NORTHWOOD UNIVERSITY'S
INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

Information Technology ("IT") resources are provided by Northwood University ("NU" or "the University") to its students, faculty, administrators, staff, contract employees and those who may be granted a guest computer account on a request basis, in support of the University's mission. These resources include, but are not limited to, technologies and information resources required for information processing, storage, and communication, whether individually controlled or shared, stand-alone or networked. This includes in-lab and classroom technologies, electronic resources, and computing and electronic communication devices and services, both wired and wireless such as, but not limited to, computers, printers, hand held devices, e-mail, instant messages, blogs, Voice over Internet Protocol (VoIP), fax transmissions, voice, data, and video communication networks, multi-media, instructional materials, and academic and administrative systems. Personal equipment connected to the University network is also subject to this policy. These guidelines apply to any user of any IT resource provided by the University and attached to the University network.

Access to University IT resources is a privilege and must be treated as such by all users of these systems. This policy outlines your responsibility in the use of these resources and is based upon the following principles:

- Electronic resources are provided for the purpose of carrying out the mission of the University.
- Your use of information resources must comply with University policies and the law.
- Your use of these resources does not cause harm to others or the electronic resources themselves.
- You are expected to use these resources ethically and responsibly.

Any member of the community who violates this policy is subject to disciplinary action as stated in this policy and possible legal action including, but not limited to, the Federal Electronic Communication Acts. In addition, the University community is bound by the NU Code of Ethics in the use of computer resources.

Other organizations operating computing and network facilities that are reachable via NU systems may have their own policies governing the use of those resources. When accessing remote resources from NU facilities, users are responsible for obeying both the policies set forth in this document and the policies of the other organizations.

ACCESS

A. General Use and Ownership

NU's IT Department is responsible for all equipment purchases, installations, disconnections, modifications, and relocations. Employees or students are **not** to perform these activities without prior written approval of the IT Department. All IT resources, systems, and services are the property of NU. These include but are not limited to, all computers and software owned by the University, any communications hardware and software provided by the University for the purpose of accessing its computers, any computer network governed in part or whole by the University, all components of the electronic communications, physical infrastructure, and any electronic communications address, number, account, or other identifiers associated with the University. All said property is expected to be used on University premises, except for situations where computers are necessary and provided for work assignments away from NU.

Users who check out hardware, software, or documentation from NU are responsible for its proper care, and for returning it undamaged in a timely fashion.

The University shall not be liable for, and the user assumes the risk of inadvertent loss of data or interference with data resulting from the University's efforts to provide and maintain the University's IT resources.

The University is not responsible for the content of users' personal web spaces, nor the content of servers, programs or files that users maintain on University IT resources or on personally-owned computers or other devices connected to the University's IT resources.

B. Access

NU provides and maintains a NU Access ID for each registered student, faculty, administrator, staff, contract employee and those who may be granted a guest computer account on a request basis. NU reserves the right to withdraw the service from anyone who misuses the system or IT resources.

Third party individuals may be provided access to University IT resources through sponsorship by an appropriate University administrator.

No unauthorized individual may use University IT resources, computer hardware or computer software. This includes, but is not limited to, family members and friends of faculty, administrators, staff, contract employees, and students.

The University reserves the right, at its sole discretion, to limit, restrict, or terminate any account or use of University IT resources, and to inspect, copy, remove or otherwise alter any data, file, or system resources which may impair or damage University IT resources or authorized use.

The University also reserves the right to inspect or check the configuration of computers and any communications hardware provided by the University for compliance with this policy, and to take such other actions as its sole discretion it deems necessary to protect the University’s IT resources.

System users and units of the University are required to report transmitting devices and their characteristics to the University IT Department and officials, if so requested. The University reserves the right to require those units or individuals found to have such devices which interfere or are suspected to interfere with operation of University systems, to discontinue use of such devices and, if necessary, to remove them from University property.

In the event of a threat to the security or reliability of the University’s IT resources, the University may suspend, terminate, or deny access of those involved in a suspected threat, violation, or misuse while the threat, violation or misuse is being investigated, or to otherwise prevent inappropriate activity. The University may also take other actions to preserve the security or reliability of the University’s IT resources and the integrity of files and other relevant information.

