

OLIVET NAZARENE UNIVERSITY

Information  Technology

Computer, Network, and Telephony Acceptable Use Policy and Guide to ONUnet:

Student Edition

Department of Information Technology
Olivet Nazarene University
(815) 939-5302



2004-2005

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/policy.html>. By agreeing to the policies set forth by the University in the Student Life Handbook, the student 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 and System Monitoring
- System Maintenance
- Lab Computers
- Student Computers
 - Minimum Supported Requirements
 - Typical New Systems 2004 – 2005
 - Services
 - Supported Operating Systems
 - Data Archiving
 - Abandonment
 - Copyright Infringement Protection
 - Repair Selection Criteria
- Computer Registration
- Wireless Access
- Internet Content Filtering
- File and Music Sharing Application
- E-Mail & Network Accounts:
 - Passwords
 - Network Storage
 - Prohibited Activities
 - Violations
 - Discovery of Pornographic Materials
 - Disciplinary Actions
 - Telecommunications
 - Resources
 - Services
 - Policy
 - Matters of Courtesy
 - Disclaimer of Liability

ONUnet

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 the University Life Handbook. Persons accessing any of the network resources are expected to practice common sense, decency, and courtesy to other users. 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.

ONUnet is a privilege and may be revoked at any time. It is provided as a resource to the Olivet community. ONUnet is restricted to authorized users, which is defined as an individual who has been assigned a 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 misuse, abuse, or vandalism.

This policy is extended 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.

Telecommunications

Olivet's Department of Information Technology provides one digital telephone for each residential room on campus. In some cases two phones will be provided in two bedroom apartments. These phones are proprietary, meaning they will only work on our telephone system. Other phones or computer modems will not work and could be damaged if plugged into the phone jack. Accordingly, Olivet provides lines, jacks, phones, and cords. Information Technology will also provide technical service to maintain this equipment.

All residential students are provided with their own individual direct dial telephone number with an associated voice-mail box for the duration of their stay at Olivet. The voice-mail system allows for an online directory to Olivet phone numbers by dialing 1411. A printed University Telephone Directory is available near the end of September of each year. Off-campus students are intended to be included in the printed directory. Off-campus students are responsible for having their correct and current local phone number in the student database. Call the Registrar at 939-5201, or the Help Desk at 939-5302, to ensure your correct phone number is listed.

Students should activate their voice-mail by inserting a seven digit password and recording their name. A recorded greeting is optional. Students may use their room phones for local (8 mile radius) and campus calling without a monthly charge. Long Distance calls will be billed to the student through Resicom, a billing agency, who will provide account codes (PIN-Personal Identification Numbers). Resicom may be contacted via the following methods: <http://www.resicom.com>, dial 7800 from campus, or 800-853-1030 for information about their discount program or any other questions.

RESICOM accounts are limited to \$100, after which the account number is deactivated. Bad debts with RESICOM will be placed on the student's account at Olivet. There is a one-time fee for the telephone service of \$25, charged the first year a student is at Olivet.

Disciplinary Actions

Violation of the Information Technology Policies may result in suspension of the user's network access, network account, or e-mail account. Removing network access for the violator may also remove access for the entire room or apartment. Upon suspending the user's access, Information Technology will notify both the user and the Office of Student Development. The notice will state which policies were violated and the next course of action. The user must respond to the letter within 24 hours. Suggested disciplinary actions 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

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 the University Life Handbook. Persons accessing any of the network resources are expected to practice common sense, decency, and courtesy to other users. 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.

ONUnet is a privilege and may be revoked at anytime. It is provided as a resource to the Olivet community. ONUnet is restricted to authorized users, which is defined as an individual who has been assigned a 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 misuse, abuse, or vandalism.

This policy is extended 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.

Changes to this Policy

This policy may be changed, altered, or amended at any time by Information Technology administrators. While Information Technology will make every effort to make users aware of changes to this policy, ultimately it is the user's responsibility to learn of these changes.

Privacy & System Monitoring

E-mail and data stored on ONUnet is considered private and confidential. The Information Technology staff of Olivet Nazarene University will strive to ensure the privacy and confidentiality of all user data. Information Technology staff will, however, generally monitor all activity on ONUnet. Single users will not be intentionally monitored unless the user shows evidence of activity not in accordance with this policy whether the action is intentionally malicious or not. In this case, Information Technology staff will use any means possible 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 student computers.

While Olivet Nazarene 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.

