Responsible Use of University Computing and Network Resources

University Policy

Applies to: Faculty, staff, students, agents, suppliers/contractors, volunteers, sponsored guests of academic and administrative units, and affiliated entities.

Responsible Office

Office of the Chief Information Officer

POLICY

Issued: 05/10/2000
Revised: 02/01/2013
Reviewed: 05/16/2016

This policy provides guidance for establishing responsibilities and limitations associated with the use of university computing resources. The general guiding principle behind the policy is that "cyberspace is not a separate legal jurisdiction;" that existing, generally applicable laws, rules, and policies apply equally to the use of university computing resources.

Adherence to this policy will require compliance with all applicable laws and university policies, and all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Purpose of the Policy

To provide expectations to support the responsible use of university computing resources.

Definitions

Term	Definition
Computing resources	Computers, computer systems, networks, and devices including but not limited to mobile phones, smartphones, and other mobile devices, and the institutional data they contain.
College, department and unit policies	Colleges, departments and units may have policies that provide for additional rights, restrictions and/or responsibilities that augment the university policy and apply to specific computers, computer systems, or networks, or to users within their specific units. These policies require approval by the chief information officer or the chief information officer's designees.

Policy Details

I. As a part of the physical and social learning infrastructure, Ohio State acquires, develops, and maintains computers, computer systems, and networks. These **computing resources** are intended for university-related purposes, including direct and indirect support of the university's teaching, research, and service missions; university administrative functions; student and campus life activities; and the free exchange of ideas among members of the university community and between the university community and the wider local, national, and world communities.

II. The rights of academic freedom and freedom of expression apply to the use of university computing resources. So, too, however, do the responsibilities and limitations associated with those rights. The use of university computing resources, like the use of any other university-provided resource and like any other university-related activity, is subject to the requirements of legal, regulatory, and ethical behavior within the university community. Responsible use of a computing resource does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

Applies to: Faculty, staff, students, agents, suppliers/contractors, volunteers, sponsored guests of academic and administrative units, and affiliated entities.

III. Colleges, departments, and units may have policies that provide for additional rights, responsibilities, and/or limitations that augment this policy and apply to specific computers, computer systems, or networks, or to uses within their specific units. These policies require approval by the Chief Information Officer or the Chief Information Officer's designees. Consult the operators or managers of the specific computer, computer system, or network or the management of the unit for further information.

IV. This policy covers use of university computing and network resources, regardless of location or device.

PROCEDURE

Issued: 05/10/2000
Revised: 02/01/2013
Reviewed: 05/16/2016

I. All users of university computing resources must:
   A. Comply with all federal, Ohio, and other applicable law; all generally applicable university rules, policies, and other governing documents; and all applicable contracts and licenses.
      1. Examples of such laws, rules, policies, contracts, and licenses include: the Family Educational Rights and Privacy Act (FERPA); Health Insurance Portability and Accountability Act (HIPAA); laws and regulations governing export control, which prohibit the electronic transmission of certain types of information to citizens of specified countries; laws governing libel, privacy, copyright, trademark, obscenity, and child pornography; the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit hacking, and similar activities; the Americans With Disabilities Act as reflected in the Web Accessibility Policy; Code of Student Conduct; Sexual Misconduct Policy; Institutional Data Policy; Disclosure or Exposure of Personal Information Policy; and all applicable software licenses.
      2. Users who engage in electronic communications with persons in other states or countries or on other systems or networks should be aware 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.
   B. **Use only those computing resources 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.
   C. **Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.** 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.
   D. **Respect the finite capacity of the computing 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 are no set bandwidths, disk space, CPU time, or other limitations applicable to all uses of university computing resources, the university may require users of those computing resources to limit or refrain from specific uses in accordance with this principle, using only those resources authorized for use. The reasonableness of any particular use will be judged by the university in the context of the relevant circumstances.
   E. **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 or as a matter of college, department, or unit policy.

Applies to: Faculty, staff, students, agents, suppliers/contractors, volunteers, sponsored guests of academic and administrative units, and affiliated entities.

F. **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. This also extends to the use of social media. Authorization to use university trademarks and logos on university computing resources may be granted only by University Communications or Trademark and Licensing, as appropriate. Contact these offices for further information and authorization.

G. FAQs regarding this policy (see Resources section) are provided for additional clarification and are incorporated by reference as part of this policy.

II. Security and Privacy

A. The university employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware that the university cannot guarantee such security. Users should engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing them regularly. Accounts and passwords may not be shared with, or used by, persons other than those to whom they have been assigned by the university.

B. While the university does not routinely monitor individual usage of its computing resources, the university may specifically monitor the activity and access the accounts of individual users of university computing resources, including individual login sessions and communications, without notice, when:

1. The user has given permission or has voluntarily made them accessible to the public, for example by posting to a publicly-accessible web page or providing publicly-accessible network services.
2. It reasonably appears necessary to do so to protect the integrity, security, or functionality of the university or other computing resources or to protect the university from liability.
3. There is reasonable cause to believe the user has violated, or is violating, this policy.
4. An account appears to be engaged in unusual or unusually excessive activity, as indicated by the reviewing of general activity and usage patterns.
5. Access is necessary and conducted pursuant to applicable university rules, policies or procedures.
6. It is otherwise required or permitted by law.

