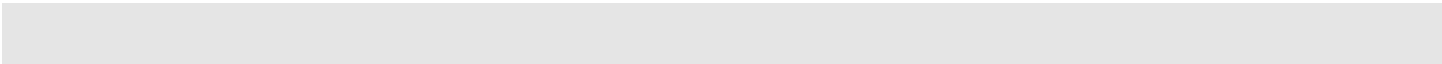
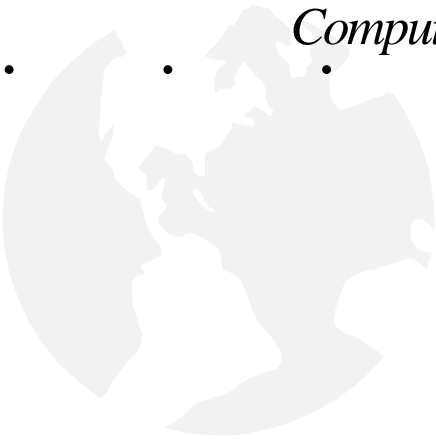


Information Services

Computer and Network Use Policy



.....

Computer and Network Use Policy

| | |
|---|-----------|
| <u>Policy Development Process</u> | 4 |
| <u>Policy Purpose</u> | 4 |
| <u>Authorized Users</u> | 4 |
| <u>Appropriate Use</u> | 4 |
| <u>Electronic Mail Use</u> | 6 |
| Purpose | 6 |
| Spamming | 7 |
| Personal Use | 7 |
| Cautions: | 7 |
| <u>Campus Software</u> | 8 |
| Standard Software | 8 |
| Area Software | 8 |
| Restricted Software | 8 |
| Local Software | 8 |
| <u>Internet Use</u> | 8 |
| <u>Network Drive Access</u> | 9 |
| N: Drive Space Limitations | 9 |
| Purchasing Additional N: Drive Space | 9 |
| <u>Student Labs and Classrooms</u> | 10 |
| Non-Academic Use of Lab Computers | 10 |
| Printing | 10 |
| <u>Dial-in Access and Use</u> | 10 |
| Eligibility | 10 |
| Requirements for Access | 10 |
| Cost of Access | 10 |
| Limitations of Access | 11 |

| | |
|---|----|
| Limitations of Responsibility _____ | 11 |
| <u>Dormitory Access</u> _____ | 11 |
| <u>Networked Computers</u> _____ | 11 |
| Desktop Computers and Peripheral Devices _____ | 11 |
| Servers _____ | 11 |
| Personally owned computers _____ | 12 |
| Assignment of IP Addresses _____ | 12 |
| <u>Privacy Issues</u> _____ | 12 |
| <u>Intellectual Property</u> _____ | 13 |
| <u>Termination of Accounts</u> _____ | 13 |
| <u>Personal Use</u> _____ | 13 |
| Incidental Use _____ | 13 |
| Commercial Use _____ | 13 |
| <u>Sanctions</u> _____ | 14 |
| <u>Student Computer Support</u> _____ | 14 |
| Goals _____ | 14 |
| Support Resources _____ | 14 |
| NNU-Owned Computers _____ | 15 |
| NNU-Standard Laptops (LAWN program) _____ | 15 |
| Student Owned Computers _____ | 15 |
| Support Specifically Not Provided _____ | 16 |

Policy Development Process

1. The Computer and Network Use Policy is intended to be a dynamic, "living" document. Consequently, the policy will be reviewed on an annual basis. Such reviews are intended to assess the efficiency and effectiveness of the policy and provide an established process for amending the policy. Questions should be directed to the Director of Information Services.

Policy Purpose

The purpose of this document is to assure that:

1. The Northwest Nazarene University (NNU) community is informed about the applicability of policies and laws concerning the computers and network on the NNU campus.
2. The users of the computer services are informed of their rights and responsibilities concerning these policies.
3. Disruptions to University computing services are minimized.

Authorized Users

1. An authorized user of the NNU network is a person who has been issued a valid account to access network services.
2. Authorized users include, but are not limited to students, faculty, administrative personnel, staff and retired faculty.
3. A computer user must not seek to gain unauthorized access to information resources or to facilitate unauthorized access by others. Sharing a network login and password with others constitutes unauthorized access.

