Technology Usage and Ethics Policy

June 14, 2024

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 operated 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.

User Accounts

The University provides user accounts to employees and students for the purpose of accessing online services and communication systems. Each person is responsible for the protection and appropriate use of their University credentials. Password length, complexity, and expiration requirements are applied to each user account. Users may change their passwords from a campus computer or by using the online password change and reset tools. Student user accounts will be deleted one year beyond their most recent term of attendance. Employee accounts will be disabled immediately upon separation.

Multi-factor Authentication

All University accounts are protected using both passwords (something you know) and a second factor (something you have) in order to complete the authentication process. The second factor may be a registered app on a smartphone, authentication code in a text message, or a security token. Both factors (2FA) are required to log into University systems making it very difficult for others to break into University accounts. All University students, employees, and trusted service providers are required to use MFA in some form to protect these accounts.

E-mail Services

UNOH faculty, staff, and students are provided a University e-mail address along with generous mailbox storage capacity to communicate with one another and the student body. Please make every effort to maintain your mailbox to keep it from overfilling. Messages destined for a mailbox that is full may be rejected without notice. Mailbox sizes will not be increased.

The University e-mail platform includes built-in limitations to discourage misuse. These limitations include blocking transmission of sensitive data to external systems, the maximum number of individual e-mail recipients per day, and the maximum size of e-mail attachments. If you need to transmit messages in type, volume, or size that exceeds these limitations, an alternate information system designed for such electronic communication should be used so long as the alternate system includes security measures that are appropriate for the data being transmitted.

Automated protection measures have been applied to University e-mail systems to ensure these systems remain safe and efficient. Inbound and outbound email messages and attachments are scanned for viruses and spam and will be blocked if such characteristics are detected. Inbound spam messages will be blocked without recipient notification. Messages that are suspected spam, but cannot be positively identified, will be delivered to the recipients "Junk Email" folder. In cases where an outbound message violates a system policy, a notification message will be sent to the originating mailbox describing the reason for the blocked message.

Any individual who knowingly attempts to circumvent University e-mail protections, or transmit viruses or spam messages, is in violation of the *Technology Usage and Ethics Policy* and may have actions taken against them per this document.

File Storage

Students and employees are provided file storage to save homework, coursework, and conduct other University business. University-managed file storage systems are accessed using your UNOH credentials and should be used when storing or working with documents related to University business. Third-party providers should never be used to store or transmit confidential personal data and is a violation of the *Technology Usage and Ethics Policy*.

Peer-to-Peer Networking

The University employs a packet shaping 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.

University Computing Disclaimer

University-managed services and devices will present a disclaimer to users attempting to log on. This disclaimer serves as a regular reminder of users' obligations according to the Technology Usage and Ethics Policy. The following is an example of a disclaimer applied to campus computers:

This computer system is the property of the University of Northwestern Ohio. It is for authorized use only. Users have no explicit or implicit expectation of privacy. By using this system, all users acknowledge notice of, and agree to comply with, the University's Technology Usage and Ethics Policy. Unauthorized or improper use of this system may result in administrative disciplinary action, civil charges/criminal penalties, and/or other sanctions as set forth in the University's Technology Usage and Ethics Policy. The University of Northwestern Ohio reserves the right to monitor use of this network to ensure network security and to respond to specific allegations of misuse. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

Software Installation

The University of Northwestern Ohio at times provides its employees with software installation media and licenses for installation onto their personal computing devices 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.

Wi-Fi (wireless) System

The University has deployed a Wi-Fi system (the eduroam SSID) that covers all of the academic buildings on campus as well as designated parking areas. This wireless system is encrypted and requires a UNOH e-mail address and password in order to gain access to it. Once authenticated, the system allows users to seamlessly roam from building to building without having to authenticate at each location. Although the wireless traffic is encrypted, UNOH does not warrant or guarantee that user data is completely safe from exposure while in use as there are ways in which this security scheme can be circumvented outside of what is detectable by UNOH systems. Therefore, while on campus, do not connect to any other named Wi-Fi system other than the university supported "eduroam" SSID.

UNOH requires that all traffic flowing over the Wi-Fi system and the wired networks be traceable to an individual user should there be any issues arising from illegal or unethical use. All Wi-Fi usage falls under the Technology Usage and Ethics policies so is therefore filtered to exclude objectionable and illegal content. As with all network traffic, UNOH maintains log files of Wi-Fi usage should illegal or unethical usage warrant an investigation.

