Ohio Administrative Code

Rule 3349-9-05 Acceptable use of computing resources.

Effective: June 11, 2017

(A) Purpose

The purpose of this rule is to outline the acceptable use of computer equipment at university without inhibiting the use of the information technology environment that is intended for the greater benefit of university community. Inappropriate use exposes university to risks including virus attacks, compromise of network systems and services, and legal issues.

(B) Scope

The scope of this rule includes all authorized users who have access to the university network, are responsible for an account on any system that resides at any university facility, and/or store any university information on university equipment or systems.

This rule applies to all equipment and systems that are owned or leased by university, including, but not limited to: computers, laboratories, lecture theaters, and video conferencing rooms across the university together with the use of all associated networks, internet access, e-mail, hardware, virtual private network, data storage, computer accounts, software, telephony services, and voicemail.

(C) Definitions

(1) "Information Technology Facilities" includes but is not limited to university computers, servers, networks, phones, printers and software.

(2) "Users/Community" refers to all university employees, students, alumni, and authorized external users for legitimate university purposes (including contractors and vendors with access to university systems).

(D) Body of the rule

(1) General use and ownership

(a) Users should be aware that the data they create on university systems remains the property of university.

(b) Each user is responsible for using the information technology facilities in an ethical and lawful way, in accordance with university policies and relevant laws.

(c) Each user is responsible for cooperating with other users of the information technology facilities to ensure fair and equitable access to the facilities.

(d) Each user is responsible for exercising good judgment regarding the reasonableness of personal use. The university accepts no responsibility for the integrity or confidentiality of personal files stored on university's information technology facilities.

(e) University reserves the right to audit networks, systems, and equipment on a periodic basis.

(2) Security and proprietary information

(a) Users should take all necessary steps to prevent unauthorized access to any information stored on university's systems.

(b) Each user is responsible for the unique computer accounts which the university has authorized for the user's benefit. Authorized users are responsible for the security of their passwords and accounts.

(c) All devices that are connected to the university network, whether owned by the user or university, shall execute a real time virus scanning software with a current virus definition file.

(d) University recommends that any information that users consider sensitive or vulnerable be encrypted before sending it outbound electronically or on magnetic media.

(3) Confidentiality and privacy information

Use of the university network and systems is restricted to authorized users only. All users accessing this system:

(a) Must maintain high levels of security & confidentiality;

(b) Must preserve the privacy required for these data;

(c) Will access records only as required to perform assigned duties;

(d) Will not access or release private information without proper authorization; and

(e) Will not publicly discuss data in a way that might identify a person.

Unauthorized use is a violation of applicable university policies and state/federal laws and regulations (such as Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338, Family Educational Rights and Privacy Act, 20 U.S.C Section 1232g; 34 C.F.R Part 99 and Health Insurance Portability and Accountability Act of 1996 Pub. L. No. 104-191, 110 Stat. 1936) and will be subject to criminal, civil and/or administrative action.

(4) Prohibited activities constituting unacceptable use

(a) The following activities are strictly prohibited on university information technology facilities:

(i) Unauthorized access to accounts, data, or files

(ii) Using of the university's name, seal, and/or logo on personal web pages, e-mail, or other messaging facilities unless expressly authorized by the university

(iii) Procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction

(iv) Accessing, creating or distributing pornographic material

(v) Running a personal business on university equipment

(vi) Making fraudulent offers of products, items, or services originating from any university account

(vii) Making statements about warranty, expressly or implied, unless it is a part of normal job duties

(viii) Effecting security attacks or disruptions of network service. Security attacks include, but are not limited to:

(a) Disruptive activities, such as denial of service attacks, packet spoofing, and forging information for malicious purposes

(b) Introduction of malicious programs into the network or server (example, viruses, worms, trojan horses, phishing attacks, etc.)

(c) Port scanning or vulnerability scanning

(d) Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty

(ix) Providing information about, or lists of, university employees directly to parties outside university without proper authorization.

(b) The following email and communications activities are strictly prohibited:

(i) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (commonly known as 'spam')

(ii) Sending defamatory, aggressive or rude e-mail messages

(iii) Sending threatening, harassing, or hate-related communications to another person via email or

telephone, whether through language, frequency, or size of messages

(iv) Sending sexually explicit material

(v) Propagating chain mail (e-mail sent to a number of people asking the recipient to send copies of the e-mail with the same request to a number of recipients)

(vi) Impersonating another person by sending a message which appears to have come from another person's computer or represent themselves as being of a different gender, race, age, etc. (e.g., in a chat session or electronic conference)

Users are entitled to use the university's e-mail and messaging facilities for private purposes, provided such use is lawful. Messaging facilities may include chat sessions, newsgroups, and electronic conferences. University reserves the right to withdraw this permission in the event that such use places the information technology facilities at risk or poses a security or other threat. Users must respect the privacy and personal rights of others.

(5) Copyright violations

(a) Violations of the rights of any person or institution protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by university is strictly prohibited.

(b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of text and/or photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which university or the end user does not have an active license is strictly prohibited.

(c) Original multimedia works are protected by copyright. The copyright act's exclusive rights provision gives developers and publishers the right to control unauthorized exploitation of their work. Multimedia works are created by combining content, music, text, graphics, illustrations, photographs, and software.

(d) Authorized users are expressly forbidden to make digital files of any commercially available multimedia works including, but not limited to, recordings, music albums, album covers, and videos, without permission of the copyright owner. Investigative bodies are able to detect infringing activities of a student, faculty, or staff member. Individual members of the university community may be held liable for damages and costs if a copyright owner takes action for infringement of copyright.

(e) Distribution of music/film files for the purpose of trade or any other purpose which affects the copyright owner prejudicially, making music files available for downloading free of charge on an internet website, is a criminal offense.

(6) Enforcement

(a) Login access to the information technology facilities is a privilege that is granted by the department of information technology. An individual's access may be restricted on the grounds that the user is in breach of this rule. Any user found to have violated this rule may be subject to disciplinary action, up to and including termination of employment.

(b) For security and network maintenance purposes, authorized individuals within university may monitor equipment, systems and network traffic at any time. The university does not generally monitor e-mail, personal web sites, files, and data stored on the university's computers or traversing the university's network. However, the university reserves the right to access and monitor e-mail, web sites, server logs and electronic files and any computer or electronic device connected to the university network, should it determine that there is reason to do so. Such reason would include, but not be limited to, suspected or reported breaches of this rule, or breach of any statutes, regulations or policies of the university, or suspected illegal activity.

(c) Unlawful use will breach this rule and will be dealt with as a discipline offense. Unlawful use of the information technology facilities may also lead to criminal or civil legal action being taken against the individual. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment. The university will not defend or support any client of the network who uses the information technology facilities for an unlawful purpose.