


|   |                                   |  |   |
|---|-----------------------------------|--|---|
| <b>Name of Policy:</b> <a href="#">Responsible Technology Use policy</a><br><b>Policy Number:</b> 3364-65-01<br><b>Approving Officer:</b> President<br><b>Responsible Agent:</b> Vice President, CIO/CTO<br><b>Scope:</b> All University organizational units |                                   | <br><b>Revision date:</b> October 26, 2020<br><b>Original effective date:</b> November 18, 2008 |   |
| <input type="checkbox"/>  | New policy proposal               | <input checked="" type="checkbox"/>  | Minor/technical revision of existing policy |
| <input type="checkbox"/>  | Major revision of existing policy | <input type="checkbox"/>   | Reaffirmation of existing policy            |

(A) Policy statement

The principles 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 principles.

Like the use of any other university-provided resource and like any other university-related activity, the use of computing resources is subject to the requirements of legal and ethical behavior within the university community. The legitimate use of a computer, computer system or network 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 of university computing resources shall comply with the requirements identified in this policy.

(B) Purpose

This policy establishes requirements for the responsible use of university computing resources, identifies security enforcement and privacy measures, and potential consequences for violations.

(C) Scope

This policy applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations. Additional policies may apply to specific computers, computer systems or networks provided or operated by specific units of the university. Consult the operators or managers of the specific computer, computer system or network in which you are interested in for further information.

(D) Definitions

- (1) Sensitive data. Sensitive data is data with respect to which the university has an obligation to maintain confidentiality, integrity, or reliability.

(E) Policy

All users of university computing technology resources must adhere to the requirements of rule 3364-65-01 of the Administrative Code, the Responsible technology use policy:

- (1) Comply with all federal, Ohio and other applicable laws and regulations, 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 Health Insurance Portability and Accountability Act (HIPAA); the Family Educational Rights and Privacy Act (FERPA); the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking", "cracking", and similar activities; the university's code of conduct; rule 3364-50-01 of the Administrative Code, The University of Toledo Title IX 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 use.

- (2) Use only those computing resources which 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.
- (3) Respect the security of sensitive data and the privacy of other users and their accounts, regardless of whether those accounts are reasonably 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.
  - (a) Refrain from storing sensitive data on to portable storage devices where appropriate.
  - (b) Refrain from using elevated administrative roles to circumvent policy or university guidelines.
  - (c) Refrain from using sensitive data outside the scope of job description and duties.
  - (d) Refrain from accessing data inappropriately
- (4) Respect the finite capacity of those 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 is no fixed bandwidth, disk space, CPU time or other limits 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 the relevant circumstances.
- (5) Refrain from using those computing 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 practices.

- (6) 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 university marketing and communications. The use of appropriate disclaimers is encouraged.

(F) Security enforcement and privacy

The university employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the university cannot guarantee the absolute security of its computing technology resources or of its users' accounts. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users should also be aware that their uses of university computing resources are not completely private. 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 necessary for the rendering of service. The university may also specifically monitor the activity and accounts of individual users of university computing resources without notice.

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 appropriate university disciplinary proceedings. Communications made by means of university computing technology resources may also be subject to disclosure under Ohio's Public Records statutes to the same extent as they would be if made on paper.

## (G) Violations

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. However, the university may temporarily suspend or block access to an account or system prior to the initiation or completion of such procedures when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, or availability of university or other computing technology resources or to protect the university from liability. The university may also refer suspect violations of applicable law to appropriate law enforcement agencies.

## (H) Education for responsible use

Use of university information technology resources is subject to the user's agreement to adhere to the standards outlined in this policy. Upon assignment of a network password, each user will electronically accept that they have received and read the responsible technology use policy. The responsible technology use policy will be posted to the campus website to increase the ability of campus users to reflect on and consult the policy.

|   |   |
|---|---|
| <p>Approved by:</p> <p><u>/s/</u><br/>Gregory C. Postel, M.D.<br/>Interim President</p> <p><u>October 26, 2020</u><br/>Date</p> <p><i>Review/Revision Completed by:</i></p> <p>Senior Leadership Team<br/>Vice President, CIO/CTO</p> | <p><b>Policies Superseded by This Policy:</b></p> <ul style="list-style-type: none"> <li>• <i>Previous 3364-65-05, effective date May 3, 2012</i></li> <li>• <i>Policy number changed from 3364-65-05 to 3364-65-01 effective January 12, 2017</i></li> </ul> <p><b>Initial Effective Date:</b> November 18, 2008</p> <p><b>Review/Revision Date:</b> January 12, 2017,<br/>October 26, 2020</p> <p><b>Next review date: October 26, 2023</b></p> |
|---|---|