Appropriate Use

The following list does not cover every situation that pertains to proper or improper use of the resources, but it does suggest some of the responsibilities that authorized users accept if they choose to use a University computing resource or the network access that NNU provides.

1. For any computer account, the user is responsible for the use made of that account. The user should set a password which will protect their account from unauthorized use, and which will not be guessed easily. If a user discovers that someone has made unauthorized use of their account, the password should be changed and the intrusion reported to the Office of Information Services. Passwords should be changed on a regular basis, to assure continued security of accounts. Accounts are assigned to individual users and users must not share passwords with others. This password should include letters and numbers and should not be a word found in the

dictionary or containing any personal information. Examples of bad passwords are: name, birth date, college, church, Chevy. Good passwords would be: A#Ty17AQ!p or Wh9en8t0go.

2. Users must not intentionally seek information about, browse, copy, or modify files or passwords belonging to other people, whether at NNU or elsewhere, unless specifically authorized to do so by those individuals. If an individual has explicitly and intentionally established a public server, or clearly designated a set of files for shared public use, others may assume authorization. However, if it is unclear whether some files are intended to be available for public use or not, the user should assume that they are private files and are not intended for public access.
3. Authorized users must not attempt to decrypt or translate encrypted material not intended for them, or obtain system privileges to which they are not entitled. Users must refrain from any action that interferes with the supervisory or accounting functions of the systems or that is likely to have such effects. If a gap in system or network security is encountered or observed it must be reported to the office of Information Services.
4. No authorized user or members of the NNU community may, under any circumstances, use NNU computers or networks to libel, slander or harass any person. Computer harassment includes:
 - Intentionally using a computer to trouble, intimidate or threaten another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's family.
 - Intentionally using a computer to contact another person repeatedly with the intent to harass, whether or not any actual message was communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease.
 - Intentionally using a computer to disrupt or damage the academic, research, and administrative or related pursuits of another.
 - Intentionally using a computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.
 - Intentionally using a computer to send or display defamatory, pornographic, obscene, or patently offensive sexual materials.
5. Users must avoid wasting computing resources. Following is a partial list of items that may be considered wasteful use of computer resources:
 - Excessive game playing or other trivial applications (Networked gaming should only be done in dorm labs during low-use times, such as Friday night)
 - Sending chain letters or other frivolous or excessive messages locally or over an attached network

- Printing excessive copies of large documents, files, images, or data, or printing documents or files numerous times because they have not been checked thoroughly for all errors and corrections

Users must be sensitive to the specialized nature of software, hardware, and services available in a limited number of locations, and allow access to those people whose work requires these specialized facilities.

6. Authorized users must not prevent others from using shared resources by running unattended processes or placing signs on devices to "reserve" them without authorization from the appropriate system manager. Absence from a public computer or workstation should be no longer than warranted by a visit to the nearest rest room. A device unattended for more than ten minutes may be assumed to be available for use, and any process running on that device terminated.
7. The University presents for use many programs and data which have been obtained under contracts or licenses specifying they may be used but not copied, cross-assembled, or reverse-compiled. The user is responsible for determining that programs or data are not restricted in this manner before copying them in any form, or before reverse-assembling or reverse-compiling them in whole or in any part. If it is unclear whether such permission has been granted, assume that it has not.
8. If a user creates or maintains electronically stored data that is important to their work or to the University in general, the user is responsible for the backup of that data. The University does backup data on its network drive at regular intervals as preparation for a catastrophic loss of resources. However, the user must decide whether or not this is an adequate substitute for making personal backups of the data the user creates or maintains.
9. Authorized users must not create or willfully disseminate computer viruses. Users should be sensitive to the ease of spreading viruses and should take steps to ensure that files are virus free.
10. Students forgetting their network password during a school year will be assessed a fee to get a new password. A request for a replacement password must be submitted to Media Services.

Again, the above are only examples and not an exhaustive list. Users should also be aware that there are federal, state and sometimes local laws that govern certain aspects of computer and telecommunications use. Members of the NNU community are expected to respect these laws, and to observe and respect University rules and regulations.

