University of Northwestern Ohio
Technology Usage and Ethics Policy
April 1, 2014

General Statement

The University of Northwestern Ohio provides computer and telephony hardware, software and systems for the use of faculty, staff and students. This document constitutes a University-wide policy for the appropriate use of all University computing, telephony, and network resources. These resources are provided for the purposes of furthering the University's academic and institutional goals. Access and usage of computing technology places a responsibility on each authorized person to conduct computing business in an ethical manner.

These guidelines are intended to supplement, not replace, all existing laws, regulations, agreements, and contracts that currently apply to those resources. Access to computer systems is granted subject to University policies and local, state, and federal laws. Appropriate use should always be legal and ethical, reflect academic honesty and community standards, and exhibit restraint in the consumption of shared resources.

The University will take appropriate disciplinary action against any employee or student who violates this policy. Conduct in violation of the principles set forth in this policy, with respect to the use of all information services and facilities available through the University, may also be subject to criminal or legal action.

Applicability

This policy applies to all users of University computing and telephony resources, and to all uses of those resources. Additional policies may apply to specific computers, computers systems, or networks provided or operation by specific departments of the University. Consult with the operators or managers of the specific computer, computer system, or network in which you are interested or with the Vice President of the Information Technology Department if in doubt of allowed usage.

Appropriate Use

Appropriate use of information technology resources includes instruction, independent study, and official work of the offices of the University. Authorized users are: (1) faculty, staff, and students of the University; (2) anyone connecting from a public information service; (3) others whose access furthers the mission of the University and whose usage does not interfere with other users' access to resources. Any misuse or violation of the University's information-technology environment will be judged in accordance with those

published policies and rules of conduct, including, but not limited to, the Student code of conduct, the Faculty Handbook, and the Employee Handbook.

It is your responsibility to be aware of the potential for, and possible effects of manipulating information, especially in electronic form, to understand the changeable nature of electronically stored information, and to continuously verify the integrity and completeness of information that you compile or use. You are responsible for the security and integrity of University information stored on your individual computing desktop system.

Account Access Password

In accordance with the University's goal of maintaining a secure computing environment, all users are required to have passwords that meet the following guidelines:

- Must be a minimum of 8 characters in length
- Must contain characters from at least 3 of the following 4 categories:
    - English uppercase letters
    - English lowercase letters
    - Numbers from 0-9
    - Non-alphanumeric symbols or punctuation (such as @, #, $, or !)
- Must be changed at least once every 3 months
- Cannot be the same as any of the previous 3 passwords
- Password cannot contain your name (first or last) or username

Passwords can be changed several ways. The methods vary depending on whether you are on campus or off campus.

If you are on campus:

- Log into one of the University computers and press Ctrl+Alt+Delete. Select the Change Password… button and enter in your new password.
- If you cannot remember your password, visit one of the password reset computers located around the campus and reset your password there.

If you are off campus, one of these methods may be used:

- Log into go.unoh.edu. Select the Change Password link and enter your new password.
- If you cannot remember your password, or if your password has expired, click the Forgot my password link on the front page of the go.unoh.edu website and reset your password.

E-mailbox Size

UNOH faculty, staff, and students are given a very generous mailbox size of 25Gb in order to communicate with one another and the student body. Please make every effort to maintain your mailbox to keep it from overfilling. Messages that are received by the server destined to a mailbox that is full may be rejected with no notice given. Mailbox sizes will not be increased.

E-mail Attachments

The maximum attachment size for any one e-mail message is limited to 25Mb outbound and 25Mb inbound. If you have an attachment larger than this, you will need to use another mechanism with which to send or retrieve it.

E-mail Viruses

Be aware that viruses are spread through e-mail attachments. For that reason, your e-mail will be scanned for viruses before ever being placed into your mailbox. If you receive an e-mail with an embedded virus or an infected attachment from someone, it will not be put into your mailbox for retrieval. Instead, you will receive a message comprising those parts of the original message that are deliverable virus free along with an appended explanation so that you are aware of the occurrence.

Any individual who knowingly propagates an e-mail virus is in violation of the *Technology Usage and Ethics Policy* and may have actions taken against them per this document.

Spam Removal

The University employs a system that screens all inbound e-mail from outside of the campus domain. This does not happen to any e-mail that remains within the confines of our own e-mail system. Any inbound e-mail that is overtly considered to be spam will not be placed into University e-mail accounts. E-mail that is suspect but cannot be positively identified as spam will be delivered to the destination e-mailbox and placed in the “Junk E-mail” folder. All other e-mail, whether spam or legitimate, will be placed as usual into the destination e-mailbox.

Peer-to-Peer Networking

The University employs a packet shaper appliance that controls the flow of bandwidth both across the internal network and in and out of the gateway to the Internet. This system also allows for the control of all network protocols that can be used for inter-computer communications. One such protocol called peer-to-peer networking has been entirely disabled on the UNOH network in addition to that which is destined to and from the Internet. The University has chosen to use this method of network traffic control in

order to comply with the provisions of the Higher Education Act Reauthorization of 2008 and the Digital Millennium Copyright Act of 1998.

