Ohio Administrative Code

Rule 3342-9-02 University policy regarding acceptable use of information technology resources.

Effective: July 8, 2021

(A) Purpose: to outline the acceptable use of university computer, network, application, telecommunications, data in digital form, or other information technology resources (hereinafter called technology resources) in order to ensure that all members of the campus community understand their responsibilities when using or accessing technology resources and to safeguard these resources.

(B) Policy statement: All users of university technology resources, whether or not affiliated with the university, and notwithstanding geographical location are responsible for their appropriate use, and by their use, agree to use them in an ethical, responsible manner and will comply with applicable federal, state and local laws and university policies. An attempt to engage in a prohibited activity is considered a violation whether the attempt is successful or not.

(C) Users with access to university technology resources must agree to and accept the following:

(1) Use of university supplied technology resources shall be for purposes that are consistent with the mission of the university. Ability to access university resources not otherwise supplied does not, by itself, imply authorization to do so.

(2) Be accountable for and only use accounts, passwords, and/or authentication credentials that they have been authorized to use for their role at the university.

(3) Only share data with others as allowed by applicable policies and procedures, and dependent on their assigned role.

(4) Comply with the security and privacy controls on all information technology resources used for university business, including but not limited to mobile and computing devices, whether university or personally owned.

(5) Comply with intellectual property rights, licensing and contractual agreements related to information technology resources.

(6) Respect the rights and privacy of others.

(7) Take responsibility for the content of their personal communications.

(8) Take reasonable care to safeguard equipment entrusted to them.

(9) Acknowledge that the principle of academic freedom shall apply to public communication in all these forms of communication, as well as in the transmission of information in both the physical and virtual classrooms.

(10) Acknowledge that the university may access data files in the course of its normal supervision of the network or system (i.e., backing up of electronic messaging material), when exigent circumstances arise (i.e., evidence of reported violations of policies or laws), or when the university receives requests pursuant to section 149.43 of the Revised Code (the Ohio Public Records Act).

(11) Acknowledge that the university cannot guarantee the absolute security and privacy of data stored on university technology resources.

(D) Unacceptable use includes and is not limited to the following list. Users are not permitted to:

(1) Share authentication details or provide access to their university accounts with anyone else (e.g., sharing the password).

(2) Impersonate another person, misrepresent their affiliation with another person or entity, engage in fraud, or hide or attempt to hide their identity.

(3) Circumvent, attempt to circumvent, or assist another in circumventing the security controls in place to protect technology resources and data.

(4) Knowingly download or install software onto university technology resources or use software

applications, which may interfere or disrupt service, or do not have a clear administrative, academic, research or scholarly use.

(5) Engage in activities that interfere with or disrupt users, equipment or service; distribute viruses or other malicious code; or install software, applications, or hardware that permits unauthorized access to technology resources.

(6) Conduct unauthorized scanning of university technology resources.

(7) Engage in inappropriate use, including but not limited to:

(a) Activities that violate state or federal laws, regulations, technology resource licensing, or university policies.

(b) Harass, discriminate or defame others.

(c) Widespread dissemination of unsolicited and unauthorized electronic communications.

(8) Engage in excessive use of enterprise technology resources, including but not limited to network capacity or enterprise server storage and computing capacity. Excessive use means use that is unrelated to academic or employment-related needs, or that interferes with other authorized uses.

(9) Use any means to view, gain access to, intercept data or network traffic, use facilities, accounts, access codes, privileges or technology resources not intended for their viewing or use.

(10) Use the universitys technology resources for commercial or for financial gain not related to the universitys administrative operations, academic, research, and scholarly pursuits.

(11) Represent personal electronic communications as being an official position of the university.

(E) Incidental personal use of technology resources, including email, is permitted provided that this use does not interfere with university operations, violate university policies, create an inappropriate atmosphere for employees in violation of law or university policy, generate incremental identifiable

costs to the university, and/or negatively impact the users job performance.

(F) Enforcement and administration

(1) Determination of violations shall be made in accordance with established applicable due process procedures (i.e., student code of conduct, collective bargaining agreement, academic and administrative grievances and appeals policies, as appropriate).

(2) Users who violate this policy may be denied access to university technology resources and may be subject to other penalties and disciplinary action, both within and outside of the university. The university may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of university or other technology resources or to protect the university from liability. The university may also refer suspected violations of applicable law to appropriate law enforcement agencies.

(3) The vice president for information technology and CIO is responsible for administering this policy.