The majority of modern portable devices such as laptops, smartphones, and tablets support encrypted Wi-Fi communications, which is required in order to use eduroam. Those devices that cannot connect accordingly will not be supported. Please visit https://support.unoh.edu for instructions on how to configure and connect to eduroam. In some cases, special software or configurations may need to be downloaded onto the device in order to complete the connection to eduroam. If the user does not agree to allow this software to configure the encrypted channel, the device will not connect and will not be supported. Once connected to eduroam, users may move freely from building to building on the UNOH campus in addition to the thousands of other university and college campuses around the world that also offer the eduroam service.

UNOH also provides the guess access SSID called "UNOH Guest". Attaching to this Wi-Fi system grants the user 24 hours use of the Wi-Fi system but the guest must complete the registration process before access is granted. All use of UNOH Guest falls under the Technology Usage and Ethics policies.

Users should be aware that Wi-Fi bandwidth is a shared resource so usage is managed and rate limited in order to ensure all users have an equal and good experience. Users should also be aware that the Wi-Fi access points have been deployed to provide coverage based upon normal populations for each area. This means that from time to time, certain exceptional situations where an abnormally high number of users have congregated, bandwidth needs may exceed capacity and performance may degrade.

The Wi-Fi system utilizes unlicensed frequencies in the 2.4/5GHz radio bands. The construction materials of buildings, the surrounding environment, other wireless devices, and the user's distance from the access point influences the quality and strength of the Wi-Fi signal. This means that performance may degrade due to possible disruptions caused by items such operating microwave ovens, florescent lighting, cordless phones, other wireless devices, and unapproved access points. If such devices are found to be disrupting the normal operations of the UNOH Wi-Fi system, users may be required to remove or turn off the offending devices or be expected to understand that some situations just cannot be remedied.

UNOH does not guarantee, real or implied, the data rates, security, or quality of this service. However, if a problem is detected, IT staff will work to resolve the issue in order to restore the service to an operational condition.

Virtual Private Network (VPN)

Employees and trusted service providers may request access to the University network via a virtual private network (VPN) connection. The VPN software creates a secure tunnel between the remote device and the UNOH campus network. This tunnel means that a hole is opened in the security mechanisms that protect network resources so that you may work from a remote location as if on campus. The VPN grants access to all University services and servers that the user is normally permitted to use while on campus. Therefore, access and use of the VPN is authorized on a case-by-case basis and must be approved by department heads in coordination with IT using this request form. Please adhere to the following:

- Users may unknowingly have viruses and such on their home computers and other devices that can traverse the UNOH network through a VPN connection. For this reason, the use of the VPN is restricted to only University supplied laptops and it must not be installed onto personal computers. Therefore, IT will not install the VPN software, or other university software onto personal laptops. Please be diligent in keeping computers and other devices within your home, or other off-campus work locations, up to date with the latest software and security updates.
- Copying large files to/from University systems may clog the connection. Therefore, large volume transfers of data should be avoided whenever possible. For example, transferring large files to and from the P: drive or print previews of very large reports coming from the administrative systems.

- IT cannot provide users with after-hours support to set up and/or diagnose their VPN problems over their home Internet connections. Internet service providers and equipment vary considerably making it difficult to do so.
- IT cannot provide users with after-hours support if they run into processing issues. This is especially true should the VPN connection drop during a process run. Please consult with IT about best practices when attempting to run large batch processes using the administrative systems.
- Users are still required to abide by the Technology Usage and Ethics Policy while using the VPN connection for University business regardless of where that activity originates.

Attaching Personal Devices to the University Network

The University understands that at times, employees may wish to attach their own personal electronic devices (such as laptops, smartphones, and tablets) to the campus 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 requires that the latest versions of Antivirus software and virus signatures be loaded onto any device connecting to its network as well as the latest updates to the host operating systems provided by the software vendors. The most recent versions of software contain the latest security patches that protect both the personal device as well as the University infrastructure.
- Any software or files of a personal/sensitive nature that others might consider to be objectionable should 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 applies to these personal devices as well.
- The Information Technology Department will only provide support services for software that was installed by IT. The IT staff should only be expected to make the software work with a reasonable effort.
- 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.

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, such as by posting to social media 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.
- Unauthorized sharing, storing, or posting of confidential information on systems not managed by the University.
- 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, storing, 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 for Information Technology 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.