Revised: November, 14nd 2013

Oakwood University Computer and Network Access Policy

Chapter 1: Oakwood University Computer Usage

Section 1.0 Appropriate Use

Accounts are provided for academic research and instruction, electronic mail, Internet access, and for activities related to the mission of Oakwood University. Each account represents an allocation of a scarce computing resource and as such is monitored by Oakwood University administrators for appropriate use. Each account is assigned for the sole use of a single user. Sharing of accounts is prohibited. The user for whom the account was created is responsible for the security of the account and all actions associated with the use of the account. Accounts may be revoked if the account is found to have been used for activities that violate any portion of this policy, the owner of the account has been found violating any portion of this policy, or the owner of the account is no longer enrolled or employed by Oakwood University. Activation of an account on an Oakwood University Host computer constitutes an agreement stating that the user understands and will abide by all policies regarding the use of the Oakwood University network.

Chapter 2: Oakwood University Computer Accounts

Section 2.1 Inactive Accounts

Active accounts are changed to the inactive state prior to deletion. The inactive state is an intermediate step between an active account and a deleted account. In the inactive state, all host access is denied and electronic mail addressed to the account is returned to the sender. Some files may be archived and deleted. An account may be reactivated from the inactive state up until the time that it is actually deleted. When an account is deleted, the username is considered unused and all files in the user's home directory are deleted. Electronic mail sent to the user is rejected.

Section 2.2 Restricted Accounts

On occasion an account may be temporarily restricted. There are many reasons why this may occur ranging from misuse of network resources, to important information that needs to be given to the user before they attempt to login again. Upon attempting to log in, the user sees a short message to the effect of "Please see the System Administrator" and the user is immediately logged out. In most cases, once a meeting with the System Administrator is completed, the account is reinstated.

Section 2.3 Sharing Accounts

Any abusive activities initiated from an account are traced back to the account owner and the account owner is held accountable. The behavior of someone with whom you have shared your account becomes your responsibility. If the abuse is such that network privileges are terminated, it is the account owner (you) who suffers. Therefore, it is the policy of Oakwood University that Oakwood University User Names are not to be shared. Each Oakwood University User Name has only one Oakwood University authorized user. If users wish to share information or otherwise collaborate in a group, then the users shall use appropriate file permissions combined with appropriate group membership to share data.

Section 2.4 Selecting a Password

Perhaps the most vulnerable part of any computer system is the account password. Any computer system, no matter how secure it is from network or dial-up attack, Trojan horse programs, and so on, can be fully exploited by intruders who can gain access via a poorly chosen password. It is important to select a password that is not easily guessed and to not share the password with ANYONE.

Chapter 3: Abuse of Computing Resources

Section 3.1 Theft and Vandalism

Oakwood University computing resources are shared by all network users on a fair and equitable basis. It is the responsibility of Oakwood University not only to provide these computing resources but also to insure that the rights of users are not infringed upon by the abuse of another. Therefore, Oakwood University utilizes every means available to detect, restrict and/or prosecute individuals responsible for the abuse of computing resources. This section serves to provide specific examples of the types of abuse not tolerated. This list is by no means complete and is subject to change without notice as new ways of abusing resources are discovered. Penalties for abuse of network resources include but are not limited to temporary restriction of network privileges, permanent restriction of network privileges, and criminal prosecution.

The appropriate Oakwood University authorities handle theft and vandalism of Oakwood University Computing resources. Oakwood University pursues and supports criminal prosecution of individuals suspected of theft and/or vandalism.

Section 3.2 Worms and Viruses

Anyone attempting to write, ftp or knowingly proliferate worms or viruses of any size, shape, or form will be remanded for criminal prosecution (and will lose their computing privileges).

Section 3.3 Use of .rhosts Files

Through the use of .rhosts files users can allow others access to their account without the knowledge of a password. This is not only a breach of security but violates the policy on account sharing as well. Use of .rhosts files is prohibited. When found, they will be deleted. Repeat offenders will lose their computing privileges.

Section 3.4 Transferring Files

Using ftp to transfer files to or from remote sites, which violate the policies of the remote site, is prohibited. In particular, transferring files which are large, contain material offensive to either site, contain information to be used for the financial gain of any party, or contain monetary or sexual solicitations is prohibited. Restrictions pertaining to the duplication of copyrighted materials also apply.

