Computer Use Policy

Approved by the Ohio Wesleyan University Faculty: March 24, 2014

I. Introduction

Ohio Wesleyan University (OWU) provides computing resources to support the educational mission and administration of the University. The University also serves as a technology resources for the local community of OWU students, faculty, and staff; the extended OWU community, including alumni and emeriti faculty and staff; and campus visitors and guests. Information Services provides and maintains the public computing infrastructure, such as the network, servers, and computer laboratories. These resources are critical for the academic, administrative, and research needs of the University community. All IS employees must sign a non-disclosure agreement upon employment. OWU community members, visitors, and guests (users) who utilize these resources are expected to comply with institutional policies as well as local, state, and federal laws and regulations. Each user will share the responsibility for safeguarding the University's computing environment. Fair, legal, and equitable use of the resources is essential for all users to maintain OWU's computing environment.

Technology environments can easily be disrupted, and digital information can effortlessly be duplicated and distributed. Responsible utilization of OWU's computing resources by users will ensure the integrity of these resources. The promotion of responsible use of the University's resources does not negate the value placed on individual privacy and intellectual property rights or the academic freedoms guaranteed by the University.

II. User Responsibilities

Access and Usage

A. User access to OWU computing resources is a privilege, and these resources are primarily for use by the immediate OWU community, such as students, faculty, and staff. Alumni, emeriti faculty, local community members, and campus visitors and guests may use public computing resources with the understanding that OWU faculty, staff, and students have priority over users engaged in non-scholarly, recreational activities such as game playing, personal Web surfing, and personal instant messaging.
B. Users are asked to be civil and respectful in all their electronic communications.
C. Users are asked to remember that he University provides access to computers and the Internet in support of its educational mission and University-related activities. Therefore, faculty, staff, and students should be mindful of how they use these resources for personal use.
D. With regard to public computing facilities, users are expected to respect other users as well as OWU staff. Verbal or physical abuse of others will not be tolerated. Excessive noise or other disruptive behavior – including cellular phone usage – is prohibited in public computing areas. Users should be able to properly identify themselves (i.e. OWU ID card) to OWU staff when asked.

E. Equipment abuse is unacceptable, and users are asked to report any mistreatment or vandalism of OWU computing resources to INFORMATION SERVICES staff (lower level of the Corns Building or 368-3210) or to Public Safety (ground floor of Smith Hall or 368-2222).
F. Only computing devices that have been properly registered with Information Services may be directly connected to the OWU network. Each authorized user is responsible for the registered devices' usage and activity originating from that device.
G. Installation of a personal network server, such as a web or file server, can compromise the integrity and security of the entire University network, and is therefore strongly discouraged. Such a server is permissible only for research or teaching purposes, and must be registered with Information Services to ensure system integrity. Information Services will provide guidelines for securing the server and service as well as for monitoring the system. In the case of an emergency, Information Services may terminate access to the server or service if the system has been compromised or improperly secured. Information Services will make every reasonable attempt to contact the server administrator prior to terminating service.

Network and Equipment Integrity

H. With regard to public lab computers, users shall not make any significant modifications to the condition or status of any computer equipment – including the alteration of critical system files, network, or peripheral connections. Installation of personal software or hardware on public lab computers is prohibited.
I. With regard to University-owned personal office, departmental, research, and teaching lab computers, users who make any significant modifications to the condition or status of any computer equipment, including the installation of hardware or software, the alteration of critical system files, network, or peripheral connections, are not entitled to, but may receive, Information Services technical support for these changes.
J. Due to the potentially crippling impact of malicious computer programs – including viruses, worms, and malware – on individual as well as shared computing resources, users who connect to any local or remote network are expected to keep their operating system and maintenance software (i.e., anti-virus and anti-spyware utilities) properly updated.

Data Security

K. Users are responsible for their own personal computer and OWU account activity and shall not allow others to use their personal accounts.
L. Users must protect and maintain the confidentiality of their passwords. Therefore, users should not share their passwords with others, and passwords should be changed frequently. Information Services recommends that you change your password once each semester.
M. Although Information Services performs regular backups of user data stored on network file servers, users ultimately are responsible for backing up their own local files and

directories. Users should make at least one physical backup copy (using a CD/DVD burner, zip drive, external hard drive, USB key, or other removable storage device) of important data on their computer systems on a consistent, ongoing basis.

