OLIVET NAZARENE UNIVERSITY

INFORMATION TECHNOLOGY

Acceptable Use Policy

Department of Information Technology
Olivet Nazarene University

(815) 939-5302

Published August 2013 Ver. 4.0

Policy Overview

1. Executive Summary

This summary is intended to present a brief overview of the policies set forth by the Department of Information Technology at Olivet Nazarene University. It is by no means exhaustive or detailed. A detailed document of the policies, procedures, and guidelines can be found at http://it.olivet.edu. By agreeing to the policies set forth by the University in the Student Life Handbook, the user also agrees to follow and adhere to the policies set forth by the Department of Information Technology found on the department website. These topics include:

- Policy Changes
- Privacy & System Monitoring
- Lab Computers
- Personal Computers and Devices
  - Data Archiving
  - Mandatory Copyright License for All Software
  - Repair Selection Criteria
- Wireless Access
- Internet Content Filtering
- Copyright Infringement: Digital Millennium Copyright Act ("DCMA")
- Accounts & Access
- Passwords
- Network Storage
- Prohibited Activities
  - Violations
- Discovery of Pornographic Materials
- Disciplinary Actions
- Disclaimer of Liability

Introduction

The Olivet Nazarene University campus computing network and telecommunications network (ONUnet) exists to further the University's teaching, scholarly research, and spiritual goals. The same ethical and community expectations outlined in the University Life Handbook apply to the use of ONUnet. All equipment is subject to the rules and conditions outlined in this Policy, the Intellectual Property Policy which references and incorporates this Policy, and the University Life Handbook. Persons accessing any of the network resources are expected to practice common sense, decency, and courtesy to other users and third party stakeholders. Individuals are responsible for the proper use of the account, including proper password protection. Any action that occurs on an individual's account or workstation is the responsibility of that individual. All students, faculty, and staff are responsible for seeing that these information systems are used in an effective, efficient, ethical, and lawful manner and for the safeguarding and protection of their user names and passwords.

Access to ONUnet is a privilege and may be revoked at anytime. It is provided as a resource to the Olivet community. Access to ONUnet is restricted to authorized users, which is defined as an individual who has been assigned an ID and password by Information Technology staff, or by any agent authorized by the Administrative Team. The use of ONUnet may be revoked at anytime, with or without notice, for any violation of the Policy,

including but not limited to misuse, abuse, infringement of third party intellectual property rights, exceeding authorized access, or vandalism to any system.

This policy applies to networks and resources outside the University that access ONUnet via the Internet. Network or resource providers outside the University may, in turn, impose additional conditions of appropriate use which the user should observe when using those resources.

Disciplinary Actions

Violation of this Policy may be considered a violation of the Computer Fraud and Abuse Act (for exceeding authorized access) and may result in suspension or termination of the user's network access, network account, or e-mail account. Suspending network access for the violator may also result in the suspension of access for the entire room or apartment in which that violator resides (for students). Upon suspending the user's access, the Information Technology Department will notify both the user and the Office of Student Development (for student violations) or the Human Resources Department (for faculty or staff violations). Suggested disciplinary actions for students include one or more of the following:

- Community service
- Fines or restitution equal to technician's time
- Criminal or civil prosecution
- Notification to parents, authorities, or head of academic department
- Dismissal from the University
- Counseling

Disclaimer of Liability

Neither the University nor any of its agents will be liable for any losses, including lost revenues, or for any claims or demands against the users of ONUnet by any other party. In no event will the University be liable for consequential damages, even if the University has been advised of the possibility of such damages. The University will not be responsible for any damages due to the loss of output, loss of data, time delay, network system's performance, software performance, hardware damage, incorrect advice from a consultant, or any other damages arising from the use of the University's network systems, information systems, or technicians.

Expanded Policy Information

1. Introduction

The Olivet Nazarene University campus computing network and telecommunications network (ONUnet) exists to further the University's teaching, scholarly research, and spiritual goals. The same ethical and community expectations outlined in the University Life Handbook apply to the use of ONUnet. All equipment is subject to the rules and conditions outlined in this Policy, the Intellectual Property Policy which references and incorporates this Policy, and the University Life Handbook. Persons accessing any of the network resources are expected to practice common sense, decency, and courtesy to other users and third party stakeholders. Individuals are responsible for the proper use of the account, including proper password protection. Any action that occurs on an individual's account or workstation is the responsibility of that individual. All students, faculty, and staff are responsible for seeing that these information systems are used in an effective, efficient, ethical, and lawful manner and for the safeguarding and protection of their user names and passwords.