Section 3.5 Games Network Games Policy

A computer network like Oakwood University’s is a powerful tool, for both recreational and non-recreational applications. For the purposes of this document, all recreational uses of the network, including but not limited to network strategy games, action games, MUDs, and chat programs, are described as "games".
In general, most games are permitted on the Oakwood University network. Games played on the network must comply with the same rules as all other network applications and must pose no risk of interference with other network operations. They must also comply with all other Oakwood University policies, including ethics policies.
Non-game network traffic has priority at all times. Games that interfere with non-game traffic, even if run within network bandwidth limitations, are prohibited from the Oakwood University network.

Some games are banned from the Oakwood University network because they have already been found to interfere with network operations.

In the event of a conflict between this policy and the policies of individual offices, labs, and computing facilities on campus, the most restrictive takes precedence. For example, if a lab says, "no games", no games are allowed in that lab.

Section 3.6 Disruptive Behavior

The Oakwood University Labs are designed to provide computing and network resources to students and employees who need them to fulfill their role in the University's mission. Since Oakwood University provides these resources for use in academic research, education and extension, the Oakwood University Labs are in effect no different than other classrooms and labs on campus and lab patrons should behave accordingly. Loud talking, profanity, boisterous or otherwise disruptive behavior is prohibited. Children are not allowed in the Oakwood University Labs. Eating, drinking, and the use of tobacco or controlled substances are also prohibited in the Oakwood University Labs.

Section 3.7 Oakwood University Unauthorized Use of Computing Resources

You must have an Oakwood University computing account to use the Oakwood University computing resources. Persons found using Oakwood University computing resources without an active account will be referred to the appropriate Oakwood University authorities. For University staff, students and faculty the individual's department head and/or dean will be notified. Incidents involving individuals not directly associated with Oakwood University will be handled by the HSV Police Department. If direct expenses are incurred during Oakwood University authorized use (i.e. paper, printer supplies, etc.), Oakwood University reserves the right to pursue full reimbursement of those costs from the individual.

Use of restricted network services without Oakwood University authorization is considered an abuse of privilege and a violation of security and may result in restriction or denial of network access. Current restricted network resources include Oakwood University Lab printers, printers reserved for use by an individual, department or research group, and workstations and servers, which have restricted login access.

Section 3.8 Breaking Into Accounts

Any attempt to gain access or to use an account other than by the owner is considered a severe violation of network policy. Such attempts include, but are not limited to

- Gaining access to a user's account while the user is away from a terminal or a workstation or
- Making efforts to determine another user's password by closely watching a login or
- Developing applications, which request or capture user passwords.

The appropriate action if you find another user logged on to an Oakwood University Lab machine or computing resource but not near the machine is to 1) determine who is the user, 2) try to locate the user, and 3) if the user is not found, log the user out immediately. Do not tamper with any programs or data files in the user's directory.

Section 3.9 Cracking Passwords

Any attempt to crack or otherwise obtain passwords is prohibited. Storing or transferring encrypted or unencrypted password information is prohibited. Writing, transferring, compiling, storing or running programs designed to guess passwords or otherwise gain unauthorized access to user or system accounts or passwords are prohibited. This includes programs or techniques designed to trick users into divulging their password.

Section 3.10 Misuse of Accounts

An account is assigned to an individual. Account sharing is prohibited. Using instructional accounts for funded research purposes is prohibited. Your account is your user identification when accessing computing resources. Any attempt to impersonate another user or conceal your identity when sending e-mail or posting to news groups is prohibited.

Section 3.11 Unauthorized Access of User Files

Unauthorized access to information contained in a user's home directory is prohibited, even if the files are readable and/or writable. When in doubt, don't read, copy, or change other users' files.

Section 3.12 Unauthorized Modification of Files

Modifying files anywhere on the system without consent of the file's owner is prohibited. This includes writing or modifying files, which have file permissions set to allow modification or writing. This also includes creating new files, renaming, or deleting existing files in directories which may have directory permissions set to allow creation or modification of files. When in doubt, don't write.

Section 3.13 Unauthorized Broadcast Messages

Sending unauthorized broadcast messages is prohibited. Sending profanity or messages abusing another user is considered a severe network violation and will result in the loss of network privileges.

Section 3.14 Use of Computing Resources For Monetary Gain

Use of Oakwood University computing resources for monetary gain or pecuniary purposes is prohibited. However, resume preparation and distribution is allowed.

Section 3.15 Licensing and Copyright Infringement

Most software packages and applications are licensed and/or copyrighted. Most licenses and copyright agreements specifically prohibit copying or unauthorized use of the software or data. When in doubt, don't copy.

Chapter 4.0 Appropriate Use of Copyrighted Material

Oakwood University expects all departments and students to be aware of how intellectual property laws, regulations, and policies apply to the electronic environment and to respect the property of others.