Telephone and Voice Messaging

The telephone and voice messaging systems transmit digital voice data in addition to storing digital recordings of voice communications. These systems are computer and storage systems that are also attached to the University network. They are regarded by the University as a telephony system that falls under this same usage and ethics policy as would any other electronic messaging system.

Software Updates

As software publishers provide software and security updates to the many applications that are installed on campus computer systems, they may be published to the computers with, or without, prior notice. Many of these updates are necessary in order to maintain the integrity and availability of each computer on the campus network. Whenever possible, everyone will be notified in advance if the updates to their computers will have an impact on their daily activities.

Remote Assistance

Members of the Information Technology department may at times provide remote assistance support to end users through the network rather than traveling to the user's office. Most problems can be resolved quickly and easily with this method of support from a remote location. At the user's request, members of the Information Technology department may remotely interact with the user's computer in order to solve computing issues. Remote assistance support will be provided if (a) the user has made a request to the Information Technology department for remote assistance; (b) the user has authorized a member of the department to interact with their workstation; (c) the issue is related to the user's responsibilities at the University; (d) the equipment is supported by the University.

Software Installation

The University of Northwestern Ohio at times provides its employees with software installation media and licenses for installation onto their home PCs as may be required by their job functions. These licenses are purchased by the University and remain the sole property of the University. Transfer of these licenses to any other individual without the express written permission of the University is not permitted. The employee is entrusted with these licenses with the understanding that these are the property of the University. If the employee moves into a new job function that no longer requires the use of these licenses or upon termination of employment from the University, the software must be removed from the system upon which it was installed.

Software Installation Disclaimer

The University does not in any way warrant the suitability of the software for installation onto the employee's personal property. It is up to the employee to verify that the system to receive the software meets the recommended specifications for the software to run as expected. The University is also not liable for any damage caused to the employee's personal property, either the operating system or the currently installed applications, stemming from the installation of the software.

Attaching Personal Property to the University Network

The University understands that at times, employees may wish to attach their own personal electronic devices (such as laptops and tablets) to its network in order to perform some elements of their job. This usage is encouraged as this benefits both the employees and the University in the achievement of our goals to better serve our students. However, the employee must adhere to the following policies before the device is attached to the network. Following these policies protects both the University's network as well as protects the employee's device from unintentional damage.

- The University will ask that the employee sign and comply with the Software Installation Policy. The employee should adhere to the Software Installation and Software Installation Disclaimer policies cited above for these personal devices. This form is available on the University web site.
- The University requires that the latest versions of Antivirus software and virus signatures be loaded onto any device connecting to its network. The University will provide a license to any employee who will be attaching their personal device to the network. This software will assure ongoing protection with no lapse in the subscriptions. This is a small cost considering the exposure that might otherwise occur.
- The device must be submitted to the Information Technology Department where it will be certified for use on the University network. In order to certify the device, they will apply the latest software updates and security patches supplied by the vendor of the operating system. They will also install the virus protection software and will do the initial virus scans. If the employee does not submit the device to this process or the device will not successfully install this software, then the employee will be prohibited from attaching the device to the University network.
- Once the device is certified by someone in the Information Technology Department, the employee may attach it to the network. The employee should regularly attach the device to the network from that point forward so that all security updates that may have accumulated since the last attachment can be made at that time. Timely updates create more secure systems and will minimize security threats.
- Any software or files of a personal nature that others might consider to be objectionable must be removed from the device before it is used on the University campus. Even though the device may be personal property, whatever programs or material that may be installed could potentially be viewed by other faculty, staff or

students in the course of performing their jobs. Therefore, all of the Technology Usage and Ethics Policy contained herein apply to these personal devices as well.

- The Information Technology Department will only provide support services that would include the software that was installed by IT. The IT staff should only be expected to make the software work with a reasonable effort. If reasonable attempts fail, the device will not be certified and will therefore be prohibited from attaching to the University network.
- The Information Technology Department cannot provide support for software that may have already been loaded onto the device that was purchased and installed for the employee's own personal use.
- The IT staff cannot provide support for software that is installed at a later date unless that software installation damages the antivirus software's functionality. In this case, a reasonable effort will be made to remedy the problem in order to make it functional again. If the software cannot be made functional again, the device will no longer be certified for use on the University network and should not be attached thereafter.

Security and Privacy

Authorized access to data or information entails both privilege and responsibility, not only from the user, but also for the system administrator. In general, the University will treat information stored on computers as confidential. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment. Users should therefore engage in "safe computing" practices by establishing appropriate access restriction for their accounts, guarding their passwords and access codes, and changing them regularly.

Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual login sessions and communication, without notice, when (a) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of University of other computing resources or to protect the University from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this policy; (d) an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) it is otherwise required or permitted by law, or necessary to respond to perceived emergency situation, must be authorized in advance by the Vice President for Information Technology under the direction of the President or the Vice President for Academic Affairs/Provost.

The University, at its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communication, to appropriate

University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings.