Electronic Mail Use

Purpose

Email services are to be provided to the NNU community for purposes of academics, administration, and communication important to community-building.

Spamming

Computer users must not send unsolicited email to the students, group of students, employees or group of employees without approval from the Office of Information Services. Computer users must not forward electronic chain letters to any person, on or off campus, except to forward a message to the Director of Information Services. Either of these offenses may result in the user's account being disabled immediately until they can be personally reminded of the policies in this document. Note: Faculty members may send email to the faculty distribution list or listserv without prior approval.

Personal Use

University electronic mail services may be used for incidental personal purposes provided such use does not:

1. Directly or indirectly interfere with the University operation of computing facilities or electronic mail services;
2. Burden the University with noticeable incremental cost;
3. Interfere with the email user's employment or other obligations to the University.
4. Result in personal financial gain, except in an incidental manner.

Cautions:

Users should be aware of the following:

1. Email is less private than users may anticipate. While the network manager will do as much as possible to protect data stored on NNU servers, an Email message intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on a listserv, for example, may be distributed to all subscribers to the listserv. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities, and thus be subject to disclosure under State and Federal law. The University cannot routinely protect users against such eventualities.
2. Email stored on University equipment, whether or not created on University equipment, may constitute a University record subject to disclosure under the state and federal laws, or as a result of litigation. The University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the laws concerning disclosure and privacy
3. The University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can the University, in general, protect users from receiving electronic mail they may find offensive. Members of the University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.
4. There is no guarantee that Email received was in fact sent by the purported sender. It is, however, a violation of this Policy for senders to disguise their identity.

Campus Software

Software available on the campus of NNU comes in several different varieties. All users must know that **all software loaded on any computer owned by NNU must have appropriate licenses and these licenses must be filed in the Software License File maintained by Information Services.**

Standard Software

Information Services provides a number of software applications that are available for general use on the campus. It is the responsibility of Information Services to maintain these software applications with the current versions and patches to make it as easy to use as possible. The licenses are purchased and maintained for general campus use. In some cases, the software licenses limit the number of simultaneous users of the product. The campus wide software includes, but is not limited to, Windows 98, Microsoft Office 2000 Professional (Word, Excel, PowerPoint, Access, Photo Editor, and Net Meeting), Microsoft FrontPage 98, Netscape Communicator, Internet Explorer, Simp Term, WS-FTP, and Novell GroupWise.

Area Software

Area Software is networked software for general campus use, but is purchased by one or more administrative or academic areas. The software will be installed by or with the cooperation of Information Services with updates funded by the sponsoring area(s) or users. Some type of joint agreement between the sponsoring area(s) and Information Services will usually fund the network storage space. Training and support will usually be the responsibility of the area(s) sponsoring the software. Examples of area software are: SPSS, Maple, Visual Basic, C++, and On-line Bible.

Restricted Software

Restricted Software is networked software with restricted use in one or more specific areas of campus. If the software has been approved by Information Services, they will provide up to four hours of initial Installation support with a charge assessed for additional installation time. It is the responsibility of the specific campus area to seek training and technical support for the product outside of the needs of the network. Any software being considered for purchase **must be approved**, before purchase, by Information Services for its compatibility with the NNU network. Examples of Restricted Software are Rasers Edge, Goldmine, and Scheduler Plus.

Local Software

Local Software is software located on a computer hard drive. This software is purchased, installed, updated, and maintained by individuals in the area using the software. Information Services is not responsible for this software. In the event that the hard drive of the local machine must be ghosted (all files deleted and campus software restored to it) then Information Services will not re-install the local software. Because the local machine is owned by NNU, a copy of the license of this software must be kept on file in the office of Information Services. Examples of Local Software: Norton Utilities, CUSeeMe, WordPerfect, etc.

Internet Use

Use of the Internet is a privilege. Individuals who use the University's computing resources are obligated to adhere to all University policies including, but not limited to those in this document.