Chapter 5.0 Disrupting or Degrading Service

Disrupting or degrading a network service is prohibited. In a large integrated computer network that is shared by a large number of users, such as the Oakwood University network many services depend upon distributed computing resources and often upon other network services. These resources include servers, printers, workstations, and the network infrastructure (hubs, routers, cabling system). These resources function in a cooperative manner to provide the variety of network services enjoyed by our many users. It is often difficult to ascertain what impact the disruption or degradation of a computing resource or a network service may have on other network users. Therefore, any disruption or degradation of service is prohibited.

The following is a short list of some methods of disruption or degradation of service:

- Turning a machine off
- Unplugging the network connection for a machine
- Modifying or reconfiguring the software or hardware of a computer or network facility. Do not modify the hardware, operating system, or application software of an Oakwood University computer unless you have been given permission to do so by the Oakwood University department or administrative unit that is in charge of the machine. The other users with whom you share the machine, and the technicians on whom you rely for support, are expecting to find it set up exactly the way they left it.
- Attempting to use more resources than the machine can handle (i.e. running a large number of I/O or computationally intensive applications)
- Excessive printing, using excessive disk space, or otherwise degrading system performance by monopolizing shared resources.
- Sending excessive email

- Running programs which lock the screen or keyboard (exceptions to this are system administrators or system administration employees working on systems related programs and machines located in offices with the approval of the office occupant

Section 5.1 CPU Usage

The machines on the Oakwood University network represent an enormous amount of processing power. It is tempting for users to attempt to run programs on as many machines as possible to decrease the total turnaround time of the job. However, running jobs on remote machines can have a serious impact on the interactive performance of the machine. This could render the machine virtually unusable to anyone else. This problem is even more acute if the offending program performs a large amount of I/O, bogging down the network and the file servers. In general, using multiple remote machines for running computational programs is prohibited. If a user has a large computational problem they should contact the systems administrator to work out a plan BEFORE running the program.

Section 5.2 Exceeding Disk Quotas

Disk quotas are in effect on the Oakwood University network. Failure to reduce your file storage below your quota within a reasonable period of time results in the deactivation of your account and e-mail address and the removal of your files.

Section 5.3 Misuse of Usenet News and Web Content

News postings deemed obscene, unduly inflammatory, or in violation of the Oakwood University harassment/discrimination are considered an abuse of network privileges. Do not post any message you would not be willing to tell someone face to face. Any attempt to forge a news posting is considered an abuse of network privileges.

You may not use the internet to access, view or download any obscene material on your personal computer or any computers owned by Oakwood University. This includes but is not limited to, pornography of any kind.

Oakwood University reserves the right to monitor and log any and all web pages that are being accessed by any employee or student of Oakwood University.

Section 5.4 Violation of Remote Site Policies

Users of remote sites or remote site services are bound by the rules, and policies of the remote site. If you do not know the remote site's rules and policies, adhere to those outlined in this document. IT cooperates fully with remote site system administrators in the investigation of remote site policy violations.

Section 5.5 Installing Software on Oakwood University Lab Machines

Oakwood University provides general-purpose software in the Labs and installs approved applications at the request of Oakwood University departments. Lab patrons should not install unapproved or personal copies of software.

Chapter 6: Enforcement

Section 6.1 Temporary Restriction

An individual's account on the Oakwood University network may be temporarily restricted due to many reasons, including:

- Maintenance or servicing of network resources

- Dissemination of information before continued use of an account
- Investigation of policy violations or suspected abuse of resources

Temporary access restrictions are intended to be short lived and usually require the account's owner to contact the appropriate system administrator for reactivation. Note that investigations of network policy violations may require any number of potentially affected accounts to be temporarily restricted. The owner of the account may not be the object of the investigation if, for example, it may be suspected that the user's password has been cracked by a third party.

Section 6.2 Permanent Restriction

If it is determined that a user's policy violations are so serious that continued use of the Oakwood University Network would infringe upon the rights or security of other users, the user's account will be permanently restricted. Permanent access restrictions must be approved by the Director of the Information Technology or his designated representative. All accounts assigned to a user may be restricted and future network privileges denied.

Section 6.3 Severe Abuse

Individuals accused of severe abuse may be referred to the Oakwood University's Discipline Committee for further action or to the appropriate law enforcement agency.

Chapter 7: Reporting Problems

Section 7.1 Physical Security

Physical security is the most important part of system security. Electronic security means nothing if the whole machine is stolen. Users should keep an eye out for any suspicious activity. If an alarm sounds in an Oakwood University Lab use the lab phone to report the problem to the IT Help Desk at (726-7464) or contact the HSV Police at 911.