System Maintenance

Regular network maintenance will be performed on ONUnet at any time. Normally this maintenance will not require network downtime. Occasionally, systems malfunction without warning. At these times, Information Technology staff may, at their own discretion, take whatever action is necessary to restore the system. . If there is a foreseeable issue with the equipment, Information Technology staff will send out a notice to all students, faculty, and staff informing them of the problem and the estimated time the resource will be restored. Information Technology has reserved one Friday¹ night each month in which non-critical network maintenance will be performed. On these dates, network access may be unavailable between the hours of 6:00pm until 7:00am the following morning. These dates are:

Fall/Winter 2004:

September 10

October 8

November 12

December 17

Spring/Summer 2005

January 14

February 18

March 18

April 8

May 20

June 17th

July 15th

August 12th

Lab Computers

The University has several public computer labs on campus. Students are encouraged to use these facilities for research, e-mail, and homework. Students should save documents every 5-10 minutes to prevent loss of data. Documents should always be saved to a floppy disk drive, a USB disk drive, 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.

Student Computers

Students are encouraged to bring personal computers to campus. A minimum of two data ports are provided in each living area to provide access to ONUnet from the dorms. In cases where there are three or more persons in a room, Information Technology will provide for extra connectivity. If extra connectivity is needed contact, Information Technology Help Desk at ext. 5302.

Students are required to have up-to-date antivirus software on their computers. Students may use their own virus software or use virus software provided by the University. The University will supply each student with virus software at no charge. This software can be installed when the student registers his or her computer. It may also be necessary to install network support software, such as a network client.

¹ Dates may be adjusted based on network need, student event schedule, or conference event schedule. Please visit <http://it.olivet.edu> for any date changes.

Types of Computers

Olivet's Department of Information Technology services many different types of computers each year. As computers age, repair and integration with ONUnet becomes increasingly difficult and in some cases impossible. Computers not meeting the minimum requirements may function adequately on ONUnet and users are welcome to attempt to connect the computers to ONUnet, however, support will not be given. All operating systems must have the English language installed.

Minimum Supported Requirements for Desktops and Laptops

Type: IBM® Compatible

Processor: Pentium III450

RAM: 64MB

Hard Drive: 500 MB Free Space

CD-ROM: 24X

NIC: Ethernet 10/100

Operating System: Windows 2000 and higher, excluding Windows ME

Typical New Systems –2004-2005

The following is a description of a typical new computer brought on campus. These specifications are intended be used as a guideline when purchasing a new computer. Information Technology does not guarantee this system will be functional on ONUnet for four years.

DESKTOP

Type: IBM® Compatible

Processor: AMD Athlon XP 3000 or Intel Pentium IV 3.0 Ghz

RAM: 512MB RAM

Hard Drive: 80 GB +

CD-ROM: 52X +

NIC: 3Com® Network Interface Card 10/100, Intel based, or integrated

Operating System: Windows 2000®, Windows XP Professional Edition®

An ISP, 5.6.Kbps modem, DSL, or Cable Modem (*online grad students only*)

LAPTOP

Type: IBM® Compatible

Processor: AMD® Athlon® XP 2800, Intel® Pentium® IV 2.8 GHz, or
Centrino® 1.5.GHz

RAM: 256MB RAM

Hard Drive: 40 GB+

CD-ROM: 40X +

NIC: 3Com® PCMCIA Network Interface Card, Intel based, or integrated

Operating System: Windows 2000®, Windows XP Professional Edition®

An ISP, 5.6.Kbps modem, DSL, or Cable Modem (*online grad students only*)

Supported Operating Systems

Many computers are arriving on campus that use Microsoft Windows 98, Microsoft Windows ME, Linux, and Macintosh. Although these systems may integrate with ONUnet, the Department of Information Technology will offer no support for these devices with operating systems other than Microsoft Windows 2000, or XP Professional. Limited support will be available for XP Home edition.

Services

The PC Repair Team of the Department of Information Technology offers many computer repair services.

No charge will be made to students for the following:

- Networking problems
- Novell client related issues
- Hard Disk Defragmentation
- Hard Disk Integrity Checking
- Floppy Disk Data Recovery
- Inspections
- Diagnostics
- Internal cleaning and dusting
- Installing Novell Client

A charge of \$25 per hour with a two-hour price cap (\$50 maximum) will be made to students for items at the technician's discretion and specifically for the following:

- Hardware issues (installations of the following: hard drives, network cards, RAM, etc.)
- Operating system reinstalls
- Virus problems
- Program installations
- File copies or data transfers
- User negligence

ONU Dell service agreement

Olivet Nazarene University currently has a hardware service agreement with Dell Computer Corp. This agreement allows University personnel to work on Dell computer hardware that is currently under warranty at no cost to student, faculty, or staff. This agreement does not include the maintenance or repair of Dell branded printers, scanners, or peripherals. This agreement pertains strictly to hardware only. All Dell computers not under warranty will be assessed regular service fees. The University will charge regular service fees for all services performed outside the Dell warranty agreement.

