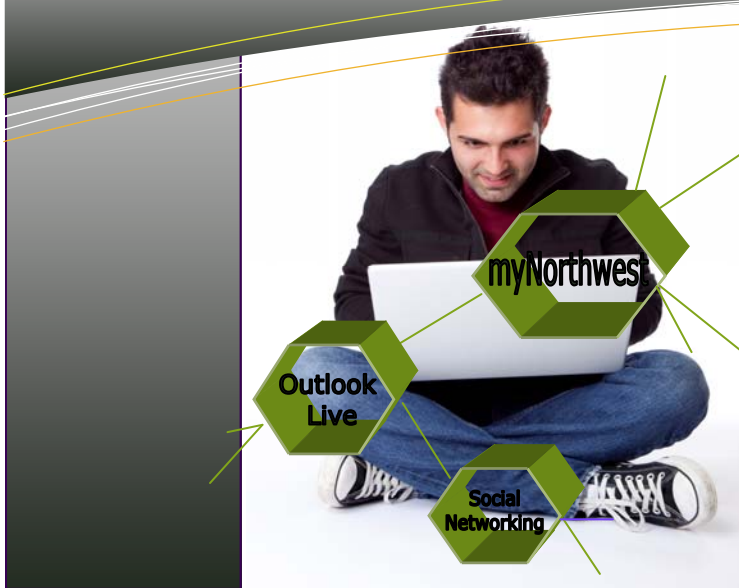


2011 Computer User's Guide

to the Electronic Campus



Acceptable Use	1
Network Stability Assurance	1
Campus Network Violations	1
What is Prohibited & Why?	2
Acceptable Resources & Uses	3
Network Legal Issues	4

It is the policy of Northwest Missouri State University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Access to this environment and campus information technology resources should be considered a privilege and must conform with all laws, with Northwest policies and with any policies specific to a resource. For more detailed information regarding acceptable usage of the Northwest network review the following policy sections, or see the *Computing Policies* web page at:

<http://www.nwmissouri.edu/compserv/ClientComputing/ComputingPolicies.htm>

Network Stability Assurance

Preserving access to information resources is a community effort that requires each member to act responsibly to safeguard network performance and stability. Therefore, both the community as a whole and each individual user have an obligation to abide by the standards set forth in this document to assure network stability and availability.

The *policies* stated in this document outline the standards for *acceptable use* of Northwest's information technology (IT) resources that include, but are not limited to, networks, hardware, software, data and telephone lines whether owned, leased or otherwise provided by Northwest. These policies *apply to all* faculty, staff, students and guest users.

University IT resources, including bandwidth itself and IP addresses, belong to Northwest Missouri State University. These resources do *not* belong to *end-users*. The computing

policies *ensure* the *availability* of campus shared resources and approved uses are *not* interrupted. *Information Systems* will manage and allocate bandwidth by application priority.

Campus Network Violations

Certain types of hardware and/or programs are prohibited on the campus network except those maintained by *Information Systems*.

Information Systems will actively monitor for the use of these types of hardware and software. If prohibited hardware or software is detected, university staff will attempt to notify the users to have them remove the hardware or software from the Northwest network. If the hardware or software is adversely affecting network performance and stability, it will result in the immediate disconnection of network connectivity.

Equipment and programs that are considered violations on the Northwest campus include, but are not limited to, the following:

- Game Consoles and Modems
- Web cams and Video Instant Messaging
- DHCP and NAT equipment
- DNS or DDNS
- Packet Sniffer or Network Data Capture Applications
- Network routers and Cable/DSL routers
- Network/Port Scanners and VPN Servers
- Wireless LAN devices and 2.4 GHz ISM band devices

See the next section for further details about these and other prohibited equipment and programs.



What is Prohibited & Why?

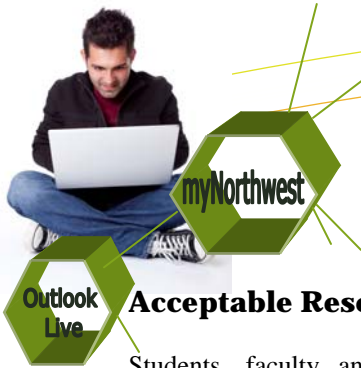
The list below are violations because they can and will interfere with the normal operations of the network. Such programs and devices interfere by doing the following: a) taking up too much bandwidth and thus, slowing down the network, b) interfering with the campus firewall, which can result in network downtime, c) try to incorrectly take over a network operation that is currently performed by Northwest networking equipment, which can negatively impact the network's functionality, or d) act as a "spy" to gain access to private data.