Section 7.2 Theft and Vandalism

Theft and vandalism should be reported immediately to the Huntsville Police as well as to IT. Do not touch anything at the scene of the crime in order to prevent the destruction of potential evidence.

Section 7.3 Electronic Security

Users who suspect that the security of their account has been breached should notify the Oakwood University Help Desk as soon as possible (726-7464). The Oakwood University Help Desk will alert the system administrator.

Section 7.4 Notification of Remote System Administrators

Violation of policies on remote system may require notification of the remote system administrator. If a remote system administrator is contacted, please notify Help Desk (726-7464).

Section 7.5 Inoperative and malfunctioning Equipment

Inoperative/malfunctioning machines and other hardware problems in the Oakwood University Labs should be reported to Oakwood University Lab Support Services.

Section 7.6 Software Problems

All software problems on Oakwood University computers should be reported to the Help Desk (726-7464) or logged in the Track-it system.

Section 7.7 Banned Programs and Utilities

All programs, services, servers, and protocols used on the Oakwood University network must comply with all applicable standards, must comply with all Oakwood University's policies, and must not interfere with proper operation of the network.

The following programs, servers, services, and protocols interfere with proper operation of the network and/or offer substantial potential for such interference and security breech. They are therefore forbidden on the Oakwood University network without prior approval from the Technology Department.

This list is not limited to and may be amended by decision of the manager of the Technology Department or an Oakwood University authorized representative.

- Utilities:
  - KeyClient before version 4.2.06
  - HP JetAdmin before version 2.4.0
- Games:
  - DOOM version 1.0
  - Spectre, all versions
- Network services and equipment:
  - Routers Including Wireless AP's (of ANY protocol)
  - DHCP servers
  - BOOTP servers
  - RARP servers
  - Proxy ARP servers
  - NDS trees
  - DNS (Domain Name System) servers
  - Novell servers
  - WINS (Windows Name Service) servers
  - Remote access (dial-in) servers of any type (including, but not limited to modems attached to computers which are connected to the Oakwood University network)
  - VPN (virtual private network) servers or workstations
  - News (Usenet) servers
  - Tunneling services
  - Wireless Access Points (sometimes called base stations) routers, and alike. ***also see Ch. 8***
  - Dedicated Firewalls (however, software firewalls such as ZoneAlarm, Norton Firewall, BlackIce, etc. on individual systems are permitted and encouraged)
  - Any service or application, which communicates using multicasts without the express permission of the Technology Department. Use of multicasts in the current network environment can easily overload the 10-megabit Ethernet parts of the network. Most of the Ethernet equipment we have does not support the management of multicast traffic.
  - Unmanaged Ethernet switches and Ethernet hubs (repeaters) are permitted. Cabling between a system and the switch or hub must be entirely contained within the immediate room where the switch or hub is located.
- Protocols:
  - IPX over layer 2 using a frame type other than Ethernet II
  - NetBIOS over IPX
  - NetBIOS over layer 2 (sometimes called NetBEUI)
  - Windows RAS (remote access services) protocols
- General:
  - Any protocol, program, or server that makes heavy use of broadcast.

Any program, protocol, server, or service not listed above that is judged to interfere with network operations, or that creates substantial risk of interference with network operations will result in their jack being disabled.

Chapter 8: Wireless Networking

Users are not permitted to set up or operate their own wireless systems on the Oakwood University campus. A wireless system has significant impacts on security and network operations. Only wireless systems installed and operated by the Technology Department are permitted. All those who are interested in setting up wireless access points must do so through the Technology Department using specified equipment. Users wishing to set up a wireless system should contact the Technology Department. Violation of this policy can result in the loss of all network privileges. ***Also see section 7.7 Banned programs and Utilities***

Chapter 9: VPN and Remote Connections

Use of a VPN (virtual private network) or any Remote Connection from off campus to any Oakwood University computer system must be authorized by the Information Technology Department. The Information Technology Dept. makes every effort to secure all network services. The user/s should be aware of the security risks when connecting remotely and take full responsibility of any security breech that may occur during a remote session. ***Also see section 7.7 (Network services and equipment)***

Chapter 10: Virus Protection

Faculty, Staff, and Students must have an Antivirus program installed on their system. A complete virus scan should be performed weekly. ***Also see section 3.2 Worms and Virus's***

Any violation of this policy or other applicable laws or policies can result in refusal or loss of network access privileges and/or disciplinary action.