Software Licensing

N. Proprietary software made available by Information Services may not be duplicated or redistributed. Users shall not alter proprietary software installed by Information Services on University-owned computers in any unlawful manner.
O. Users who install their own software must observe the software's licensing agreement.

Email

P. The University will send official communication via campus e-mail only. Students shall regularly check and maintain their OWU e-mail account. If they desire, students can automatically forward their OWU e-mail to their preferred account.
Q. Authorized users – including current students, faculty, and staff – may utilize the campus-wide electronic mail message distribution system. This system is checked throughout each business day the University is officially open. For more information, refer to the OWU Campus-Wide E-Mail Distribution Policy at http://helpdesk.owu.edu/Campus-wideGroupLists.

III. University Responsibilities

Network Access

A. Through its direct Internet connection and remotely accessible connections, OWU operates as an Internet Service Provider (ISP) for its users. This provides users will access to local (on-campus) and remote computing resources. Network access interruptions or outages may sometimes result from events outside the University's control.

Equipment Maintenance

B. Users are responsible for reporting problems and unusual behavior of computing equipment to Information Services. Although Information Services makes every reasonable effort to troubleshoot and resolve equipment issues in a timely fashion, it is not possible to guarantee that all issues will be resolved in a satisfactory manner due to actions or accidents beyond reasonable control. Users maintaining their own computing equipment are responsible for maintaining equipment in a secure condition that does not adversely affect the performance of the OWU network or other computers. Information Services will provide guidelines to facilitate these preventative measures.

Campus Server Access

C. Each OWU account is assigned storage space (quota) on one or more hard disk devices for saving and accessing files, including e-mail and Web content. Users may apply for

additional quota when necessary for academic or administrative activities by contacting Information Services.

Computer and Software Inventory and Remote Assistance

D. Each OWU-owned device will contain inventory management software to assist in managing and tracking hardware and software. Data will be collected and stored on a central server, including hardware information and installed software applications, to allow for accurate inventory reporting, analysis, computer life cycle, and license management. Remote assistance software will be configured to require user authorization prior to the remote session being granted. Users of the OWU owned device may opt out of the computer inventory system at their discretion.

IV. Acceptable and Unacceptable Use

A. Usage that violates any institutional, local, state, or federal rule, regulation, or law is prohibited.
    a. This includes but is not limited to unauthorized duplication or dissemination of copyrighted materials, including electronic text, graphic files, commercial software, and audio and video files (particularly in a peer-to-peer application environment, regardless of whether such activity is internal or external to the OWU campus).
    b. This includes but is not limited to interstate communications for illegal or fraudulent purposes; unauthorized access to or modification of information from national defense or financial systems; creation, possession, or distribution of graphic or computer graphic depictions of minors engaged in sexual activity; or inappropriate access of computing systems to commit crimes.

B. Usage that harasses or infringes upon the rights of another person or entity is prohibited. This includes but is not limited to the transmission of abusive, obscene, threatening, or libelous material.

C. Usage that involves unsolicited or unsanctioned commercial activity is prohibited. This includes but is not limited to the use of University computing resources to operate personal for-profit ventures or to disseminate for-profit mass e-mailings (spam).

D. Usage for publishing Web content or similar information using campus resources requires the users to be responsible for following all provisions of this policy. This includes but is not limited to copyright and commercial activity that is not directly related to the University's mission.

E. Usage that bypasses or manipulates the security or integrity of any local or remote system or network is prohibited. This includes but is not limited to unauthorized access to a closed network or system (including hacking or service spoofing), unauthorized transmission or receipt of user access privileges (including login or password information), or attempts to intentionally obfuscate, misdirect, disguise, or forge the identity of a computer user, system, or network.

F. Usage that involves creating or releasing malware is prohibited. This includes but is not limited to viruses, worms, and spyware.

V. Copyright Issues

Users may not violate copyright law (Title 17, U.S. Code) through the unauthorized installation, distribution, or reproduction of any material that is defined by intellectual property rights. For more information, refer to the Libraries Copyright information page at http://libguides.owu.edu/copyrightandfairuse.

