except for situations where computers are necessary and provided for work assignments away from Northwood offices.
- Users who borrow hardware, software, or documentation from Northwood University are responsible for its proper care, and for returning it in a timely fashion.
- Many Northwood systems are made available on an unmonitored basis. It is the responsibility of every user to act in such a manner as to not cause damage to physical equipment. Accidental damage, or damage caused by other parties, should be reported to the Information Technology staff as soon as possible so that corrective action can be taken.
- Modifying configuration of any computer, terminal, printer, or network device without prior approval of Information Technology is prohibited. Deliberate alteration of system files will be considered malicious destruction of University property.
- All Users are responsible for using University facilities in an effective, ethical, and lawful manner. Many resources, such as disk space, CPU cycles, printer queues, batch queues, login, and software licenses, are shared by all users. No user may monopolize these resources.
- The University has installed firewalls to assure the safety and security of the University's networks. Only those Internet services and functions with documented business purposes for the University will be enabled at the Internet firewall.
- Users are responsible for picking up their printer output in a timely fashion to avoid theft or disposal.
- Other organizations operating computing and network facilities that are reachable via Northwood systems may have their own policies governing the use of those resources. When accessing remote resources from Northwood University facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

ADVISORIES

Every effort is made by Information Technology to prevent the loss of data in the event of hardware or

ACCEPTABLE USE POLICY

- 7 -

software failure or through human error. Backups are regularly made of administrative systems and system servers. (Backups are **not** made of data stored on personal computers.) It must be recognized that in rare cases it may not be possible to restore the latest version of every data file from these backups and some data loss may occur. Because these cases are outside Information Technology's control, the staff cannot be held liable for any loss of data arising directly or indirectly from failure of hardware, software or from human error.

Information Technology staff has the responsibility to provide advance notice of system shut downs for maintenance, upgrades, or changes so users may plan around periods of system unavailability. However, in the event of an emergency, Information Technology staff may shut down a system with little or no advance notification. Every effort will be made to give users a chance to save their work before the system is taken out of service.

ACKNOWLEDGEMENTS

Merit/MichNET Acceptable Use Policy

Simmons, William R., Engineering Computer Network, Policy on Access and Usage, Purdue University

Randolph-Macon Woman's College Acceptable Use Policy

Whitworth College Computer Policy

Drexel University Security of Enterprise System Plan

Acknowledgment of Acceptable Use Policy

Procedure

Complete the following steps:

1. Read the "Acceptable Use Policy".
2. Sign and date in the spaces provided below.
3. Return this page only to Human Resources, Midland campus. Access to Northwood computer systems will be denied until the signed agreement is received.

Signature

By signing below, I agree to the following terms:

- i. I have received and read a copy of the "Acceptable Use Policy" and understand the same;
- ii. I agree to abide by the terms and conditions of this document when using Northwood University supplied equipment and/or software.

Signature: _____

Printed Name: _____

Date: _____