Additionally, electronic mail, voice mail, and other data stored on the University's network of computers may be accessed by the University for the following purposes (a) troubleshooting hardware and software problems; (b) preventing unauthorized access and system misuse; (c) retrieving business-related information; (d) investigating reports of violation of this policy or local, state or federal law*****; (e) complying with legal requests for information*****; (f) rerouting or disposing of undeliverable mail.

> *****The network administrators or authorized designees will need specific approval from the President or the Vice President for Academic Affairs/Provost or an appropriate designee to access these items. The extent of the access will be limited to what is essentially necessary to acquire the information.

To the greatest extent possible in a public setting, individuals' privacy should be preserved. However, privacy or confidentiality of documents and messages stored on University-owned equipment cannot be guaranteed. Users of electronic mail and messaging systems should be aware that, in addition to being subject to authorized access, these communications in their present form cannot be secured and are, therefore, vulnerable to unauthorized access and modification by third parties.

Policy

All users of University computing resources must:

- **Comply with all federal, Ohio, and other applicable law; all generally applicable University rules and policies; and all applicable contracts and licenses.** Examples of such laws, rules, policies, contracts, and licenses include the laws of libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking," "cracking," and similar activities; the University's code of student conduct; the University's sexual harassment policy; and all applicable software licenses. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware that they may also be subject to the laws of those other states and countries and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses.
- **Use only those computing resources that they are authorized to use and use them only in the manner and to the extent authorized.** Ability to access computing resources does not, by itself, imply authorization to do so. Users are responsible for ascertaining what authorizations are necessary and for obtaining them before proceeding. Accounts and passwords may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the University.
- **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** Again, ability to access other persons' accounts does not, by itself, imply authorization to do so. Users are responsible for

ascertaining what authorizations are necessary and for obtaining them before proceeding.

- **Respect the finite capacity of those resources and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.** Although there is no set bandwidth, disk space, CPU time, or other limit applicable to all uses of University computing resources, the University may require users of those resources to limit or refrain from specific uses in accordance with this principle. The reasonableness of any particular use will be judged in the context of all of the relevant circumstances.
- **Refrain from using those resources for personal commercial purposes or for personal financial or other gain.** Personal use of University computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other University responsibilities, and is otherwise in compliance with this policy. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.
- **Refrain from stating or implying that they speak on behalf of the University and from using University trademarks and logos without authorization to do so.** Affiliation with the University does not, by itself, imply authorization to speak on behalf of the University. Authorization to use University trademarks and logos on University computing resources may be granted only by the President or Vice President for Academic Affairs/Provost.

Examples of Prohibited Use

Use of the University of Northwestern Ohio's network and computer systems are conditioned upon compliance with this and other University policies and all applicable laws. Though not exhaustive, the following list is provided to emphasize that these activities are not allowed on the University's networks or computer systems:

- Unauthorized use of facilities, accounts, access codes, privileges and information.
- Viewing, listening, copying, altering, or destroying anyone's files or recordings without explicit permission from that individual.
- Using the University's computers, telephony, network facilities, information services or resources in the commission of a crime.
- Representing one's self electronically as another user.
- Unlawfully harassing others.
- Creating and/or forwarding chain letters.
- Posting or mailing obscene materials.
- Game playing by anyone that interferes with business and academic use of network resources by others.
- Streaming of movies, television, or other video and audio content that interferes with business and academic use of network resources by others.
- Making, distributing, or using unauthorized copies of licensed software.

- Unauthorized copying, reproducing, or redistributing others' text, photos, sound, video graphics designs or other information formats.
- Unauthorized downloading and/or distributing copyrighted material.
- Introducing destructive software e.g., "virus" software or attempting system crashes.
- Configuring software or hardware to intentionally allow access by unauthorized users.
- Attempting to circumvent or subvert any system's security measures.
- Advertising for commercial gain.
- Distributing unsolicited advertising.
- Disrupting services, damaging files or intentionally damaging or destroying equipment, software, or data belonging to the University or others.
- Using computing resources for unauthorized monitoring of electronic communications.
- Creating and/or posting material that is publicly accessible that is not specifically sanctioned by the Vice President for Information Technology, the Vice President for Academic Affairs/Provost, or the President.

Remember, your surfing habits can be monitored and stored in a centralized database for misuse reporting. In case of doubt, users bear the burden of responsibility to inquire concerning the permissibility of external network uses prior to execution. Such questions should be directed to the Network Administrator or the Vice President for Information Technology.

Reporting Violations

All users and departments should report any discovered unauthorized access attempts or other improper usage of University computers, networks, or other information processing equipment. If you observe, or have reported to you, a security or abuse problem, with any University computer or networked facilities, including violations of this policy, you should notify the Vice President of the Information Technology Department or the Vice President for Academic Affairs/Provost.

Enforcement

Users who violate this policy may be denied access to University computing and telephony resources and may be subject to other penalties and disciplinary action, both within and outside of the University. Violations will normally be handled through the University disciplinary procedures applicable to the relevant user. However, the University may temporarily suspend or block access to an account, while investigating alleged misuse, and when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability. The University may also refer suspected violation of applicable law to appropriate law enforcement agencies.