VI. Privacy of Information

Personal information transmitted over the University network or stored on University-owned computers will be examined, with notice, only if the Chief Information Officer, in consultation with the Provost, has reason to believe that:

- The integrity and/or security of the campus network has been compromised in an unacceptable manner
- A violation of a local, state, or federal law or regulation has occurred; or
- A violation of Ohio Wesleyan University's Computer Use Policy has occurred.

To maintain OWU computing resources, Information Services regularly backs up centralized data and logs, monitors network traffic patterns and system availability, inventories hardware and software applications, and performs other related activities necessary to ensure services for all users.

VII. Policy Enforcement and Modifications

A. Violations of this policy will be punished and may include temporary or permanent loss of computing privileges, temporary or permanent disconnection from local or remote networks, or other technology-related disciplinary actions as deemed appropriate by Information Services.
B. Student users who violate this policy may be referred to the University Judicial System and/or the Academic Affairs Office, based on the scope and severity of the violation.
C. Professional faculty and staff users who violate this policy may be referred to their Officer-level supervisor (Provost, Dean, Vice President, etc.) and/or the University President, based on the scope and severity of the violation.
D. Violators of this policy may be liable for civil and criminal prosecution, and it should be understood that nothing in this policy precludes enforcement under local, state, or federal laws or regulations.
E. Information Services, along with the Committee on Teaching, Learning, and Cross-Cultural Programming, is responsible for interpreting and modifying this policy, and for implementing operational procedures to support the policy and philosophy. Any modifications to this policy will be communicated through the Information Services Web site, the ISNEWS e-mail list, printed memoranda, the Daily Bulletin, etc. If a user disagrees with the substance and/or implementation of this policy, the user may first

discuss the matter with the Director of Information Services. If the situation is not resolved, it may be escalated to the Chief Information Officer (CIO). Failing adequate resolution of the matter with the CIO, faculty may appeal the matter to the Provost, who will make the final decision on the matter.

OWU Student Computer Use Policy Terms of Use and Service Agreement

This document describes the student's responsibility in using University computing resources. The downloading of unauthorized Internet files will not be tolerated at the University. Violations of this policy will be punished and may include temporary or permanent loss of computing privileges, temporary or permanent disconnection from local or remote networks, or other technology-related disciplinary actions as deemed appropriate by OWU Libraries and Information Services. You also may be referred to the University Judicial System and/or the Academic Affairs Office, based on the scope and severity of the violation.

1. I will connect my personal computer to OWU computing resources only after ensuring the operating system and maintenance software (i.e., anti-virus and anti-spyware utilities) have been properly updated. I will continue to apply software updates in a timely fashion or as directed by INFORMATION SERVICES.
2. I will regularly check and maintain my personal OWU e-mail account. The University will send official electronic communications to this account only.
3. I will not use OWU computing resources to violate any institutional, local, state, or federal rule, regulation, or law. This includes but I not limited to unauthorized duplication or dissemination of copyrighted materials including electronic text, graphic files, commercial software, and audio and video files (particularly in a peer-to-peer application environment, regardless of whether such activity is internal or external to the OWU campus) or inappropriate access of computing systems to commit crimes.
4. I will not use OWU computing resources to harass or infringe upon the rights of another person or entity. This includes but is not limited to the transmission of abusive, obscene, threatening, or libelous material.
5. I will not use OWU computing resources for unsolicited or unsanctioned commercial activity. This includes but is not limited to using University computing resources to operate personal for-profit ventures or disseminating for-profit mass e-mailings (spam). Also, users who publish Web content or similar information using campus resources are responsible for following all provisions of this policy – particularly in relation to copyright and commercial activity that is not directly related to the University's mission.
6. I will not use OWU computing resources to bypass or manipulate the security or integrity of any local or remote system or network. This includes but is not limited to unauthorized access to a closed network or system (including hacking, port probing or service spoofing), unauthorized transmission or receipt of user access privileges (including login or password information), or attempts to intentionally obfuscate, misdirect, disguise, or forge the identity of a computer user, system, or network.

NOTE: The entire OWU Computer Use Policy is online at
http://infoserv.owu.edu/pdfs/ComputerUsePolicy.pdf