MOUNT VERNON
NAZARENE UNIVERSITY
Life Changing

Computer Use Protocol

Purpose

Computer facilities and equipment at Mount Vernon Nazarene University are provided for instructional and administrative use to enable the University to more effectively fulfill its mission to provide a Christian liberal arts education. The following protocols are provided to assure that the University's significant investment in computing technology is used in accordance with this purpose. These protocols augment the University's *Staff Handbook* and *Faculty Handbook*.

Commitment to Integrity

Mount Vernon Nazarene University requires its employees and students to observe a high standard of personal, business, and academic ethics. In observing those high ethical standards, all employees and students must act with honesty and integrity in carrying out duties and responsibilities to ensure compliance with all applicable federal, state and local laws and regulations.

The computer use protocol operates under the University's broad technology infrastructure policy (http://mvnu.edu/policies/Technology%20Infrastructure%20Policy.pdf).

Ownership

Computer resources, as defined below, that were purchased by the University are the exclusive property of the University and not the user's private property.

Definitions

Computer Resources. These resources include, but are not limited to, Information Technology Services (ITS) equipment, web servers, e-mail servers, file/print servers, networks, network connections, wireless connections and devices, telephones and telecommunications systems, printers, scanners, computers and multi-user systems, whether they are located in offices, public areas, classrooms, or laboratories, etc.

User. The person using the computer resources as defined above.

Owner. The person or entity that has provided the funds to purchase the computer resources. For the sake of these protocols as they relate to Graduate and Professional Studies (GPS) laptops, GPS students are considered owners.

Authorized Users

Computer resources are provided for the use of the University's undergraduate students, graduate students, faculty, staff, and administrators. Limited access may be granted to other users on a limited time basis, based on established University procedures.

Computer Accounts

Accounts are assigned for University-related work. If there is reasonable suspicion of illegal or unethical activities, the University reserves the right to inspect its property. It is important to remember that the computer is not a secure environment for private material. The Information Technology Services (ITS) Department assigns accounts and activates them for authorized users.

Users should change passwords frequently and should avoid using their own names, that of a spouse or friend, or a password that could easily be guessed. Passwords must be kept private to the user. For increased password security, passwords should be created with a minimum length of seven alphanumeric characters using a combination of numbers, letters, and special characters.

The use of a computer account by unauthorized persons is prohibited. If an authorized user's association with the University ends, all computer accounts assigned to that person are no longer valid and will be deleted. Accounts inactive for more than a calendar year may be deleted by ITS personnel.

The use of a University computer account or login by anyone (including, but not limited to roommates, friends, relatives, or co-workers) other than the user to whom the account has been assigned is prohibited. Exceptions may be made in offices according to established office procedures created in that area.

Authorized and Unauthorized Uses

General Provisions. The following broad protocols are in effect for computer use.

- The use of University computing resources is to be in harmony with Mount Vernon Nazarene University's educational mission, ethical standards, policies, and protocols.
- The use of University-owned computer resources, as defined above, shall only be for University purposes, and not for operating a for-profit or non-profit business or ministry.
- Information posted to public web-based forums must be consistent with University ethical standards, mission, privacy/confidentiality laws, campus regulations, and guidelines. Public forums include, but are not limited to, blogs (e.g. Facebook, Xanga), wikis, and personal/corporate web pages. The University advises its constituents to limit specific personal information posted to these open forums for security and safety reasons.
- No person shall knowingly gain access to, or attempt to gain access, any computer resources without the consent of the owner of these resources, or other person authorized by the owner.
- No person shall knowingly access, alter, delete, or destroy data, information, or programmatic instructions on computer resources without consent of the owner.
- No person shall knowingly create or add a set of instructions, programmatic code, or data into a computer resource that will cause that resource to do anything unwanted by the owner. This includes, but is not limited to, computer "viruses," operating system or software upgrades.
- Attempting to circumvent University computer security, filtering, or printer accounting systems, or using University computer systems or computer networks in attempting to circumvent these types of systems elsewhere is prohibited.
- No person shall use a computer resource to eavesdrop on another user or to collect passwords or other authentication information.
- No persons shall use a computer resource anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise to escape responsibility for their actions.

Copyright and Legal Concerns. The following protocols are in effect as they apply to copyright and related legal issues.