Dorm Internet Access Policy

Revised: November, 14nd 2013

As a resident of Oakwood University Residence hall you have the privilege of connecting your privately owned personal computer to the Housing Residential Network (ResNET), so long as you agree to the following guidelines. Your use of ResNET is governed by state and federal laws and the Oakwood University Internet access policy.

Although the primary purpose of ResNET should be for activities which are academic in nature, you may use ResNET resources for recreational purposes so long as those activities do not violate any governing law or policy or impede the free use of campus network or ResNET resources by other users.

Your use of ResNET is considered a privilege not a right and can be revoked at any time. In order to receive and retain this privilege you are required to comply with the following and includes the afore mentioned **"Oakwood University Network Access Policy"**

Antivirus software

All Students are encouraged to have some form of antiviral software installed on their computer. It is in your best interest to keep the antiviral definitions for your antiviral software package up-to-date.

Windows updates

You must keep your system up-to-date with the latest security/vulnerability patches for your particular operating system.

IP Addressing

You may not configure your computer with any address other than one provided by Oakwood University. Connection to the Oakwood University network is restricted to DHCP issued addresses.

Personal Servers

You may not configure your computer as a network server of any kind without the express written permission of Oakwood University.

Switch's and Routers

You must not connect any devices such as switches, hubs, wireless access points, routers, Xbox or any other game oriented device to the network without the express written permission of the Oakwood University.

Applications and Protocols

You must not download or use any application or software that provides unauthorized network access or traffic. The use of any software which allows repeating, bridging (Internet Connection Sharing), routing, etc. is strictly prohibited.

NOTE: It is your responsibility to read your system and application documentation to prevent potential violations before software is used on the Oakwood University network.

For example, hosting a web site, hosting a gaming server, hosting a streaming video and/or audio server is prohibited.

Also, providing server services for DHCP/BOOTP, NAT, NTP, FTP, IRC and NFS is prohibited.

File and print sharing is allowed and limited to connections within the Housing facilities.

P2P File sharing software such as limeware, Imesh and alike is Strictly Prohibited by Oakwood University.

Hacking

You may not download or use any application used for eavesdropping (sniffers) or protocol analyzers.

Furthermore, the possession of such utilities on your computer shall be considered a violation of this policy.

Web Content

You may not use the internet to access, view or download any obscene material on your personal computer or any computers owned by Oakwood University. This includes but not limited to, pornography of any kind.

Oakwood University reserves the right to monitor and log any and all web pages that are being accessed by any employee or student of Oakwood University.

Operating Systems

You must be a licensed user of a supported operating system. Windows 98, 2000, XP, Vista, Linux, or Apple Are permitted.

Please follow these guidelines to reduce your own computer's vulnerability when connected to the network. With your cooperation and that of the other students in the residence halls we will be able to provide better network services for everyone.

Any violation of this policy or other applicable laws or policies can result in refusal or loss of ResNET access privileges and/or disciplinary action.

Oakwood University Email Usage Policy

I. INTRODUCTION

This Policy clarifies the applicability of law and of other Oakwood University policies to electronic mail. It also defines new policy and procedures where existing policies do not specifically address issues particular to the use of electronic mail.

Oakwood University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. Oakwood University affords electronic mail privacy protections comparable to that which it traditionally affords paper mail and telephone communications. This Policy reflects these firmly held principles within the context of the Oakwood University's legal and other obligations.

Cautions:

Users should be aware of the following:

1. Both the nature of electronic mail and the public character of Oakwood University's business (see Caution 2 below) make electronic mail less private than users may anticipate. For example, electronic mail intended for one person sometimes may be widely distributed because of the ease with which recipients can forward it to others. A reply to an electronic mail message posted on an electronic bulletin board or "listserver" intended only for the originator of the message may be distributed to all subscribers to the listserver. Furthermore, even after a user deletes an electronic mail record from a computer or electronic mail account it may persist on backup facilities. Oakwood University cannot routinely protect users against such eventualities.

2. Electronic mail, whether or not created or stored on Oakwood University equipment, may constitute an Oakwood University record subject to disclosure under the Alabama Public Records Act or other laws, or as a result of litigation. However, the Oakwood University does not automatically comply with all requests for disclosure, but evaluates all such requests against the precise provisions of the Act, other laws concerning disclosure and privacy, or other applicable law.

Users of Oakwood University electronic mail services also should be aware that the Alabama Public Records Act and other similar laws jeopardize the ability of Oakwood University to guarantee complete protection of *personal* electronic mail resident on Oakwood University facilities**.**

The Alabama Public Records Act does not, in general, apply to students except in their capacity, if any, as employees or agents of Oakwood University. This exemption does not, however, exclude student email from other aspects of this Policy.