Access to ONUnet is a privilege and may be revoked at anytime. It is provided as a resource to the Olivet community. Access to ONUnet is restricted to authorized users, which is defined as an individual who has been assigned an ID and password by Information Technology staff, or by any agent authorized by the Administrative Team. The use of ONUnet may be revoked at anytime, with or without notice, for any violation of the Policy, including but not limited to misuse, abuse, infringement of third party intellectual property rights, exceeding authorized access, or vandalism to any system.

This policy applies to networks and resources outside the University that access ONUnet via the Internet. Network or resource providers outside the University may, in turn, impose additional conditions of appropriate use which the user should observe when using those resources.

2. Changes to this Policy

This policy may be changed, altered, or amended at any time. While the University will undertake reasonable efforts to make users aware of changes to this policy, ultimately it is the user's responsibility to visit the University's Information Technology website to learn of these changes.

3. Privacy & System Monitoring

The content of e-mail and data stored on ONUnet should not be considered private or confidential. All emails and other electronic communications sent or stored on the Unviersity's systems are considered the property of the University. The existence of such email, including header information indicating to whom the email was sent or from whom the email was sent along with the time and date of the sending is also not considered private and

confidential. Likewise, files attached to emails stored on ONUnet are also not considered private and confidential.

As a practical matter, the University does not review in the ordinary course the content or attachments of emails. Information Technology staff will, however, generally monitor all activity on ONUnet. Individual users will not be intentionally monitored unless the user shows evidence of activity not in accordance with this Policy or applicable law whether the action is intentionally malicious or not. In such a case, the University will take reasonable steps to ensure the activity ceases. This includes, but is not limited to, monitoring user network traffic, monitoring website accesses, accessing and viewing user data and searching or seizing computers owned by the University, even if used by students, staff or faculty.

While the University strives to maintain stability and security in all network systems, it does not guarantee the security, the confidentiality, or the integrity of any data stored or transmitted through ONUnet. Security precautions and procedures are in place to prevent such occurrences; however, the nature of data transmissions natively is not absolutely secure.

The University will comply with all search warrants and subpoenas. By using the University's systems, you hereby give consent to disclosures in connection with search warrants, subpoenas, and investigations into suspected violations by users of this Policy or applicable law. The University reserves and intends to exercise the right to review, audit, intercept, access and disclose messages and date created, received or sent over its computer and/or systems for any purpose.

4. Lab Computers

The University has several public computer labs on campus. Users are encouraged to use these facilities for research, e-mail, and homework. Users should save documents every 5-10 minutes to prevent loss of data. Documents should always be saved to external media or to the user's network drive. Data that is not stored in these locations may be erased and considered irretrievable. Never load personal programs or change settings on these computers.

5. Personal Computers and Devices

Users are encouraged to bring personal computers to campus. Users are required to have up-to-date antivirus software on their computers. In addition, users are required to install all services packs and important or security updates for their operating system. It may also be necessary to install network support software, such as a network client or security agent. Users are required to register all network connected devices with Information Technology.

5.1. Data Archiving

All data archiving is subject to the University's Intellectual Property Policy. It is the responsibility of Olivet's faculty, staff, and students requesting assistance from

Information Technology to backup all critical information including, but not limited to, documents, spreadsheets, and databases, onto their H drives and/or external media including, but not limited to, CDs, DVD's, external devices, or flash drives. Media content and files should be copied to external media and not network drives.

5.2. Mandatory Copyright License for All Software

Installation of software requires proper licensing. This proof can be in the form of a CD with license kit, or a unique product ID. By using Olivet's network you affirm that you have legal entitlement or licensing to all software, media files, and all other files on your computer.

5.3. Repair Selection Criteria

Information Technology reserves the right to refuse service to any computer. The refusal may occur at any point during the service call.

6. Wireless Access

To compliment ONUnet's wired network, Olivet's Department of Information Technology provides complete campus wide wireless network access for all registered students, faculty, staff and guests in all residential and academic buildings as well as most outdoor locations. Wireless devices must be registered with Information Technology prior to placing them on ONUnet. As complete coverage is available and to decrease disruption to this service users are not permitted to use their own wireless access points (WAP's) or devices capable of performing the function of an access point.

Also to decrease the likelihood of interference, wireless printers are not permitted on ONUnet unless the printer is directly connected to a computer and the wireless features have been disabled.