C. Use

Those who use University IT resources are expected to do so responsibly. They must comply with local, state and federal laws and regulations, with this and any other University policies and procedures and with normal standards of personal courtesy and conduct.

EXPECTATIONS

As a user of IT resources at NU, you can expect:

A. Security of PCs, Laptops, and Work Stations

All PCs, Laptops and Work Stations are secured with a password-protected screensaver and the automatic activation feature set at 15 minutes or less when idle.

Please note, however, there is no guarantee of security and some NU systems and resources are made available on an unmonitored basis. It is the responsibility of every user to act in such a manner as to not impair security and not to cause damage to University physical equipment or IT resources.

B. Protection of Inbound and Outbound E-mail and Attachments

NU’s IT Department makes reasonable efforts to scan inbound and outbound e-mail and attachments for spam. NU’s IT Department also continuously scans all e-mail with virus scanning software with a current virus database for anything that could be a threat to the system such as viruses and Trojan Horses (Trojans). The scanning for threats may lead to a modification of e-mail headers, non-delivery of messages containing viruses or Trojans, deleting of attachments, and blocking of messages. NU’s IT Department reserves the right to block e-mail that exhibits characteristics of spam, viruses, Trojans or anything else that could threaten the University’s network infrastructure or IT resources.

Users must still use extreme caution, however, when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, and Trojans.

C. Electronic Communications and Files

NU follows generally accepted security measures, but cannot guarantee electronic communications are completely protected from unauthorized access by individuals who possess the skill and desire to breach security measures. Therefore, e-mail and other types of electronic communications should not be used to communicate confidential or sensitive matters.

The University reserves the right to audit, inspect, and monitor networks and systems and/or disclose electronic communications in transit or storage without consent of the holder on a periodic basis:

- When required by and consistent with law (i.e., search warrants, subpoenas, freedom of information requests).
- When there is a reason to believe a violation of law, University policy, rules, regulations or procedures has taken place.
- To maintain the security or performance of the infrastructure.
- To ensure compliance with this Policy.

Users must be aware that networks, systems, and all electronic communications:

- May be accessed and monitored in the normal course of business by system administrators.
- May be released to the public (as may be requested through the Freedom of Information Act).
- May require special measures to gain or limit access.
- May be subject to preservation, seizure, discovery proceedings and disclosure and publication in legal actions.

There is no expectation of privacy on any NU network or system.

RESPONSIBILITIES

Protecting NU's systems, data, networks, and IT resources is the responsibility of everyone in the university community. You are responsible for all activity on your account. This includes, but it not limited to, destructive or illegal activity by someone using your account identity.

NU's Information Technology Acceptable Use Policy does not and is not intended to create any legal duties, liabilities, or warranties by NU and use of NU's IT resources is provided on an "as is" basis and makes no and expressly disclaims all representations or warranties of any kind, express, or implied, with respect to NU and does not create any contractual, or other legal rights in, or on behalf of any other party.

A. Protecting IT Resources from Physical Access

You are responsible for the physical security of Information Technology devices you use and the data they contain. Keep doors locked to protect equipment. Portable equipment such as notebook computers, Personal Digital Assistants (PDAs), and mobile phones must be secured whether on campus, traveling, or at home. Confidential or sensitive documents and data should be encrypted.
Keep your account secure by preventing others from getting access to your computer.

Log off or lock IT resources/devices before leaving them unattended.

B. Protecting IT Resources from Unauthorized Electronic Access

Authorized NU users are responsible for the security of their passwords and accounts. Persons attempting to gain unauthorized access to a system often do so through user accounts, and your password is a safeguard against such access. Keep passwords secure and do not share accounts. If you suspect someone may have discovered your password, change it immediately. It is required that user passwords be changed, at a minimum, every 180 days.

NU's IT Department will NEVER ask you to send your account information or password over e-mail.

C. Use E-mail and other Electronic Communications Responsibly

All University electronic communications are to be used in an ethical and responsible manner.