3. Oakwood University, in general, cannot and does not wish to be the arbiter of the contents of electronic mail. Neither can Oakwood University, in general, protect users from receiving electronic mail they may find offensive. Members of the Oakwood University community, however, are strongly encouraged to use the same personal and professional courtesies and considerations in electronic mail as they would in other forms of communication.

4. There is no guarantee, unless "authenticated" mail systems are in use, that electronic mail received was in fact sent by the purported sender, since it is relatively straightforward, although a violation of this Policy, for senders to disguise their identity. Furthermore, electronic mail that is forwarded may also be modified. Authentication technology is not widely and systematically in use at Oakwood University as of the date of this Policy. As with print documents, in case of doubt receivers of electronic mail messages should check with the purported sender to validate authorship or authenticity.

5. Encryption of electronic mail is another emerging technology that is not in widespread use as of the date of this Policy. This technology enables the encoding of electronic mail so that for all practical purposes it cannot be read by anyone who does not possess the right key. The answers to questions raised by the growing use of these technologies are not now sufficiently understood to warrant the formulation of Oakwood University policy at this time. Users and operators of electronic mail facilities should be aware, however, that these technologies will become generally available and probably will be increasingly used by members of the community.

II. PURPOSE

The purpose of this Policy is to assure that:

A. Oakwood University community is informed about the applicability of policies and laws to electronic mail;
B. Electronic mail services are used in compliance with those policies and laws;
C. Users of electronic mail services are informed about how concepts of privacy and security apply to electronic mail; and
D. Disruptions to Oakwood University electronic mail and other services and activities are minimized.

III. DEFINITIONS

The terms "electronic mail" and "email" are used interchangeably throughout this Policy.

IV. SCOPE

This Policy applies to:

- All electronic mail systems and services provided or owned by the Oakwood University; and
- All users, holders, and uses of Oakwood University email services; and
- All Oakwood University email records in the possession of Oakwood University employees or other email users of electronic mail services provided by Oakwood University.

This Policy applies only to electronic mail in its electronic form. The Policy does not apply to printed copies of electronic mail. Other Oakwood University records management, however, do not distinguish among the media in which records are generated or stored. Electronic mail messages, therefore, in either their electronic or printed forms, are subject to those other policies, including provisions of those policies regarding retention and disclosure.

This Policy applies equally to transactional information (such as email headers, summaries, addresses, and addressees) associated with email records as it does to the contents of those records.

This Policy is effective immediately.

V. GENERAL PROVISIONS

As noted in the Introduction, Oakwood University recognizes that principles of academic freedom, freedom of speech, and privacy of information hold important implications for electronic mail and electronic mail services. This Policy reflects these firmly held principles within the context of Oakwood University's legal and other obligations.

A. Purpose.

In support of its threefold mission of instruction, research, and public service, Oakwood University encourages the use of Oakwood University electronic mail services to share information, to improve communication, and to exchange ideas.

B. Oakwood University Property.

Oakwood University electronic mail systems and services are Oakwood University facilities as that term is used in other policies and guidelines. Any electronic mail address or account associated with Oakwood University, or any sub-unit of Oakwood University, assigned by Oakwood University to individuals, sub-units, or functions of Oakwood University, is the property of The Regents of Oakwood University.

C. Service Restrictions.

Those who use Oakwood University electronic mail services are expected to do so responsibly, that is, to comply with state and federal laws, with this and other policies and procedures of Oakwood University, and with normal standards of professional and personal courtesy and conduct. Access to Oakwood University electronic mail services, when provided, is a privilege that may be wholly or partially restricted by Oakwood University without prior notice and without the consent of the email user when required by and consistent with law, when there is substantiated reason to believe that violations of policy or law have taken place, or, in exceptional cases, when required to meet time-dependent, critical operational needs. Such restriction is subject to established campus-wide procedures or, in the absence of such procedures, to the approval of the appropriate *Oakwood University Vice President*.

D. Consent and Compliance.

An email holder's consent shall be sought by Oakwood University prior to any inspection, monitoring, or disclosure of Oakwood University email records in the holder's possession, Oakwood University employees are, however, expected to comply with Oakwood University requests for copies of email records in their possession that pertain to the administrative business of Oakwood University, or whose disclosure is required to comply with applicable laws, regardless of whether such records reside on a computer housed or owned by Oakwood University .

E. Restrictions on Access Without Consent.

Oakwood University shall only permit the inspection, monitoring, or disclosure of electronic mail without the consent of the holder of such email (i) when required by and consistent with law; (ii) when there is substantiated reason to believe that violations of law or of Oakwood University policies have taken place; (iii) when there are compelling circumstances; or (iv) under time-dependent, critical operational circumstances.