Data Archiving

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, floppies, CDs, zip disks, external hard drives, or flash drives. Media content and files should be copied to external media and not network drives.

This data should be archived prior to placing a work order. Once a work order is placed it will be assumed by Information Technology that all critical information is already archived. Parties that require assistance archiving data should call Information Technology at x-5302.

Abandonment

Repairs performed on computers will be completed as soon as possible. Owners will be notified as soon as the computer repair is complete. Owners must retrieve their computer as soon as it is convenient. Information Technology will notify the owner with one phone call, one e-mail, and one written notice. Machines not retrieved within 30 days of the completion notice will be considered abandoned and will become the property of the University.

Copyright Infringement Protection

Installation of software will require proof of licensing. This proof can be in the form of a CD with license kit, or a unique product ID. These items must be inspected and received by Information Technology personnel before any operation is performed on a personal computer. All software licensing agreements performed during the installation of a program will be made on the behalf of the student.

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. The criteria for refusal of service may include any of the following:

- Nature of the hardware
- Failure to provide sufficient software license information
- Work environment
- Discretion of the on-site service technician

Complimentary University Provided Software

Olivet Nazarene University provides software to students during their stay at Olivet at no cost. This software includes Computer Associates E-Trust antivirus software and Microsoft's Office 2003 Professional Suite. This suite includes MS Word, Excel, Powerpoint, Access, and Outlook.

Computer Associates E-Trust anti-virus software is available on the student CD included in the registration packet. It is also available via download at registermycomputer.olivet.edu.

Microsoft Office 2003 is available through the cashier's office in Miller Business Center. A \$50 deposit is required for use of the CD media. Once the CD is obtained it is available to install on any ONU student computer. It must be returned

to Miller Business Center in good condition within three business day or the deposit will not be refunded.

Computer Registration

Students are required to register all network connected devices with Information Technology. This registration process must be done the first time the device is connected to ONUnet and each fall semester the student is enrolled. The registration process must be done online at <http://registermycomputer.olivet.edu>.

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, and staff in all residential and academic buildings as well as most outdoor locations. Students are encouraged to use these services by bringing their own 802.11 a,b, or g wireless access cards. Wireless access cards must be registered with Information Technology prior to placing them on ONUnet. As complete coverage is available and to decrease disruption to this service students are not permitted to use their own wireless access points (WAP's) .

Internet Content Filtering

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

A third-party service monitors Internet sites around the world and provides Olivet with regular updates of these sites. This third-party service assigns these sites to categories. Information Technology filter entire categories that contain content that is contrary to the spiritual principles of the University.

Occasionally, legitimate sites are blocked. Information Technology staff may investigate sites that users feel should or should not be blocked. If a user discovers a site that should not be blocked, the individual should e-mail whyisthispageblocked@olivet.edu. When contacting Information Technology, remember a real person responds to these e-mails and will try to help. Please be courteous and civil in your communications.

To investigate sites that should not be blocked, the following information must be included in the e-mail:

1. To ensure messages are coming from on campus, an Olivet e-mail account must be used.
2. The exact URL being blocked
3. A simple explanation why this page should not be blocked.

If these conditions are not met, the request will be delayed or discarded. Any request sent using a rude, derogatory, uncivil language or tone will be disregarded and a copy of the

communication will be sent to the Director of Information Technology for further action. The student may be subject to further disciplinary action by the Office of Student Development.

File and Music Sharing Applications

It is University policy to prohibit the unauthorized exchange of copyrighted materials over any medium including file sharing applications such as KaZaa, BearShare, Morpheus, or Gnutella. Information concerning persons using file sharing programs may be given to authorities without the user's knowledge. Pay-for download services such as I-Tunes and Napster are allowed on a limited basis.