Messages such as e-mail should meet the same standards for distribution or display as if they were hard copy documents. Identify yourself clearly and accurately in all electronic communications.

If by accident you receive a confidential file, you should not share it with anyone else.

D. Using Resources Responsibly, Efficiently, and Fairly

Each user should make efficient use of network resources. No user may monopolize these resources. Do not use your computer as a server. Users are also responsible for picking up their printer output in a timely fashion to avoid theft or disposal.

NU faculty and staff may use the University Information Technology resources for incidental personal purposes provided such use does not:

- Directly or indirectly interfere with the University operations and services.
- Burden the University with noticeable incremental cost.
- Interfere with the user's employment or other obligations to the University.

- Violate the law, University policies or procedures, or reasonable standards of decency and civility.

Electronic records arising from such personal use may, however, be subject to the presumption of being a University electronic record.

E. Complying with University Policies, Rules, and State and Federal Laws

Users of University IT resources agree to comply with applicable federal and state laws and the policies, standards, and procedures of the University and of any Internet service provider for the University. Under no circumstances is an employee of NU authorized to engage in any activity that is illegal under local, state, federal or international laws while utilizing NU-owned resources.

Users shall also abide by the EDUCOM code regarding ethical and legal use of software as referenced below:

> Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. (http://net.educause.edu/ir/library/html/code.html)

All NU employees and students shall use software only in accordance with the license agreement. To transfer the possession without permission, of any copy, modification or merged portion of any licensed program, whether gratuitously or for gain, violates this Policy and is prohibited. Anyone who makes, acquires, or uses unauthorized copies of computer software or otherwise violates this Policy shall be subject to disciplinary action in accordance with University policy. They may also be subject to personal liability under copyright law. Anyone using personal software on University devices must demonstrate evidence of ownership.

University IT resource users must not place copyrighted material that they do not have the copyright holder's permission to access or possess on the University's IT resources or on personally-owned devices or systems connected to the University's IT resources. University IT resource users shall not engage in unauthorized copying, transmission, distribution or downloading of such works. System users are ultimately responsible for ensuring that the copyright holder has granted permission to make or distribute the copy in question. Suspected misuse of copyrighted materials may result in the exercise of the University's investigatory rights with or without notice to the user and suspension from University IT resources. Also, the user may be subject to University discipline and civil, or criminal liability.

UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). The list below of prohibited activities is not all inclusive; rather, it includes examples of what NU considers to be clearly inappropriate behavior and unacceptable uses of its Information Technology resources.

- Violation of the rights of any person or NU intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NU or the owner of the computer.

- Unauthorized use of copyrighted material including, but not limited to, photographic images or copyrighted music, and the installation of any copyrighted software for which NU or the end user does not have an active license.

- Any activity by which an individual violates such matters as University or third party copyright or patent protections, as well as license agreements or other contracts.

- Using University resources for Peer-to-Peer (P2P) file-sharing applications such as Kazaa, Limeware, Shareaza, BitTorrent, or similar technology to upload, download, acquire, store, use, distribute or otherwise transmit unlicensed copyrighted works including, but not limited to, music, videos, games, software and digital media is a violation of Federal Copyright Law and the Northwood Code of Ethics. Allowing other computers to gain access to copyrighted works on your system via the University IT resources or computer network is prohibited.

- Introduction of malicious computer codes or programs into any University-owned electronic resources, networks or servers, or on the device of another.

- Disclosure of an account password, or an attempt to access, or actual access to an Information Technology resource by providing false or misleading information.

- Use of an Information Technology resource such as e-mail, telephone, paging, text messaging, instant messaging, or any other new electronic technologies that may emerge, to create, post, transmit material or messages that violate NU's policies against discrimination, harassment on account of age, race, religion, sex, ethnicity, nationality, disability, height, weight, marital status, familial status, or other protected class, status or characteristic or other applicable laws.

- Use of an Information Technology resource to threaten another person's physical safety, or to intentionally, recklessly or negligently harm others.

- Use of an Information Technology resource for illegally participating in the viewing or exchange of pornography.