When the contents of email must be inspected, monitored, or disclosed without the holder's consent, the following shall apply:

1. *Authorization*.

Except in emergency circumstances, and pursuant to Paragraph V.E.2, the responsible Oakwood University Vice President must authorize such actions in advance and in writing. This authority may not be further re-delegated. Requests for such non-consensual access must be submitted in writing following procedures to be defined by each campus. Oakwood University counsel's advice shall be sought prior to authorization because of changing interpretations by the courts of laws affecting the privacy of electronic mail, and because of potential conflicts among different applicable laws. Where the inspection, monitoring, or disclosure of email held by faculty is involved, the advice of the Campus Academic Senate shall be sought in writing in advance, following procedures to be established by each campus. All such advice shall be given in a timely manner. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

2. *Emergency Circumstances*.

In emergency circumstances, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures. If the action taken is not subsequently authorized, the responsible authority shall seek to have the situation restored as closely as possible to that which existed before action was taken.

3. *Notification*.

In either case, the responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with other Oakwood University policy, notify the affected individual of the action(s) taken and the reasons for the action(s) taken. Each campus will publish, where consistent with law, an annual report summarizing instances of authorized or emergency non-consensual access pursuant to the provisions of this Section.

4. *Compliance with Law*.

Actions taken under Paragraphs 1. and 2. Shall be in full compliance with the law and other applicable Oakwood University policy. This has particular significance for email residing on computers not owned or housed by Oakwood University. Advice of counsel always must be sought prior to any action taken under such circumstances. It also has particular significance for email whose content is protected under the Federal Family Educational Rights and Privacy Act of 1974, which applies equally to email as it does to print records.

5. *Recourse*.

Procedures for the review and appeal of actions taken under Sections V. C, D, and E and under Section VII shall be implemented (or existing procedures adapted) by each campus to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of Oakwood University were in violation of this Policy.

6. *Misuse*.

In general, both law and Oakwood University policy prohibit the theft or other abuse of computing resources. Such prohibitions apply to electronic mail services and include (but are not limited to) unauthorized entry, use, transfer, and tampering with the accounts and files of others, and interference with the work of others and with other computing facilities. Under certain circumstances, the law contains provisions for felony offenses. Users of electronic mail are encouraged to familiarize themselves with these laws and policies.

VI. SPECIFIC PROVISIONS

A. Allowable Use

In general, use of Oakwood University electronic mail services is governed by policies that apply to the use of all Oakwood University facilities. In particular, use of Oakwood University electronic mail services is encouraged and is allowable subject to the following conditions:

1. *Purpose*.

Electronic mail services are to be provided by Oakwood University organizational units in support of the teaching, research, and public service mission of Oakwood University, and the administrative functions that support this mission.

2. *Users*.

Users of Oakwood University electronic mail services are to be limited primarily to Oakwood University students, faculty, and staff for purposes that conform to the requirements of this Section.

3. *Non-Competition*.

Oakwood University electronic mail services shall not be provided in competition with commercial services to individuals or organizations outside Oakwood University.

4. *Restrictions*.

Oakwood University electronic mail services may not be used for: unlawful activities; commercial purposes not under the auspices of Oakwood University; personal financial gain (see applicable academic personnel policies); personal use inconsistent with Section VI. A. 8; or uses that violate other Oakwood University policies or guidelines. The latter include, but are not limited to, policies and guidelines regarding intellectual property, or regarding sexual or other forms of harassment.

5. *Representation*.

Electronic mail users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of Oakwood University or any unit of Oakwood University unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer shall be included unless it is clear from the context that the author is not representing Oakwood University. An appropriate disclaimer is: "These statements are my own, not those of Oakwood University."

6. *False Identity*.

Oakwood University email users shall not employ a false identity. Email may, however, be sent anonymously provided this does not violate any law or this or any other Oakwood University policy, and does not unreasonably interfere with the administrative business of Oakwood University.

7. *Interference*.

Oakwood University email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on any computing facilities, or unwarranted or unsolicited interference with others' use of email or email systems. Such uses include, but are not limited to, the use of email services to: (i) send or forward email chain letters; (ii) "spam," that is, to exploit listservers or similar broadcast systems for purposes beyond their intended

scope to amplify the widespread distribution of unsolicited email; and (iii) "letter-bomb," that is, to resend the same email repeatedly to one or more recipients to interfere with the recipient's use of email.

8. *Personal Use*.