E-Mail & Network Accounts:

Each full-time student, faculty, or staff member will receive a network account and an e-mail account. E-mail maintenance will be regularly preformed. Student e-mail accounts will be limited to 50MBs. While no incoming e-mail message will be rejected, accounts exceeding this limit will be denied the ability to send e-mail. E-mail accounts will be maintained as long as the user is associated with the University. Accounts will be terminated after graduation or withdrawal. Files and e-mail existing in these accounts will be deleted and should be considered irretrievable. E-mail accounts will also be terminated for the following reasons:

- Abuse or misuse
- 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
- Dismissal from the University

Network and e-mail accounts assigned to an individual or group must not be used by others without explicit permission from the owner or administrator. 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.

Information Technology will attempt to filter viruses from e-mail received by Olivet students, faculty, and staff. Users will be notified if a virus was contained in an e-mail that was directed to them.

Information Technology will also attempt to mark or filter spam and unsolicited e-mail from entering the campus. During this process, legitimate e-mail may be inadvertently filtered. Users should contact Information Technology if this occurs. If you receive spam you feel should have been filtered, forward the e-mail to SPAMCOP@OLIVET.EDU. Information Technology will analyze the e-mail and, if certain criteria are met, the addresses may be added to the blocked list.

Passwords

Individuals 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 individual's 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.

Every 90 days, users are required to change passwords. When choosing a new password use a combination of upper and lowercase letters, numbers, and special characters (i.e. !@#\$%^&*).

If a password is forgotten, Information Technology can issue a new password. Information Technology will not give passwords over the phone. Individuals requiring their password to be reset must visit Information Technology in person and request a password reset.

Network Storage

Each user is granted a certain amount of storage space on the campus network. Typically this will be identified as the H:\ drive when a user logs into the network. This storage may be used to store documents, research, and various class and 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 multimedia files may be removed if the user is abusing the amount of storage space provided. The user is responsible for deleting or removing old or obsolete files. Users may also access the files via the Internet by going to <https://storage.olivet.edu>.

Prohibited Activities

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

Information Technology staff members are charged with enforcing the Information Technology Policies which appear in part within the University Life Handbook and on the Information Technology website (<http://it.olivet.edu/policy.html>), and any other policy set forth by the University. Staff members will respond to all network incidents including denial of service attacks, virus incidents, and any other malicious or inappropriate behavior that occurs on ONUnet. Information Technology may, with or without notice, provide investigative support to University, local, state, and federal law enforcement agencies.

Computer facilities at Olivet are a shared resource that require's 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:

Violations

The following list of violations is not meant to be exhaustive or complete. Violations of the telecommunication or computing network policy are by no means limited to this list.

- Attempting to defeat the network, servers, or administrative computer's security systems, mechanisms, or controls.
- 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.
- 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.
- Possessing, using, distributing, or developing password cracking programs, algorithms or any hacking utility.
- 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.
- Any action intended to disrupt normal system services or which adversely affects other users' accounts, electronic material, e-mail, or network performance.
- Obtaining, copying, or distributing copyrighted software without the expressed written consent of the copyright holder.
- Accessing or attempting to access another users' data without their permission.
- Using another person's computer without their knowledge to accomplish any action that is in violation of Olivet's Computer User Code of Conduct.
- Any attempt to probe or scan ONUnet or any network outside of ONUnet.
- Any action that is deemed threatening or harassing to ONUnet users, administrators, or persons outside of ONUnet.
- The creation or intentional distribution of any virus or worm.
- Disabling, tampering with, or accessing any ONUnet system, network device or cabling.

- 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.
- Using ONUnet for commercial or solicitous purposes.
- 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.
- Failure to report discovered network security flaws.
- Failure to report violations incidents of policy violations.
- Using a network-based proxy to circumvent content filtering systems, bandwidth control mechanisms, and any network security device.
- Sending e-mail or anyother type of electronic communication that contains profanity, crude language, or sexually explicit messages 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.
- Using, downloading, or installing any peer-to-peer file sharing application such as Gnutella, BearShare, KaZaa, or Morpheus.

Discovery of Pornographic Materials

If pornographic or obscene files are located on a student owned 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 room or apartment. The Office of Student Development and/or the Office of Academic Affairs will be notified immediately. Service to the room or apartment may not be restored until Information Technology receives notice from the Office of Student Development and/or the Office of Academic Affairs to reactivate network service.

Disciplinary Actions

Violation of the Information Technology Policies may result in suspension of the user's network access, network account, or e-mail account. Removing network access for the violator may also remove access for the entire room or apartment. Upon suspending the user's access, Information Technology will notify both the user and the Office of Student Development . The notice will state which policies were violated and the next course of action. The user must respond to the letter within 24 hours. Suggested disciplinary actions 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

Telecommunications

Resources:

Olivet's Department of Information Technology provides one digital telephone for each residential room on campus. In some cases two phones will be provided in two bedroom apartments. These phones are proprietary, meaning they will only work on our telephone system. Other phones or computer modems will not work and could be damaged if plugged into the phone jack. Accordingly, Olivet provides lines, jacks, phones, and cords. Information Technology will also provide technical service to maintain this equipment.