7. Internet Content Filtering

In accordance and agreement with the University's beliefs, principles, and community expectations outlined in the University Life Handbook, Information Technology will continuously monitor and prohibit access to websites that are pornographic in nature or are deemed inappropriate for the Olivet community.

8. Copyright Infringement: Digital Millennium Copyright Act ("DCMA")

It is the University's policy to prohibit the unauthorized reproduction of copyright protected materials in any medium. The following DMCA policy is part of our Intellectual Property Policy and posted on the University's website:

> If you believe that content available on or through this site ("Website") infringes one or more of your copyrights, please send our Copyright Agent by mail, email or

fax a notification ("Notification") providing the information described below. A copy of your Notification will be sent to the person who posted the material addressed in the Notification.

Pursuant to federal law you may be held liable for damages and attorneys' fees if you make any material misrepresentations in a Notification. Thus, if you are not sure whether content located on or accessible via a link from the Website infringes your copyright, you should contact an attorney.

All Notifications should include the following:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
- Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
- Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
- Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
- A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.\

Notifications should be sent to:

Jeffrey P. Rice
Olivet Nazarene University
One Univeristy Avenue, Bourbonnais Il 60915
Fax: 815-939-5081
Email: copyright@olivet.edu

NOTICE TO REPEAT INFRINGERS OF THE DMCA POLICY:

The University will terminate a user's access to our systems if, under appropriate circumstances, the user is determined to be a repeat infringer. Since most faculty,

staff, and student positions require access to our systems in order to complete duties and obligations, termination of access due to repeat infringement can have serious consequences to employment or continued enrollment.

9. Accounts & Access:

Each full-time student, faculty, or staff member will receive a network account and an e-mail account. E-mail accounts will be maintained as long as the user is associated with the University. Network accounts, including email, will be terminated after graduation or withdrawal or upon termination of employment. Files existing in these accounts will be deleted and will be irretrievable. E-mail accounts may be terminated for any of the following reasons:

- Abuse or misuse, including but not limited to copyright violations or the transmission of pornography
- Withdrawal from the University
- Termination of employment by the University
- Request by the Office of Student Development
- Request by the Director of the Office of Human Resources
- Request by the Academic Dean
- Request by the Director of Information Technology
- Request by the Department of Public Safety
- Dismissal from the University

Network and e-mail accounts assigned to an individual or group must not be used by others. Individuals are responsible for the proper use of the account, including proper password protection. Any action that occurs on an individual's account or workstation is the responsibility of that individual.

10. Passwords

Individual's are responsible for the proper use of all accounts (network, e-mail accounts, etc) including proper password protection. Passwords should never be shared with anyone and should not be written in a location where they can be easily discovered. Any action that occurs on an individuals account or workstation is the responsibility of that individual. No one from Information Technology will ever call and ask you for your password. If this occurs, please notify Information Technology immediately.

11. Network Storage

Each user may be granted a certain amount of storage space on the campus network. This storage may be used to store authorized documents, research, and various class and appropriate personal files. Do not store music or video files on the network unless they are class related. Disk and storage space will be monitored and files may be removed if the user

is abusing the storage space provided. The user is responsible for deleting or removing old or obsolete files.

12. Prohibited Activities

One of the goals of the Department of Information Technology is to provide the Olivet community and authorized users with a secure computing environment and eliminate computer and network abuse originating from Olivet's campus. The University reserves the right to take immediate corrective action without prior notification to the user if a violation is adversely affecting ONUnet or any other telecommunications or computing networks. Immediate corrective action may involve disabling network accounts, e-mail accounts, network access, and any other means of stopping the violation.

The Information Technology Department is charged with implementing enforcement decisions arising from violations of this Policy. The University may, with or without notice, investigate and act upon any known or suspected violations of this Policy or any policy set forth by the University. The University may provide investigative support to, local, state, and federal law enforcement agencies.

Computer facilities at Olivet are a shared resource that requires users to observe standards of behavior to ensure the rights of other users. This resource is a privilege and may be revoked at any time. All users are expected to avoid the following violations:

12.1. Violations

The following list of violations is provided as a list of examples only as is not meant to be exhaustive or complete.

12.1.1. Malicious Activity Violations

- Attempting to defeat the network, servers, or administrative computer's security systems, mechanisms, or controls.
- Possessing, using, distributing, or developing password cracking programs, algorithms, keystroke loggers, or any hacking utility.
- Launching or participating in a denial of service attack or any other action with the intent of damaging or disrupting any network, system, or device on or outside of ONUnet.
- Disabling, tampering with, or accessing any ONUnet system, network device or cabling.
- Any action intended to disrupt normal system services or which adversely affects other users' accounts, electronic material, e-mail, or network performance.