- Use of an Information Technology resource for commercial gain, product advertisement, or political activities without authorization of the University.

- Use of an Information Technology resource to make fraudulent offers of products, items, or services.

- Deliberate disruption of NU's computer systems, networks, or other Information Technology resources.

- Port scanning or security scanning without prior approval by NU's IT Department.

- Circumvention of user authentication or security of any host, network or account.

- Use of an Information Technology resource to access or transmit the files or communications of other students, faculty, or staff without authorization, or to provide information about, or lists of, students, faculty or staff to persons, groups, or organizations outside the University without authorization.

- Use of an Information Technology resource to create or forward "chain letters", "Ponzi", or other "pyramid" schemes of any kind.

- Unauthorized use of e-mail header information or forgery of e-mail header information (e.g., sending or posting electronic mail or other communications while misrepresenting or concealing the true identity, role, identification, address, signature, or indicia of another person, organization or entity of the sender or author).

- Accessing a computer, the NU system, or other devices without appropriate permission and without following proper login procedures.

- Tapping a network or running a "sniffer" program.

- Using software tools that attack Information Technology resources.

- Causing or allowing access, modification or destruction of any files, programs, settings, or data transmitted or stored by any device without permission.

- Unauthorized destruction, alteration, dismantling, disfiguring, or preventing rightful access to, or otherwise interfering with the integrity of NU Information Technology resources, computer-based information, or information resources.

- Sending unsolicited e-mail messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (e-mail spam)

- Soliciting e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

- Creating or forwarding e-mail bombing attacks (intentional e-mail transmissions that disrupt normal e-mail service).

- Creating or intentionally sending viruses or other harmful programs or files.

- Modifying the configuration of any computer, terminal, printer, or network device without prior written approval of the IT Department is prohibited. Deliberate alteration of system files will be considered malicious destruction of NU property.

- Deliberately disrupting the NU computer systems, networks or other IT resources.

- Individual or departmental deployments of wireless networks are not allowed. NU provides wireless access. Any unauthorized wireless access point found connected to the campus network will be considered a security risk and disabled.

CONSEQUENCES

Any employee found to violate local, state, federal or other applicable laws, NU policies, procedures or standards of conduct, is subject to disciplinary action under University policy. Any suspected violation of local, state, federal or other applicable laws may be reported to the appropriate legal authority.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution
- If you break the law, you can be prosecuted. Even if you are not charged or convicted criminally, you can be held personally liable, and you can be suspended or dismissed from the University.

Any student found to violate federal or state laws or regulations, NU policies, procedures or standards of conduct, will be subject to disciplinary action under NU's Student Code of Conduct. Any suspected violation of state or federal laws or regulations may be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including suspension or expulsion from school.
- Criminal prosecution.
- If you break the law, you can be prosecuted. Even if you are not charged or convicted criminally, you can be held personally liable, and you can be suspended or dismissed from the University.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action. The University may also refuse or restrict access to any person or group that the University in its sole discretion determines has violated the policies set forth in this document or any supplemental ones.

The University reserves the right to suspend access to University IT resources or to impose other restrictions if users are believed to have been operating in violation of either law or University_policy governing IT resources. The University retains the right, subject to applicable law and policy, to search and seize, for investigative purposes, any hardware or systems connected to University IT resources if there is cause to suspect that such hardware or systems were used in violation of law, or University policies governing IT resources. Restoration will be at the sole discretion of the University. The University will, to the full extent required under law, cooperate with all legal requests for information, including, but not limited to, disclosure of system user account information when properly made by law enforcement or legal representatives pursuant to court order, subpoena or other legal process.

REPORTING AN INCIDENT

If an incident is a threat to personal safety, immediately contact Campus Security or other local law enforcement agencies.

Any incident involving the misuse of IT resources, a security violation, or suspected security violation should be reported to the IT Department as soon as possible orally and in writing so that corrective action can be taken, if necessary. Users are also responsible for cooperating in any NU investigation into any suspected misuse of IT resources or suspected security violation. Accidental damage, or damage caused by other parties, should also be reported to the Information Technology staff as soon as possible so that corrective action can be taken.