

MOUNT VERNON NAZARENE UNIVERSITY

COMPUTER REGULATIONS AND POLICIES

I. PURPOSES

Computer facilities/equipment at MVNU are provided for instructional and administrative use to help the University more effectively fulfill its mission to provide a Christian liberal arts education. The following policies are provided in order to assure that the University's significant investment in computing is used in accordance with this purpose.

II. OWNERSHIP

Computer resources (as defined below in "III. Definitions") which were purchased by the University, are the exclusive property of the University and not the user's private property.

III. DEFINITIONS

Computer Resources: These resources include, but are not limited to, the administrative computer, instructional technology equipment, web servers, mail servers, file/print servers, networks, network connections, wireless connections and devices, telephones and telecommunications systems, printers, scanners, computers and multi-user systems.

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

Owner: The person or entity that has provided the funds to purchase the computer resource. For the sake of these policies as they relate to Adult and Graduate Studies (AGS) laptops, AGS students are considered owners, though they do not officially own the systems until they graduate.

IV. AUTHORIZED USERS

Computer resources are provided for the use of MVNU 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.

V. COMPUTER ACCOUNTS

- A. 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.
- B. MVNU computing departments will assign accounts and activate them for authorized users.
- C. Users should change their passwords frequently and should avoid using their names, their spouse's or friends' names, or a password which 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.
- D. Use of a computer account by unauthorized persons is prohibited. If an authorized user's association with MVNU (as stated in IV) 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 authorized MVNU computing personnel.

- E. Use of an MVNU 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 faculty/staff offices according to individually established office procedures created in that area.

VI. UNAUTHORIZED USES

A. General Policies

1. Use of a computer resource in violation of Mount Vernon Nazarene University regulations and policies, ethical standards, or mission is prohibited (Note also item X).
2. No person shall knowingly gain access to, or attempt to gain access to any computer resources without the consent of the owner of these resources, or other person authorized by the owner.
3. No person shall knowingly access, alter, delete, or destroy data, information, or programmatic instructions on computer resources without consent of the owner.
4. No person shall knowingly create or add a set of instructions, programmatic or otherwise into a computer resource that will cause that resource to do anything unwanted by the owner.

(Examples of 3 and 4 include, but are not limited to, computer "viruses", operating system or software upgrades)
5. Attempting to circumvent MVNU computer security, filtering, or printer accounting systems, or using MVNU computer systems or computer networks in attempting to circumvent these types of systems elsewhere is prohibited. (Note item X)
6. No person shall use a computer resource to eavesdrop on another user or to collect passwords or other authentication information.
7. All modem and wireless access point connections must be approved by the Director of Network Computing. The unauthorized use of modems and wireless access points on campus is prohibited (for example to access an external Internet service provider from the residence halls).
8. 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.
9. Use of MVNU computer resources, as defined in section III, for operating a for-profit or non-profit business or ministry entity is prohibited unless approved by the Computer Policy Council (see section XI).
10. 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. MVNU advises its constituents to limit specific personal information posted to these open forums for security and safety reasons.

B. Copyright and Legal Issues

1. 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.
 - a. 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 to use copies of copyrighted software which you did not buy from the author or the publisher.

- b. Shareware is software that has a copyright, but which the author has agreed may be freely distributed. It is legal to copy and give away this software, but if you choose to use it yourself, you must send a license fee to the author, whose name appears with the copyright notice. You 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, you must either purchase the software or uninstall it.
 - c. 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.
2. Copyright laws must be respected at MVNU. NOTE: The full copyright policy of MVNU can be found at <http://www.mvnu.edu/policies>
 - a. 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.
 - b. 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.
 3. 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 MVNU), libel, privacy, obscenity and pornography.

C. Software Issues

1. No unauthorized person shall provide to anyone data containing passwords or computer software to produce that data.
2. The use of personally licensed software on university owned office and lab systems is discouraged. Any personally licensed software which is installed must be officially registered with Network Computing and a copy of its license sent to the Director of Network Computing.

D. Physical Property Issues

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

E. Limitations

1. 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.
2. Wasteful or extravagant use of MVNU 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. (Note also item VI.E.3)

3. Use of computer resources and facilities is limited to bona fide MVNU 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 use for instructional, research, or administrative purposes. Use of office computer resources for personal purposes during work hours should be kept to a minimum and is subject to the supervisor's discretion.