- For copyright purposes, there are three general classifications of software, each with different rules that govern one's ability to copy or use it legally.
    - Fully copyright protected software includes all commercially sold programs and any other programs that contain a copyright notice. It also generally includes any software that contains no notice of any kind. Software that falls into either of the other two categories below will carry notices to that effect. Copyrighted software may not be copied, except for one backup copy to be made and maintained by the original owner. In addition, it may be used only by the person to whom it is licensed and may not be shared by several people. It is illegal to sell, give away, or use copies of copyrighted software that the user did not buy from the author or the publisher.
    - Shareware is software that has a copyright, but that the author has agreed may be freely distributed. It is legal to copy and give away this software, but if the user chooses to utilize it, he/she must send a license fee to the author, whose name appears with the copyright notice. The user must abide by the terms of the shareware agreement. For example, some shareware programs allow free use only for a specified period of time. When the free use time expires, the user must either purchase the software or uninstall it.
    - Public domain software (freeware) is that which has been released by its author for public ownership. This software may be freely copied, used, shared, or given away. It may not be sold for profit.
- University computer users must comply with University copyright regulations. The University's copyright regulations can be found at http://mvnu.edu/policies/copyright.pdf.
    - Computer software or data, including but not limited to, text, video, audio/music, or picture files, may not be copied, or used in violation of the license agreement or copyright provisions.
    - Unless specifically allowed by its owner and copyright, proprietary software must not be placed into public locations. Such locations include, but are not limited to, file servers, shared computer files or folders, and web servers.
- Users must comply with all state, federal, and international laws. These laws include, but are not limited to, laws of copyright, trademark (including items relating to Mount Vernon Nazarene University), libel, privacy, obscenity, and pornography.

Software. These software use protocols are in effect for University computing systems users.

- No unauthorized person shall provide to anyone data containing passwords or computer software to produce that data.
- The use of personally licensed software on University-owned office and laboratory systems is discouraged. Any personally licensed software tht is installed must be officially registered with and sent to the office of the Director of Information Technology Services.

Physical Property. Compliance with the following protocols is expected of University computer users.

- University computer resources may not be moved by an unauthorized person to another office, laboratory, dormitory, or elsewhere on or off campus. Mobile technologies (e.g. notebooks, tablet PCs, PDAs, cell phones, etc.) are the responsibility of the assigned user.
- No unauthorized person shall knowingly connect, disconnect, tamper with, or make changes to any computer resource unless appropriate permission is granted by the owner.

Limitations. The University reserves the right to regulate the use of computer resources, including but not limited to, connection times, connection speeds, and filtering of content. Wise counsel includes:

- Wasteful or extravagant use of University computer resources is prohibited. Extravagant use includes, but is not limited to, peer-to-peer networking applications (e.g., KaZaA, Gnutella, Scour, BitTorrent, eDonkey, Ares), network games (e.g., Half-Life, Doom, Battle.net), and applications capable of downloading large files (e.g., QuickTime, Real, WinMedia). The applications themselves are not prohibited or extravagant per se, but can be used in inappropriate and excessive ways inconsistent with the University's educational purposes.
- The use of computer resources and facilities is limited to bona fide University administrative, research, instructional, or limited personal purposes. Personal use or non-academic interests such as browsing recreational web sites, playing games, chat facilities, or sending personal e-mail is a lower priority, and is allowed so long as it does not displace or disrupt instructional, research, or administrative purposes. The utilization of office computer resources for personal purposes during work hours should be kept to a minimum and is subject to the supervisor's discretion.

Network Security. To protect persons and property, the following protocols are normative expectations.

- Anyone attaching a computer system to the University network must exercise due diligence in keeping computers spyware/mal-ware, worm, and virus free. This includes, but is not limited to, computers owned by students in the residence halls, and private systems owned by faculty and staff. Examples of measures for keeping a system spyware/mal-ware, worm, and virus free include, but are not limited to, keeping security patches from the appropriate operating system vendor up-to-date, installing virus protection and keeping its definitions updated, and utilizing safe practices in opening attachments in e-mail.
- The University reserves the right to deny network access to any computer that is infected with a worm, virus, or any other software that negatively impacts the University network. In matters of priority, wholesale access to network resources may be denied in preference to mission critical applications.
- Users that persistently spread worms or viruses and do not exercise due diligence in protecting against them may be subject to denial of access or monetary charges.

E-Mail and Telephone Use

University employees and students are expected to use computer resources and the telecommunication system consonant with the University's education mission, ethical standards, policies, and protocols.

General Provisions. The following broad protocols are in effect for e-mail and telephone use.

- The e-mail system is the property of Mount Vernon Nazarene University and is provided for the purpose of carrying out the mission of the University. Assignment of an account and the selection of a private password does not entitle the user to privacy of e-mail messages. If there is reasonable suspicion of illegal or unethical activities, the University reserves the right to enter the e-mail system and review, copy, or delete any messages, and disclose such messages to the appropriate authorities.
- For positive identification purposes, the name portion of voice mail greetings must be the name of the user the voice mail box has been assigned. The longer greeting portion of the voice mail greeting must be consistent with University protocols.
- Employees are to use the official e-mail disclaimer for any messages that contain confidential material. The text of the disclaimer is "This message, including its attachments, is intended only for the named recipient(s) and may contain confidential material, the confidentiality of which must be maintained by the recipient(s) by not forwarding or disseminating without the permission of the sender. If you are not the intended recipient(s), you are notified that the disclosure, copying, or distribution of this message is strictly prohibited. If you have received

this message in error, or are not the named recipient(s), please notify the sender at either the e-mail address or telephone number above and delete this e-mail from your computer immediately. Thank you."