Services:

Each residential student is provided with their own individual direct dial telephone number with an associated voice-mail box for the duration of their stay at Olivet. The voice-mail system allows for an online directory to Olivet phone numbers by dialing 1411. A printed University Telephone Directory is available near the end of September of each year. Off-campus students are intended to be included in the printed directory. Off-campus students are responsible for having their correct and current local phone number in the student database. Call the Registrar at 939-5201, or the Help Desk at 939-5302 to ensure your correct phone number is listed.

Students should activate their voice-mail by inserting a seven digit password and recording their name. A recorded greeting is optional. Students may use their room phones for local (8 mile radius) and campus calling without a monthly charge. Long Distance calls will be billed to the student through Resicom, a billing agency, who will provide account codes (PIN-Personal Identification Numbers). RESICOM may be contacted via the following methods: <http://www.resicom.com>, dial 7800 from campus, or 800-853-1030 for information about their discount program or any other questions.

Olivet provides room locator information to the E911 emergency services system.

Other services provided include music on hold and direct dial calling, both USA and internationally. There is also an 800 number which gives students access to charge calls to their accounts from anywhere in the continental USA.

Policy:

There is a one time telecommunication fee of \$25 applied the first year a student lives in student housing. This is good for four or more years. Olivet places a limit of \$100 per month on student invoices. Accounts that exceed the limit are deactivated.

Olivet will assign to the student's account on campus any unpaid telephone invoices that Resicom turns over as delinquent. These charges will be treated as any other charge to the student's account. Resicom will deactivate the student account blocking further charged calling.

A reactivation fee will be placed on any account that is deactivated due to exceeding the limit or delinquency. A prepaid account will be required if the account is turned over to Olivet for collection; see Reicom's policy manual at its web site: <http://www.resicom.com>

It is the policy of Olivet that telephone service is not to be used in a harassing or threatening manner. Campus Telecommunications will trace all such activity. The results of the trace will be given to the Office of Public Safety and the Office of Student Development.

Olivet reserves the right to monitor and remove any inappropriate greeting placed in the voice mail system. Individual voice-mail service may be removed if used inappropriately. Olivet reserves the right to deactivate phone service from a room if improper use of equipment or service persists.

Matters of Courtesy

Users should be aware that computer and telephone use involves matters of courtesy:

- Always be polite and courteous in any communication.
- Network files should be deleted when no longer needed to make disk space available, and so that repeated backups of unneeded files can be avoided.
- Because printing can be expensive, users should preview documents before printing, print as few draft copies as possible, and print only as many final copies as necessary.
- To avoid "junk mail" electronic messages, users should consider the level of interest of the targeted audience before sending electronic mail to large groups.
- Never send anything that would embarrass you if it were passed on to other people. E-mail is simple to duplicate and spread. Be cautious what you write.
- Use your e-mail and voice-mail in a professional and courteous manner.

- Do not send e-mail or voice messages that are harassing, abusive, or threatening.
- Do not write e-mail or leave voice-mail when you are particularly upset. If you choose to compose a message anyway, delay sending it until you have had some time to calm down.
- Also be cautious about using biting sarcasm or humor. E-mail doesn't allow for facial expressions or vocal inflections, so the recipient could take your comment to be insulting or degrading. Prevent adverse reactions by using some common sense.
- Chain letters and forwards are annoying and generally pointless. They also provide scores and scores of e-mail addresses to people who might harass the people using those addresses. Use some discretion before you use the forward command.
- If you are not the only person who receives a specific e-mail, don't reply to everyone who did, unless there is a specific reason to do so.
- When you leave a computer after you've logged in, be sure to log out or lock the screen, even if you think you're only going to be gone for a few moments. A lot can happen when you're not around. You are responsible for any offensive messages sent from your e-mail account and any actions done from the machine while you are logged in.
- Remember that all laws regarding copyright, defamation, discrimination and other forms of written communication also apply to e-mail.
- If you become aware of any person who violates this policy, please report it immediately to Information Technology at ext 5302. Your name will be kept anonymous.

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 PC Repair technicians. The University will attempt to correct conditions and restore information losses.