Network Drive Access

Access to network drives is provided for several purposes:

- **Application Drives:** Some network drives contain files and resources that allow users to run software applications which are distributed across the network. Generally, users do not have the ability to write or copy files to these drives, only to read from them for the purpose of running the applications. Examples of application drives include the drives designated M: and Z:
- **Shared Drives:** Access is provided to a “shared” drive, generally designated with the drive letter “S:” Users can create folders on the S: drive which can be accessed by other users. Many campus departments place all their common files on the S: drive. There are separate S: drives for Faculty/Staff and for Students. Staff users can access the students’ S: drive (as S:\Students) but students cannot access the Staff S: drive. A folder named “Common” is provided on S: for both staff and students use. The Common folder is provided as a convenient place for temporary storage. It is NOT A SAFE place for long term storage, as anyone can open or delete files residing there.
- **Userdata Drive:** Access is also provided to each user’s personal space on the network, named “Userdata” accessed using the drive letter “N:” This is the recommended location to store all personal files which are needed on a regular basis.

NOTE: In NNU’s computing environment, it is **unsafe practice to store files of any importance on the local (C:) hard disk drive.** Information Services is charged with maintaining university-owned computers. This requires the freedom to re-image (or “ghost”) the local hard drives at any time, causing **all data on C: to be lost.**

Instead, **store important files on your N: drive**, which is backed-up to tape on a regular basis. It is wise to also make your own backup copy of important files on other reliable media, such as a USB Flash drive, a Zip disk, or a CD (requires a CD burner). Do **NOT** trust important data to a floppy disk. They are notoriously unreliable.

N: Drive Space Limitations

Each user is given some personal space on the network, named “userdata” (designated as drive N:). Student accounts are limited to 75 Megabytes on their N: drive. Staff accounts are allotted 250 Mb. This space is intended as a relatively safe place to store important files. The amount of space is adequate for most users’ file storage needs. It is the user’s responsibility to manage their personal space. That means doing periodic file cleanup. **Windows Explorer** is the recommended tool for this.

Purchasing Additional N: Drive Space

Additional personal network space can be purchased if needed. Students may have their space limits increased in 75 megabyte increments, at a cost of \$30 per 75 megabytes per academic year. To purchase additional drive space, go to Media Services.

At the beginning of each academic year (around the end of August), all student accounts are reset back to the current default space limitation (currently 75 Mb). If a student’s N: drive exceeds the limit, this will not prevent them from logging in. However, they will not be able to save anything until they delete some files or purchase another space increase for the year.

Student Labs and Classrooms

1. Students of Northwest Nazarene University will have access to many computer stations on campus, which the Office of Information Services will maintain. These will include, but not be limited to, computer labs, computer classrooms, and computers in the classrooms. The Director of Information Services will also make available ports for individual personal student use from the dorm rooms.
2. Students will have access during reasonable hours to computer labs within the learning centers, and also have access to the computer labs in each dorm during hours designated by the Residential Director (RD) or Student Development. Computer TAs will be assigned to the Wiley 115 computer center during reasonable hours, as available, for assistance with computer problems.

Non-Academic Use of Lab Computers

Use of the Public Computing Facilities is for purposes related to the University's mission of education, research, and public service. Students and faculty may use these computing resources for these purposes. Games and other personal enjoyments should be kept to a minimum. Computer users must cease any game playing or personal use when the computer labs become nearly full. If a person needing to work on the computers sees another person playing games, they may ask the game player to allow them to use the computer for work related to the University's mission. If the request to use the computer is refused, the person needing to work should ask a representative of Information Services to assist them. A person refusing to cease personal computing during these events will lose network privileges.

Printing

Students will be given a fixed allotment of laser-quality printing each term. A fee will be assessed for additional pages beyond the initial allotment. Students will be given credit for defective copies that are beyond their control if documented by a Wiley TA or a RD.

Dial-in Access and Use

Northwest Nazarene University will operate and maintain a dial-in server for the use of account holders from off-campus locations.

Eligibility

Any full-time faculty, emeritus faculty, administrative personnel, or staff member, or any full-time off-campus student of Northwest Nazarene University is eligible for a dial-in account.

Requirements for Access

Certain computer requirements must be met in order to use the dial-in server. These are posted on the website <http://www.nnu.edu/academics/dialin/dialup.htm>.