- For reasons of security, privacy, and reliability of delivery, students and employees are prohibited from auto-forwarding the University e-mail to an off-campus provider.
- University e-mail accounts must be the sole authoritative source for University business e-mail and exchange of University data.

Limitations. The University reserves the right to manage e-mail storage. This includes, but is not limited to, e-mail expiration/expunging based on the age or size of messages, regulating account size by means of quotas, and regulating mass e-mail distributions.

- The Information Technology Services Department reserves the right to manage voice mail storage. As such, any greetings or messages left on voice mail can be saved, deleted, moved, etc. at the discretion of and by University authorized personnel.
- Campus-wide distribution of e-mail is subject to the "E-mail and Voice Mail Distribution Guidelines", which defines acceptable distribution of messages to the campus community. Suspected violations of these distribution guidelines should be reported to the office of the alleged violator's senior administrator.

Prohibited Activities. Honesty, integrity, and transparency dictate that certain activities be avoided.

- No person shall send a message in such a way that it appears to be sent by another person.
- No person shall provide a list of post office addresses, e-mail addresses, or phone numbers of campus students or employees to an outside agency without authorization by the University's Business Affairs Office.
- The use of University computer or telephone systems to harass or slander others is prohibited.
- Posting of information to electronic forums beyond their appropriate purpose scope is prohibited. These forums include, but are not limited to, newsgroups, listservs, or electronic bulletin boards.
- Originating or propagating correspondence that is unrelated to the University's institutional purpose and requesting that the message be forwarded to multiple unspecified users is prohibited. Examples of these messages include, but are not limited to, chain letters, e-mail hoaxes, and solicitation for pyramid schemes.

Computer Laboratory Use

All computer use protocols described previously extend to University computer laboratories. Specific laboratory protocols include the following:

- The computer laboratory environment is similar to that of a library – quiet work and subdued conversation.
- Due to the focus on student learning, children and pets are not permitted in computer laboratories.
- Data or programs that are left on computer laboratory systems will be automatically deleted on restart. Any data that is to be saved must be stored on removable media or network drives.
- All computer sessions must be terminated before leaving the laboratory. The University reserves the right to terminate unattended sessions.
- Drinking and eating in computer laboratories should be avoided to prevent potential hardware damage.

- Any laboratory or printing activity must be finished before laboratory closing time or the beginning of a scheduled class session in that laboratory. Computer laboratories will close at their designated times.
- All persons must comply with the instructions given by the employee on duty in the computer laboratory.

Security and Privacy

The University is committed to abiding by local, state, and federal legislation regarding confidentiality and privacy (e.g., Gramm-Leach-Blily Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act, etc.). Users of University resources share in that commitment as defined in general University policies (http://www.mvnu.edu/policies). To that end, users are expected to demonstrate the following best practices to preserve security and privacy.

- The user will archive and delete any personal data or programs from University owned machines when the user's official relationship with the University is finished.
- Users should exercise diligence in securing their own data and/or the data they have access to via their job responsibilities. Examples of this include, but are not limited to, logging out of computers when finished especially in public areas, "locking" their sessions when stepping away from the system for an extended period of time, not placing confidential information in non-restricted network areas, closing out all browsers when finished with authenticated web sessions such as using the administrative system, etc.
- Individuals must secure ITS approval prior to using any non-university software or cloud-based services (e.g., Google docs, Dropbox, etc.) that utilize the University network infrastructure.

Enforcement

Suspected violations should be reported to the following: Graduate and Professional Studies student violations to the Associate Vice President for Graduate and Professional Programs, all other student violations to the Vice President for Student Life, staff violations to the Director of Human Resources, faculty violations to the Provost. All suspected violations must also be reported to the Director of Information Technology Services, since immediate action, temporary or otherwise, may warrant initiation by ITS personnel based upon the circumstances. These individuals, with appropriate consultation, will determine if an investigation is warranted and initiate that investigation.

In addition to other sanctions, access to some or all computer resources may be revoked for a violation of the above regulations and policies, or any unlawful activity. The University will aid law enforcement in the investigation and prosecution of any suspected illegal activity.

Exceptions

Exceptions to these protocols must be approved by the Provost and Chief Academic Officer, or Vice President for Finance and Chief Financial Officer.

Questions

The following individuals can be contacted for questions on the computer use protocol as outlined here.

For	Contact
Any question	Unit supervisor
Reporting misuse of University information technology infrastructure	Unit supervisor, Provost and Chief Academic Officer, or Director of Human Resources, Director of Information Technology Services

The following outlines the approval, review, and revision history of the computer use protocol.

Version	Approval Date of Version	Version Type
1.0	Technology Advisory Council, March 26, 2007	Initial release; portions of the document are used with permission from Bowling Green State University, The Ohio State University, and The University of Iowa.
1.1	March 26, 2008	Minor update and planned review
1.2	Institutional Effectiveness Office, July 27, 2012	Update related to re-organization of University policies, re-formatted for consistency across protocol documents, and changes in position titles within the University