Any such individual monitoring, other than that specified above, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer or the Chief Information Officer's designees (see Contacts section below).

C. Users should be aware the use of university computing resources may not be private. For example, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, logging of activity, reviewing of general usage patterns for the unauthorized disclosure of institutional data, scanning of systems and network ports for anomalies and vulnerabilities, and other such activities that are necessary to render service or to meet university legal obligations

D. The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate university personnel or law enforcement agencies and may use those results in university disciplinary proceedings. Communications made by means of university computing resources are also generally subject to Ohio's Public Records Act to the same extent as they would be if made on paper.

III. Enforcement

A. Users who violate this policy may be denied access to university computing 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. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed, by the Office of Student Conduct.

B. The university may temporarily suspend or block access to an account, prior to the initiation or completion of such disciplinary procedures, when it reasonably appears necessary to do so to protect the integrity, security, or

Applies to: Faculty, staff, students, agents, suppliers/contractors, volunteers, sponsored guests of academic and administrative units, and affiliated entities.

functionality of university or other computing resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Responsibilities

Position or Office	Responsibilities
Office of the Chief Information Officer (OCIO)	1. Manage policy inquiries. 2. Review and respond to requests for approval of unit policies. 3. Coordinate prior authorization for investigatory monitoring. 4. Manage policy enforcement.
Colleges, VP units and regional campuses	1. Comply with applicable laws; this policy; university rules, policies, and other governing documents; contracts; and licenses. 2. Seek approval from the OCIO for any governing document related to university computing and network resources. 3. Work with the OCIO and coordinating university offices on policy enforcement. 4. Confer with the OCIO to designate specified individual within areas to handle monitoring authorization requests. 5. Contact the chief information officer or the chief information officer's designees to request investigatory monitoring. 6. Issue corrective action as appropriate under university policies.
Faculty, staff, students and other users of university computing resources	1. Ascertain, understand, and comply with applicable laws; this policy, university rules, policies, and other governing documents; contracts; and licenses. 2. Ascertain, understand, and comply with applicable unit policies. 3. Use only those computing resources you are authorized to use and only in the manner and extent authorized. 4. Respect the privacy of other users and their accounts. 5. Limit use so as not interfere unreasonably with the activities of other users. 6. Refrain from using university resources for personal commercial purposes or for personal financial or other gain.
Office of Legal Affairs	Provide advice and legal oversight when applicable.
Office of Human Resources	1. Provide guidance related to university policies issued by the Office of Human Resources. 2. Conduct fact-finding investigations and issue findings and action steps. 3. Issue corrective action as appropriate.

Resources

University Policies, policies.osu.edu/
Web Accessibility policy, ada.osu.edu/resources/osu-web-accessibility-policy.pdf
Disclosure or Exposure of Personal Information policy, ocio.osu.edu/assets/Policies/disclosurepolicy.pdf
Institutional Data policy, go.osu.edu/idp-document
Public Records policy, compliance.osu.edu/PublicRecordsPolicy.pdf
Sexual Misconduct Policy, hr.osu.edu/policy/policy115.pdf

Cloud Computing Guidelines, ocio.osu.edu/assets/Policies/ccgV7.pdf
FAQ for Responsible Use of University Computing and Network Resources, ocio.osu.edu/policy/policies/responsible-use/faq
Federal Export Control Regulations, orc.osu.edu/regulations-policies/exportcontrol/
FERPA, ocio.osu.edu/policy/policies/regulations/
HIPAA, ocio.osu.edu/policy/policies/regulations/
Information Security, ocio.osu.edu/itsecurity

Applies to: Faculty, staff, students, agents, suppliers/contractors, volunteers, sponsored guests of academic and administrative units, and affiliated entities.

Office of Trademark and Licensing, trademarklicensing.osu.edu/
Office of University Communications, ucom.osu.edu/
Ohio Public Records Act, compliance.osu.edu/public-records/
Virtual Legality: An Overview of Your Rights and Responsibilities in Cyberspace, ocio.osu.edu/policy/policies/responsible-use/virtual-legality/

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions, authorization for investigatory monitoring	Office of the Chief Information Officer, Director, Information Technology, Risk Management, and Governance	614-292-1508	ITPolicy@osu.edu
Academic issues	Office of Academic Affairs	614-292-5881	oaa.osu.edu
Legal issues	Office of Legal Affairs	614-292-0611	legal.osu.edu
Corrective action	Office of Human Resources, Employee and Labor Relations	614-292-2800	ohrc@hr.osu.edu hr.osu.edu/elr

History

Issued: 05/10/2000
Revised: 02/01/2013
Edited: 01/25/2016
Reviewed: 05/16/2016