3354:1-50-05.1 Technology resources procedure.

(A) User access.

The College operates and maintains Technology Resources to facilitate achievement of its missions and goals. Access to Technology Resources is a privilege granted to Users, but is not a right. Access may be denied, and Technology Resources may be seized, at any time and without notice. Every User is subject to this procedure, and other applicable policies and procedures of the College.

(B) Prohibited User behavior.

(1) Using Technology Resources to violate, or while violating, any law or College policy or procedure.

(2) Accessing or attempting to access any Technology Resource without proper authorization from the Information Technology Services ("ITS") Department; or using any Technology Resource to access or attempt to access any other party's technology resource without proper authorization.

(3) Using Technology Resources to access, display, transmit, or store obscene or pornographic materials or communications.

(4) Interfering or attempting to interfere with the operation of any Technology Resource, or with any User's use or access.

(5) Sharing without prior ITS authorization any username, password, or other access security method; or using or facilitating the use of any Technology Resource that is subject to any access restriction without prior ITS authorization.

(6) Using any Technology Resource to send any communication using a false name, or using any other method that suggests another individual is the sender.

(7) Using any Technology Resource in a manner inconsistent with contractual obligations or other legal restrictions applicable to the College.

(8) Using Technology Resources in such a way as to appear to express the views of the College (except to the extent one is properly authorized to do so).

(9) Knowingly or intentionally introducing any bugs, viruses, worms, malware, backdoors, keyloggers, or other "malicious software" to Technology Resources; or knowingly or intentionally using Technology Resources to propagate any bugs, viruses, worms, malware, backdoors, keyloggers, or other "malicious software."

(10) Using non-supported and non-approved tools such as, but not limited to, voice, storage, or video technologies on Technology Resources or personal devices to conduct College business. This provision does not apply to faculty engaged in the development of course curriculum, course content, teaching, student evaluation, and conducting scholarly inquiry.

(C) No expectation of privacy.

Users should not have an expectation of privacy in anything they create, store, send, or receive using Technology Resources. Users should be aware that communications and other information sent or received through Technology Resources may not remain confidential, and may be decrypted while in transit or while stored on the sending or receiving Technology Resources. The College reserves the right, with or without notice, to monitor, access, and record all User activities involving Technology Resources.

The College monitors and records User Internet activity. Periodically, this activity may be analyzed for individuals' violations of College policies and procedures. (At any time, Users may obtain a list of Internet activity associated with their account by submitting a request to the Vice President of ITS.) The normal operation and maintenance of Technology Resources generally includes the backup and caching of certain data and communications, the logging of activity, the monitoring of general usage patterns, and other activities.

The College may also specifically monitor and record the activity and accounts of individual Users of Technology Resources, including individual login sessions, communications, and any other activities, without notice,

when (a) the User has voluntarily made them accessible to the public, as by posting online; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of College or other Technology Resources or to protect the College from liability; (c) reasonable cause exists supporting the belief that the User has violated, or is violating, College policy or procedure; (d) a User account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns; or (e) when such monitoring or recording is otherwise required or permitted by law. Individually-targeted monitoring described in (b) through (e) must be authorized in advance by the Vice President of ITS, Vice President of Human Resources, or the College President.

The College, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary proceedings. Communications and other information transmitted or stored using Technology Resources may also be subject to disclosure under Ohio's public records laws.

(D) Installation of software and connection of devices.

Only ITS may install software on Technology Resources, or connect any device to Technology Resources. Any User who connects a device or installs software in violation of the foregoing does so at the User's own risk, and the College may hold such Users responsible for any associated costs, claims, losses, or liabilities. Devices connected or software installed by anyone other than ITS will not be supported by the College, and may be removed by the College at any time without notice and without any liability for any damages whatsoever to any party.

(E) Security.

Users must take reasonable steps to ensure the security and privacy of the information they are authorized to access. Users must utilize strong, unique passwords for the systems they are granted. Users must secure devices and systems by locking or logging out when unattended. In the event suspicious activity is suspected, users should contact the helpdesk or the Information Security Department immediately. Sensitive or confidential information must be transmitted only to authorized parties using secure methods, such

as encrypted protocols. Sensitive or confidential information must only be stored in approved access-controlled locations. Users should avoid unnecessarily storing or collecting sensitive data. Any such data should be deleted when no longer needed in accordance with records retention.

Users must not attempt to circumvent or bypass security measures in use by the College. This includes but is not limited to tampering with or disabling security software, using VPN to bypass filtering, or using hardware devices and/or software designed to prevent workstations from automatically locking due to inactivity.

Users are expected to take annual security awareness training where available. The above practices are not intended to be an all-inclusive list of reasonable steps.

(F) Violations.

Violation of this procedure may result in sanctions up to and including: immediate and permanent termination of access privileges; and civil or criminal legal action by the College, law enforcement organizations, and injured third parties. In addition, students, faculty, and staff may be subject to disciplinary actions described in other applicable College policies and procedures.

(G) Notices and disclaimers.

(1) The College may restrict or terminate User access at any time, without notice, and with or without any reason.

(2) Users are solely responsible for storing their files on approved network drives. Failure to do so may result in damage or complete loss of files and all associated information.

(3) The College disclaims any and all representations or warranties, expressed or implied, about the Technology Resources' quality; effectiveness; safety; fitness for any purpose; and lack of errors, viruses, worms, or other "malicious software."

(4) The College is not responsible for offensive or illegal material which may be accidentally or intentionally sent, received, or displayed while using computers or networks belonging to the institution.

(5) The College is not responsible for damaged, lost, unavailable or stolen data, intellectual property, or other real property resulting from or occurring while using Technology Resources.

(6) The availability of Technology Resources is not guaranteed to any extent whatsoever.

(7) Technology Resources sometimes link to or contain materials generated or posted by College departments, organizations, students, employees, or others. Such materials do not necessarily represent the official views of the College.

(8) The College does not assume any responsibility or risk for User's use of the Internet. The College does not operate, control or endorse any information, products or services on the Internet in any way.

(9) Users should avoid personal uses of Technology Resources that result in any charge to the College. Users must promptly identify all such charges to the College, and promptly provide full reimbursement.

(10) Users may not use College resources for mining crypto-currencies.

(11) Technology Resources are intended for teaching, learning, and conducting College operations.

(H) Capitalized terms not defined in this procedure shall have the meaning given to them in the Technology Resource policy.

(I) The College President hereby designates the Executive Vice President of Administration or that person’s designee to take all steps necessary and appropriate for implementing this procedure.

Effective Date: April 26, 2022
Prior Effective Date: February 28, 2022
Procedure amplifies: 3354:1-50-05