Oakwood University electronic mail services may be used for incidental personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not:

(i) directly or indirectly interfere with Oakwood University operation of computing facilities or electronic mail services

ii) burden Oakwood University with noticeable incremental cost; or

(iii) interfere with the email user's employment or other obligations to Oakwood University. Email records arising from such personal use may, however, be subject to the presumption of an Oakwood University Email Record, regarding personal and other email records. Email users should assess the implications of this presumption in their decision to use Oakwood University electronic mail services for personal purposes.

B. Security and Confidentiality

1. The confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, including this Policy, by unintended redistribution, or because of inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using email to communicate confidential or sensitive matters.

2. Business and Finance, *Legal Requirements on Privacy of and Access to Information*, prohibits Oakwood University employees and others from "seeking out, using, or disclosing" without authorization "personal or confidential" information, and requires employees to take necessary precautions to protect the confidentiality of personal or confidential information encountered in the performance of their duties or otherwise. This prohibition applies to email records. In this Policy the terms "inspect, monitor, or disclose" are used within the meaning of "seek, use, or disclose".

3. Notwithstanding the previous paragraph, users should be aware that, during the performance of their duties, network and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of Oakwood University email services, and on these and other occasions may inadvertently see the contents of email messages. Except as provided elsewhere in this Policy, they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect email when re-routing or disposing of otherwise undeliverable email. This exception is limited to the least invasive level of inspection required to perform such duties. Furthermore, this exception does not exempt postmasters from the prohibition against disclosure of personal and confidential information of the previous paragraph, except insofar as such disclosure equates with good faith attempts to route the otherwise undeliverable email to the intended recipient. Re-routed mail normally should be accompanied by notification to the recipient that the email has been inspected for such purposes.

4. Oakwood University attempts to provide secure and reliable email services. Operators of Oakwood University electronic mail services are expected to follow sound professional practices in providing for the security of electronic mail records, data, application programs, and system programs under their jurisdiction. Since such professional practices and protections are not foolproof, however, the security and confidentiality of electronic mail cannot be guaranteed. Furthermore, operators of email services have no control over the security of email that has been downloaded to a user's computer. As a deterrent to potential intruders and to misuse of email, email users should employ whatever protections (such as passwords) are available to them.

5. Users of electronic mail services should be aware that even though the sender and recipient have discarded their copies of an electronic mail record, there might be back-up copies that can be retrieved. Systems may be "backed-up" on a routine or occasional basis to protect system reliability and integrity, and to prevent potential loss of data. The back-up process results in the copying of data onto storage media that may be retained for periods of time and in locations unknown to the originator or recipient of electronic mail. The practice and frequency of back-ups and the retention of back-up copies of email vary from system to system. Electronic mail users are encouraged to request information on the back-up practices followed by the operators of Oakwood University electronic mail services, and such operators are required to provide such information upon request.

C. Archiving and Retention

Oakwood University records management policies do not distinguish among media with regard to the definition of Oakwood University records. As such, electronic mail records are subject to these policies. In particular, such records are subject to disposition schedules in the Oakwood Records Disposition Schedules Manual, which distinguishes among different categories of records, from the ephemeral to the archival.

Oakwood University does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up (see Section VI. B. 5), if at all, only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may at times serve the latter purpose incidentally. Operators of Oakwood University electronic mail services are not required by this Policy to retrieve email from such back-up facilities upon the holder's request, although on occasion they may do so as a courtesy.

Email users should be aware that generally it is not possible to assure the longevity of electronic mail records for record-keeping purposes, in part because of the difficulty of guaranteeing that electronic mail can continue to be read in the face of changing formats and technologies and in part because of the changing nature of electronic mail systems. This becomes increasingly difficult as electronic mail encompasses more digital forms; such as embracing compound documents composed of digital voice, music, image, and video in addition to text. Furthermore, in the absence of the use of authentication systems (see Section I, Caution 4), it is difficult to guarantee that email documents have not been altered, intentionally or inadvertently.

Email users and those in possession of Oakwood University records in the form of electronic mail are cautioned, therefore, to be prudent in their reliance on electronic mail for purposes of maintaining a lasting record. Sound business practice suggests that consideration be given to transferring (if possible) electronic mail to a more lasting medium/format, such as acid-free paper or microfilm, where long-term accessibility is an issue.

VII. POLICY VIOLATIONS

Violations of Oakwood University policies governing the use of Oakwood University electronic mail services may result in restriction of access to Oakwood University information technology resources. In addition, disciplinary action, up to and including dismissal, may be applicable under other Oakwood University policies, guidelines, implementing procedures, or collective bargaining agreements.