Cost of Access

There will be a monthly fee assessed to employees of the University for use of the dial-in server. Off-campus students pay their fee through the Student Technology Fee. This fee covers the first 20 hours of use each month, and a separate fee will be assessed for every hour of use over the 20 hours.

Limitations of Access

Access is limited to email and the Internet. Note: In the case of heavy demands on the computer network, or the Information Services Personnel, priority will be given to the on-campus computer network.

Limitations of Responsibility

Information Services will be responsible for the correct installation and operation of the dial-in software if the computer is brought to campus. This will be the extent of the responsibility of Information Services to personally owned computers.

Dormitory Access

In each dorm, access will be granted to students with their own computers who wish to have access to the Internet from their dorm rooms. They will also be able to access their student email account, similar to the manner outlined in the section titled "Dial-In Access." Information Services personnel will provide port activation and setup assistance through the school year. Help to students with computers that fall below the minimum computer standards will be extremely limited. Minimum standards for dorm computers as of Winter term 2000 is a Pentium 100 with 32 Megabytes of RAM and running Windows 95

Networked Computers

Desktop Computers and Peripheral Devices

1. All computer and printer purchases on campus must be approved by Information Services. Computers and Printers connected to the Network will only be approved from recommended vendors.
2. All computers and printers donated to campus must be approved by Information Services before they can be connected to the network. Only devices from recommended vendors will be approved.
3. A computer user must not attempt to modify or remove computer equipment, software or peripherals that are owned by Northwest Nazarene University without proper authorization. If a modification creates a problem on that computer or the network Information Services has the right to charge the user or department for the cost and time to fix the problem. An example of this would be connecting a video device to a campus computer that has not been approved.

Servers

Servers connected to the NNU network must be under the supervision of Information Services. No school, department or organization on campus may install and operate a server, either autonomous or connected to the NNU network, without the authorization of the Director of Information Services. Presently, three areas have been authorized to install servers. These are: Computer Science (for the purpose of teaching the skills of networking), Riley Library, and the Wesley Center. These may continue to run their servers so long as the department / organization involved:

1. Files an updated Administrative / Root Access Password and contact information of the server administrator with the Director of Information Services.
2. Authorizes Information Services personnel to access the server, if needed, to solve a network problem that is believed to be caused by that server. This would only be done after an attempt has been made to reach the person listed as the contact person.
3. Agrees to maintain the server on their own.
4. Does not use the server to provide services already provided by Information Services. Examples include DNS, DHCP and Mail services.
5. Does not, under any circumstance, install a Novell server.

Note: Students installing personal computers as servers in their dorm rooms may do so without prior authorization from Information Services as long as they agree to 2 and 4 above and as long as the activity on the server meets the requirements of all other items in this policy document. This allows students to learn and practice networking technology. If those machines are used in a way that impacts Network access for the campus, or for commercial purposes, their access will be blocked at their port switch. Examples of unacceptable uses would be: Video Streaming, Multiple 56 K streams to the Internet or setting up FTP servers to which Internet users may connect.

Personally owned computers

Personally owned computers may not be connected to the NNU network. The exception to this policy will be made in the dormitory living areas. An owner of a private computer who holds a valid user account and who is granted access to the NNU network assumes the privileges and responsibilities specified in this Policy document.

Assignment of IP Addresses

Information Services will have sole responsibility for assigning a single IP address to each on-campus student-owned computer, as well as to each piece of computer equipment owned by NNU and connected to the NNU network. Violation of this policy may result in loss of network privilege.

Privacy Issues

A user must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users. Users who are authorized to access private information are required to preserve the confidentiality of such information in conformance to the Family Educational Rights and Privacy Act of 1974 as Amended in 1995(FERPA).

FERPA establishes that:

- the development of guidelines and policies for restricting access so as to ensure proper use of educational record data are institutional responsibilities, and
- Northwest Nazarene University should establish procedures for initially instructing and periodically reminding school officials (i.e., individuals defined by Northwest Nazarene University as having a legitimate educational interest) of confidentiality requirements prior to granting a school official access to the student information system

Intellectual Property

A user must attribute and honor the intellectual property rights of others. This includes information gathered from the World Wide Web.