- Any attempt to probe or scan ONUnet or any network outside of ONUnet.
- The creation or intentional distribution of any virus,worm, or malicious code.

12.1.2. Unauthorized Access Violations

- Accessing or attempting to access another users' data without their permission.
- Obtaining or using another person's computer without their knowledge.
- Disguising one's identity in any way, including the sending of falsified messages, removal of data from system files, masking of process names, masking or spoofing of MAC or IP addresses or using any other unauthorized IP address.
- Using or obtaining another user's electronic identification is considered fraud. Electronic identification includes, but is not limited to: voice-mail passwords, telephone dialing codes, login ID, password, MAC address, IP address, e-mail address, ID card, or Tiger Dollars Card.
- Providing any unauthorized user with access to a personal login ID or establishing any function or device which provides unauthorized access to ONUnet via the Internet or otherwise.

12.1.3. Security Violations

- Installing or using a wireless access point that is not owned by the University.
- Neglecting or purposely avoiding registering a personal computer with Information Technology.
- Using a network-based proxy to circumvent content filtering systems, bandwidth control mechanisms, and any network security device.

12.1.4. Digital Piracy Violations

- Obtaining, copying, or distributing copyrighted materials without the expressed written consent of the copyright holder including but not limited to sharing unlicensed peer-to-peer files. See DCMA section above.
- Using, downloading, or installing any peer-to-peer file sharing application.

12.1.5. Personal Conduct Violations

- Sending e-mail or any other type of electronic communication that contains profanity, crude language, or sexually explicit messages, or any content defined as inappropriate by the University to any individual on or off ONUnet.

- Distributing, possessing, or accessing files, images, or videos that are pornographic in nature via ONUnet. This includes, but is not limited to websites, electronic media, peer-to-peer, or file sharing programs.
- Any action that is deemed threatening or harassing to ONUnet users, administrators, or persons outside of ONUnet.
- Using ONUnet for commercial or solicitous purposes.
- Failure to report discovered network security flaws.
- Failure to report incidents of policy violations.

12.1.6. Use of Unapproved Equipment

- Possessing or using routers or manageable switches
- Possessing or using wireless access points or range extending devices
- Possessing or using wireless printers without disabling the wireless features

In addition to other laws, rules, and regulations, all of the violations above, and any similar violations, will be considered acts which exceed a registered user's authorized access rights and may be considered a violation of the federal Computer Fraud & Abuse Act: http://www.law.cornell.edu/uscode/text/18/1030

13. Discovery of Pornographic Materials

If pornographic or obscene files are located on a computer or if the user continuously attempts to access pornographic websites or materials, Information Technology may remove network service from the offending user and associated office, room or apartment. The Office of Student Development, the Office of Academic Affairs and/or the Office of Human Resources will be notified immediately. Service to the area may not be restored until Information Technology receives notice from the Office of Student Development, Office of Human Resources and/or the Office of Academic Affairs to reactivate network service.

14. Disciplinary Actions

Violation of this Policy may be considered a violation of the Computer Fraud and Abuse Act (for exceeding authorized access) and may result in suspension or termination of the user's network access, network account, or e-mail account. Suspending network access for the violator may also result in the suspension of access for the entire room or apartment in which that violator resides (for students). Upon suspending the user's access, the Information Technology Department will notify both the user and the Office of Student Development (for student violations) or the Human Resources Department (for faculty or staff violations). Suggested disciplinary actions for students include one or more of the following:

- Community service

- Fines or restitution equal to technician's time
- Criminal or civil prosecution
- Notification to parents, authorities, or head of academic department
- Dismissal from the University
- Counseling

In addition, violations may subject the user to civil and criminal liability, including but not limited to statutory damages under the Copyright Act or damages under the Computer Fraud and Abuse Act. The University will cooperate with any law enforcement investigations into any user's alleged violations of this Policy and may choose, at its own discretion, to cooperate with any civil complainant.

15. Disclaimer of Liability

Neither the University nor any of its agents will be liable for any losses, including lost revenues, or for any claims or demands against the users of ONUnet by any other party. In no event will the University be liable for consequential damages, even if the University has been advised of the possibility of such damages. The University will not be responsible for any damages due to the loss of output, loss of data, time delay, network system's performance, software performance, hardware damage, incorrect advice from a consultant, or any other damages arising from the use of the University's network systems, information systems, or technicians.