- **DHCP (Dynamic Host Configuration) or NAT (Network Address Translation) Equipment.** Software or equipment that provide DHCP services or operate as NATs are not permitted.
- **DNS (Domain Name Server) and/or DDNS (Dynamic Domain Naming System).** Equipment that provides DNS or DDNS services is not permitted on the Northwest network.
- **Modifying physical network [MAC] addresses is prohibited.**
- **Network/Port Scanners.** Equipment or programs that probe other equipment connected to the Northwest campus in order to gather information about services provided by that equipment are not permitted on the Northwest network.
- **Packet Sniffer or Network Data Capture Applications.** Equipment or programs that listen, read, capture or *sniff* network traffic not specifically intended for receipt by that equipment are not permitted.
 - * A packet *sniffer* is the same concept as a *wiretap* on a telephone line.
- **Network Routers and Cable/DSL Routers.** Equipment that provides TCP/IP subnet routing services is not permitted on the Northwest network.
- **VPN (Virtual Private Network) Servers.** A VPN Server that provides access to the campus network is not permitted.
- **Wireless LAN Devices.** Wireless LAN devices, including wireless printers, are prohibited except those maintained and configured by *Information Systems*.
- If you enable Internet Connection Sharing so that your computer functions as an access point for other devices, thus, turning it into a router, you are in violation of Northwest policy.

- **Other Wireless Devices, 2.4 GHz ISM Band.** *Information Systems* reserves the right to restrict or prohibit the use of any equipment that uses the 2.4 GHz radio frequency to ensure the stability of the Northwest's 2.4 GHz network. This includes, but is not limited to, wireless printers.
- **Modems.** Modems providing dial-in services are not permitted if the dial-in connection provides access into the Northwest network.
 - * Modems providing dial-out service are permitted if the computer is not concurrently connected to the Northwest network and the dial-up service.
- **Game Consoles.** Game consoles are prohibited from connecting to the Northwest network.
- **Webcams and Video Instant Messaging.** Webcams and video instant messaging are both prohibited on the Northwest network.

Want to play network games, operate a webcam and use video instant messaging? You can purchase DSL service independently through the local telephone company. Be sure NOT to connect to the DSL service and the Northwest network simultaneously.

- **Setting or Resetting Traffic Priority.** Any attempt by client PCs to set or reset priority for traffic on the Northwest network is prohibited.
- **Other Services and Servers.** A server is defined as any machine or device that provides files or services using the campus network or sends more data than it receives. Examples:
 - * FTP and FXP Servers.
 - * HTTP (World Wide Web) Servers.
 - * IRC, Mail and Domain Logon Servers.
 - * MP3, Music, or Video Servers.
 - * Open File Servers or shares.
 - * Browse Master & Tunneling Programs.
 - * Network game software, including emulators.
 - * Peer-to-Peer File Sharing Programs.
 - * Remote Access or Remote Management software.
 - * Any software or hardware that bypasses network management tools such as the campus firewall.
 - * Any other equipment that is determined by *Information Systems* to interfere with the normal operation of the Northwest network.
- Do not load another operating system on your university-provided notebook or tablet computer.



Acceptable Resources & Uses

Students, faculty and staff *may use* the Northwest network for *most* academic and personal tasks, such as searching the internet, chatting via a messenger program, sending email and any other activity that does not negatively impact the normal operations of the campus network.

Some other *acceptable uses* of the campus network include the following:

- Sharing a printer.
- The sharing of files on your computer for your personal use, academic class or academic team collaboration.
 - * Sharing must be limited to access by Northwest username and password.
 - * Additionally, sharing must be limited to Microsoft *Windows* sharing capabilities by use of said Northwest username and password.
 - * When sharing do not share to the entire network, but rather to a specific user or users.
 - * Be aware that enabling the *share* option on hard-disk files will permit *anyone* connected to the campus network to read and possibly modify your computer's data.

- Recreational and academic *ports* may be *requested* and are evaluated on an individual basis. Any opened ports will be closed at the end of the Spring trimester.
- Resources and servers maintained or authorized by *Information Systems*.

Want to play network games, operate a web-cam and use video instant messaging? You can purchase DSL service independently through the local telephone company. Be sure NOT to connect to the DSL service and the Northwest network simultaneously.

Legal sources of online content can be found at:

<http://www.educause.edu/legalcontent>

If you have questions regarding campus computing policies or would like to have a port opened, please see **Online Support** at:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/index.htm

The above web page should answer most questions. However, if it does not, please contact the *Information Systems—Client Computing Help Desk* at 660-562-1634 or helpdesk@nwmissouri.edu.