Termination of Accounts

Accounts will be terminated under the following conditions:

1. Discontinuing students or graduating students. Accounts of students who have not returned by the last day of registration may be terminated.
2. Employee Resignation. The account may be terminated after 30 days, if faculty or staff has resigned their position (in good standing) within the University. It is the responsibility of the immediate supervisor to instruct the employee to dispose of account contents appropriately. Note: Emeritus professors will receive account privileges indefinitely.
3. Terminated Employees. Accounts of terminated employees may be disabled and/or terminated upon completion of the final day of employment by NNU. It is the responsibility of the immediate supervisor to instruct the employee to dispose of account contents appropriately.
4. Computer Abuse. If it is determined that an individual's abuse of the computer network warrants termination, the account may be disabled immediately.

(Extensions of faculty, staff, or student account privileges will be granted for up to a period of six months, for individuals with demonstrated administrative or academic needs. Requests for extension must be submitted to the Director of Information Services and must be accompanied by a letter from a sponsor (department chair, supervisor, faculty advisor, etc.)

Personal Use

Incidental Use

While the NNU network is not intended for activities unrelated to appropriate NNU functions, incidental personal use is allowed. Any personal use must not interfere with the use of others engaged in the completion of NNU functions.

Commercial Use

NNU computer and network resources should not be used for commercial purposes except in a purely incidental manner. Employees of the University may seek this permission from the Office of the Dean of Academic Affairs. Students may seek this permission from the Office of Student Development. Users shall not use NNU facilities, supplies, materials, equipment or services for commercial use without first obtaining approval of the appropriate dean or director and arranging for the payment of total cost for such use.

Sanctions

Penalties for violation of this policy range from the loss of computer resource privileges to dismissal from the University, prosecution, and/or civil action. Each case will be determined separately on its merits.

1. If the offender is an employee of the University, the computer resource may be disabled and the immediate supervisor shall recommend to the Dean of their respective School and the Vice President for Academic Affairs the appropriate sanction in accordance with due process and the right to appeal.
2. If the offender is a student, the computer resource may be disabled and all pertinent information will be turned over to the Dean of Student Life and Development who will exercise the student judicial process.

Student Computer Support

Goals

The goals of the student computer support provided by NNU Information Services are twofold:

1. Help ensure that the computing experience of all NNU students is as positive and helpful to their education goals as possible.
2. Assist students in preparing for the use of technology in their future careers after leaving NNU. This implies that we assist in educating them in basic computer “survival skills.” It is our hope that when leaving the campus all our students are computer-savvy enough to be successful in our high-tech world.

Support Resources

Computer support for students is provided through several avenues:

- The **Student Computer Support Specialist (SCS)** is a full-time Administrative Personnel position. This person is the primary technical support liason for students.
- The SCS is responsible to establish and maintain the **Student HelpDesk**. Accessible via email, phone or walk-in visits, the Student HelpDesk is staffed 40 hours per week, during the normal work hours.
- **Computer Teaching Assistants (TAs)** are trained in NNU network and computing support. Computer TAs report to the SCS and are available to help students in the Wiley 115 Main Computer lab Monday through Saturday from 7:30 AM until 11:00 PM and Sunday evening form 8 PM until 11:00 PM. Other Computer TA duties include:
 - Maintain and clean the ten other computer labs campus-wide.
 - Maintain and clean about 30 Teaching Station computers located throughout the campus.
 - Specialist TAs assist the SCS in providing basic tech support for computers belonging to students.
- The **Computing Resources web pages**, located on the NNU Intranet (http://intranet.nnu.edu/computing_resources.htm) provide on-line technical

information, downloadable resources and support request forms. The SCS is responsible for maintaining the student support sections of these web pages.

- **Self-Help Guides** are technical “how-to” documents which are kept up-to-date and available for free in the Wiley 115 Computer Lab.

NNU-Owned Computers

All NNU-owned lab computers are fully supported and maintained by Information Services Department personnel. The SCS is primarily responsible for the condition of general use labs across the campus.