F. Network Security Issues

1. It is required that anyone attaching a computer system to the University network exercise due diligence in keeping their computers spyware/mal-ware, worm and virus free. This includes, but is not limited to, computers owned by students in the residence halls, AGS students with university supplied laptops, 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.
2. 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.
3. 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.

VII. E-MAIL and TELEPHONE USES

- A. Use of a computer resource or telephone in violation of Mount Vernon Nazarene University regulations and policies, ethical standards, or mission is prohibited. (Note also item X)
- B. General Policies
 1. 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.
 2. The name portion of voice mail greetings must be the name of the user the voice mail box has been assigned to. The longer greeting portion of the voice mail greeting must be consistent with university ethical standards, regulations and guidelines.
 3. Both students and employees should use their personal (non-departmental) calling cards when making personal long distance calls on university-owned telephones.

4. Employees are to use the official e-mail disclaimer for any messages that contain confidential material. The text of the disclaimer is "This message 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 dissemination, distribution or copying of this message is strictly prohibited. If you receive 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."
5. For reasons of security, privacy and reliability of delivery, students and employees are prohibited from auto-forwarding their MVNU e-mail to an off-campus provider.

C. Limitations

1. MVNU computing departments reserve 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. Please refer to the document "E-mail Storage Management" for further details on quotas and expirations.
2. The Department of Network Computing 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 MVNU authorized personnel.
3. 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 responsible senior administrator.

D. Prohibited Activities

1. No person may send a message in such a way that it appears to be sent by another person.
2. 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.
3. The use of MVNU computer resources or telephones to harass or slander is prohibited.
4. Posting of information to electronic forums beyond their scope is prohibited. These forums include, but are not limited to, newsgroups, listservs, or electronic bulletin boards.
5. Originating or propagating correspondence that is unrelated to MVNU'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, traditional chain letters, e-mail hoaxes, and solicitation for a pyramid plan.

VIII. MOUNT VERNON CAMPUS COMPUTER LAB USE

- A. Use of a computer resource in violation of Mount Vernon Nazarene University regulations and policies, ethical standards, or mission is prohibited. (Note also item X)
- B. The computer lab environment is similar to that of a library--quiet work and subdued conversation.
- C. Children and pets are not permitted in the computer labs.

- D. Data or programs that are left on computer lab system hard drives will be automatically deleted on restart. Any data that is to be saved must be stored on removable media or network drives.
- E. All computer sessions must be terminated before leaving the lab. The University reserves the right to terminate unattended sessions.
- F. Drinking, eating, or loitering in the computer lab is prohibited.
- G. Any lab or printing activity must be finished before lab closing time or the beginning of a scheduled class session in that lab. Computer labs will close at their scheduled time.
- H. All persons must comply with the instructions given by the employee on duty in the computer lab.

IX. SECURITY AND PRIVACY

- A. All users of MVNU's computer resources are required to abide by local, state and federal privacy legislation including, but not limited to, GLB, FERPA, HIPAA, etc. NOTE: additional policies relating to security and privacy can be found at <http://www.mvnu.edu/policies>.
- B. It is the responsibility of the user to archive and delete any personal data or programs from university owned machines when the user's official relationship with the university is finished.
- C. 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.

X. ENFORCEMENT

- A. Suspected violations should be reported to the following: Adult and Graduate Studies student violations to the Director of Academic Services for AGS, all other student violations to the Associate Dean of Student Development, staff violations to the Director of Human Resources, faculty violations to the Vice President for Academic Affairs. These individuals, with appropriate consultation, will determine if an investigation is warranted and initiate that investigation.
- B. 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.
- C. MVNU will aid law enforcement in the investigation and prosecution of any suspected illegal activity.

XI. EXCEPTIONS

Exceptions to these regulations and policies must be approved by the Computer Policy Council consisting of the Vice President for Academic Affairs, the Vice President for Finance and Management and the Vice President for University Relations.

Some of the policies in this manual have been used fully or in part, with permission from the policy documents of the following Universities: Bowling Green State University, The University of Iowa, The Ohio State University

The Technology Advisory Council approved these policies on March 26, 2007. Revision: file: compregfinal07-1.