Installing Personally Owned Software on University Provided Notebook Computers

Students, faculty and staff wanting to install personally-owned software on Northwest notebook computers may do so, as long as they are an administrator on the notebook computer they want to install software on.

Students, faculty and staff are administrators on the notebook computer they were issued through the Jon T. Rickman *Electronic Campus Support Center* (ECSC).

If you install a program and it does not work, immediately uninstall the program within the Control Panel using the Add/Remove Programs tool.

The ECSC is not responsible for backing up (copying) personal files or non-university provided software on personally-owned computers. The ECSC is also not responsible for backing up personal files or non-university provided software on university-provided notebook computers.

Need Help?

If you have questions about installing personally-owned software on a Northwest notebook computer, contact the *Information Systems—Client Computing Help Desk* at 660-562-1634.



A Word About Wireless

Faculty, staff and students with a valid Northwest Network Account (username and password) should have no trouble using the Northwest secure wireless network. There is a non-secure wireless network available in select buildings for use to those with personally owned notebook computers that do not have a valid Northwest Network account.

Wireless is active in several classrooms and most public areas including, but not limited to, Owens Library, the Station, Student Un-

ion, Forest Village Community Building, South Complex and Roberta lobbies, Valk entry (center), Colden Hall (3rd level center), Garrett-Strong (2nd level center), Fine Arts entry (center) and the Administration Building (3rd level). All campus computing policies apply to the campus wireless network. See the *Wireless Connection* link on the Online Support web page at:

http://www.nwmissouri.edu/compserv/ClientComputing/Online_Support/index.htm



Network Legal Issues

Anyone using Northwest computing resources are required to follow the *acceptable use* policy of the *Missouri Research and Education Network* (MOREnet), Northwest's internet service provider (ISP). See the following web page for MOREnet policy:

<http://www.more.net/?q=content/service-policies>

Northwest provides access to IT resources for students, faculty and staff in support of Northwest's educational mission statement and official academic duties. When logging onto the Northwest network, a user implicitly affirms that they will abide by Northwest's computing and networking policies.

The following is illegal and unethical on the Northwest network:

- It is illegal to acquire access and use services and data that do not belong to you.
- It is illegal to copy or delete data that is not yours.
- It is illegal and unethical to view, reproduce, alter or distribute child pornography.
- It is illegal to display sexually explicit material in a public place where a minor potentially might view the material.
- It is illegal to possess, distribute or otherwise access and use adult or child pornography in violation of state or federal law.
- Likewise, it is unacceptable and unethical to access or use any sexually explicit material without a bona fide official or educational purpose in open areas or work areas of the university.

The above legal concepts and guidelines apply to all media. Please see the *Judicial Code* in your *Student* or *Faculty/Staff Handbook* for further campus policies. Listed below are various Northwest network regulations and *Judicial Code* violations of the network:

- Do not disjoin your university-provided notebook computer from the NWMSU domain.
- Do not rename your campus-provided computer.
- Do not use Northwest's IT resources to gain unauthorized access to a computing resources on or off campus.

- Do not install servers on the Northwest network. Servers are not permitted except for those approved by *Information Systems*.
 - * A server is defined by *Information Systems* as any device that provides files or services using the campus network or sends more data than it receives.
- Do not plagiarize or infringe on the privacy rights, intellectual property rights or copyrights of others.
- Do not distribute or copy, through any mechanism, electronic or otherwise, a program, music, motion picture or other type of digital media without proper authorization. Please see the *Copyright Policies* section of the *User's Guide*.
- Do not install programs or hardware that might interfere with the intended operations of the Northwest network or computing equipment.
- Do not prevent, interfere or harass users utilizing Northwest IT resources.
- Do not create, distribute or use any program that may damage or negatively impact another user on the Northwest network.
- Do not send email or Net Send messages to unwilling recipients.
- Protect the access and integrity of technology resources and user account information.
 - * Users are responsible for maintaining security by protecting their personal files, usernames, passwords, accounts, and printouts from unauthorized users.
- Do not open a file or run a program sent to you unless you thoroughly trust the source and know what the file or program does.
- Do not use university IT resources for personal profit. Online gambling is considered a personal profit activity.
 - * Please see the campus *Judicial Code* in your student or faculty/staff handbook for further policies regarding this and other issues.
- Do not use Northwest IT resources to advertise or solicit sales that violate the university's solicitation policy.
- Do not assign an IP address to a computer on the Northwest network without authorization from *Information Systems*.