NNU-Standard Laptops (LAWN program)

Laptops purchased through NNU as part of the Local Area Wireless Network (LAWN) program will be fully supported by NNU Information Services Staff for two years following their purchase. Currently NNU-Standard Laptops (the Micron Transport XT) are warranted by the manufacturer for defective parts exchange for three years under Micron’s “Advanced portable exchange” program. Micron laptops are also covered under Micron’s 5/1 limited warranty. Thus, after the initial two year period, students can deal directly with the manufacturer for any warranty repairs or service.

This support includes dealing with the manufacturer for defective parts replacement for the two year period. Software support is provided contingent on the student not deleting or substantially modifying the NNU-standard “image” as supplied by NNU. In other words, NNU can provide full technical support only for the configuration we have tested to assure full compatibility on that laptop with our network. Modifications which would nullify this include changing the disk partitions as supplied, changing the Operating System, etc.

Student Owned Computers

This category includes any personal computer owned by a student which is not the NNU-Standard laptop. These include laptop and desktop “IBM-PC compatible” computers.

Network Connectivity

Installation, configuration and troubleshooting of hardware and software required or related to connectivity to the NNU network is provided as-needed and free-of-charge by the SCS and TA staff. This includes Ethernet connectivity in dorm rooms and dial-up connectivity for use from off-campus locations.

Virus Prevention

Installation and assistance in configuring anti-virus software which the student purchases at their own expense.

Virus Damage Control

The SCS will provide assistance in recovery of data and disinfecting of virus –infected student computers. It is the student’s responsibility to keep up-to-date anti-virus protection on their personal computers. If a student’s computer becomes reinfected due to the student’s negligence in providing adequate protection, NNU will not provide repeat maintenance on that computer. In addition, if a student, through such negligence, poses a virus infection threat to others on the campus, their connection privileges to the NNU network may be terminated.

Limited Data Backup and Recovery

If the student’s computer has been damaged or shows signs of imminent hard drive failure, NNU will provide assistance in data recovery and or backup of academic materials only.

NNU will not backup or recover non-academic or pirated materials or software, specifically including music files, media files, pornographic or illicit materials, etc.

Assistance with Software Provided by NNU

NNU currently provides for campus-wide software licensing of the full Microsoft Office suite of applications, the GroupWise email client, and a few other selected applications. The SCS and TAs will assist students in installation, configuration and troubleshooting of such software.

Service Locations

NNU's network is configured for "dynamic IP addressing" of student workstations on the network. This allows us to perform nearly all personal computer maintenance tasks at a central location, rather than necessitating visits to dorm rooms across campus. This approach is much more efficient for the support personnel. The troubleshooting and support approach is as follows:

If the problem seems to lend itself, the SCS or Computer TA will attempt to "walk through" initial troubleshooting and problem resolution via telephone.

If the student is "over their head" or the problem seems too complex for phone support, the student can bring their computer to the Wiley 115 Computer lab where they can check it in for support.

In the rare event that the nature of the problem necessitates on-site troubleshooting, the SCS or TA will make an appointment to visit the Student's dorm room. No male TAs will be sent to female dorms or female TAs to male dorms. A male SCS may visit female dorms, but only in the late morning or afternoon hours. When entering dorm halls, a male SCS must call out "man in the hall" and the door to the dorm room must remain propped open at all times.

Support Specifically Not Provided

The following are examples of the kinds of support NNU cannot provide for personally-owned student computers:

- No "house calls" are made to off-campus locations, and only rarely to dorm rooms (see "Service Locations" above).
- Major hardware upgrades or extensive repairs are not provided, with the exception of NNU-Standard Laptops. Major upgrades and extensive repairs include: Operating System upgrades, CPU replacements, extensive diagnostics on motherboards or RAM components, etc.
- Monitors: We cannot open a monitor to diagnose a problem. High voltages are present inside monitors which present safety hazards.
- Research and purchasing of upgrade components is not provided. Limited recommendations of what and where to purchase computer components and upgrades may be provided on a personal basis, but such advice does not constitute NNU-endorsement of any business or product.
- Exceptions: On rare occasions, it may make sense to provide one of the services listed above. If in the judgment of the computer TA the service will not take more than one or two hours at maximum, and will effect a major improvement in operation of the computer, then the TA must discuss the situation with the SCS and receive approval before proceeding.