YOUNGSTOWN STATE UNIVERSITY

RESOLUTION TO MODIFY
ACCEPTABLE USE OF UNIVERSITY TECHNOLOGY RESOURCES POLICY, 3356-4-09

WHEREAS, University Policies are being reviewed and reconceptualized on an ongoing basis; and

WHEREAS, this process can result in the modification of existing policies, the creation of new policies, or the deletion of policies no longer needed; and

WHEREAS, action is required by the Board of Trustees prior to replacing and/or implementing modified or newly created policies, or to rescind existing policies.

NOW, THEREFORE, BE IT RESOLVED, that the Board of Trustees of Youngstown State University does hereby approve the modification of the University Policy stated above and attached hereto.

Board of Trustees Meeting
June 7, 2024
YR 2024-64

3356-4-09 Acceptable use of university technology resources.

Responsible Division/Office:	Information Technology Services
Responsible Officer:	VP for Finance and Business Operations
Revision History:	August 1999; November 2010; December 2012; March 2016; June 2021; March 2023; June 2023; June 2024
Board Committee:	Finance and Facilities
Effective Date:	**June 7, 2024**
Next Review:	2029

(A) Policy statement. University technology resources are provided to the university community to support its academic and administrative functions in accordance with its teaching, research, and service missions. These resources are intended to be used for the educational and business purposes of the university in compliance with this policy.

(B) Scope. This policy applies to all users and uses of university-owned technology resources (including those acquired through grant processes) as well as to any non-YSU and/or remote technology devices while connected to the YSU network. This policy also covers the use of generative AI technologies, such as language models, image generation models, and other AI-powered tools, whether provided by the university or obtained from external sources.

(C) Parameters.

(1) Technology resources (computing, digital recordings, networking, data and network services) are provided to the university community in order to fulfill the mission of the university.

(2) While the university recognizes the importance of academic freedom and freedom of expression, as a public employer, the university also has a responsibility to comply with all federal and state laws and regulations, as well as the obligation to fulfill its mission.

(3) Use of university-owned technology to access resources other than those supporting the academic, administrative, educational,

research and services missions of the university or for more than limited, responsible personal use conforming to this policy is prohibited.

(4) Technology resources provided by the university are the property of the university. University-owned technology is not intended to supersede the need for technology purchases for personal purposes.

(5) As the university is a public entity, information in an electronic form may also be subject to disclosure under the Ohio public records act to the same extent as if they existed on paper. All use is subject to the identification of each individual using technology resources (authentication).

(6) Use of technology is subject to the requirements of legal and ethical behavior and is intended to promote a productive educational and work environment.

(D) Definitions.

(1) Generative AI refers to a category of artificial intelligence (AI) systems that are designed to generate new content, such as text, images, or other forms of data, based on patterns and information it has learned from existing data. Unlike traditional AI systems that follow explicit instructions or rules, generative AI has the ability to create novel outputs by learning from large datasets.

(2) Private institutional data is defined in university policy 3356-4-13, "Sensitive information/information security"; rule 3356-4-13 of the Administrative Code and encompasses information of a sensitive, confidential, or personally identifiable nature, such as social security numbers, student records, medical information, financial records, and research data with privacy concerns.

(3) Public data is defined in university policy 3356-4-13, "Sensitive information/information security"; rule 3356-4-13 of the Administrative Code and comprises non-sensitive, non-confidential information that does not personally identify individuals, including publicly available research publications, course catalogs, general university information, and non-sensitive statistical data.

(E) User requirements. All users of the university-owned technology resources (computing, digital recordings, networking and data), regardless of affiliation with the university, must:

(1) Use only those technology resources that they are authorized to use and use them only in the manner and to the extent authorized.

(2) Protect the confidentiality, integrity and availability of technology resources.

(3) Comply with all federal, Ohio, and other applicable law as well as applicable regulations, contracts, and licenses.

(4) Comply with all applicable policies at Youngstown state university (YSU).

(5) Respect the right of other technology users to be free from harassment or intimidation.

(6) Respect copyrights, intellectual property rights, and ownership of files and passwords.

(7) Respect the privacy of other users and their accounts, regardless of whether those accounts are securely protected.

(8) Respect the finite capacity of technology resources and limit use so as not to consume an unreasonable amount of or abuse those resources or to interfere unreasonably with the activity of other users or to disrupt the authorized activities of the university.

(9) Limit personal use of university technology resources so that such use does not interfere with one's responsibilities to the university.

(10) Not attempt to circumvent information technology security systems or the university "IT Security Manual."

(11) Not use any radio spectrum space on any YSU-owned or YSU-occupied property, unless it is part of an approved wireless services deployment by the university.

(12) Not use technology resources for personal commercial purposes or for personal financial or other gain unless specifically approved by the university.

(13) Not state or imply that they speak on behalf of the university without authorization to do so and not use university trademarks and logos without authorization to do so.

(F) User responsibilities.

(1) By accepting employment, being admitted as a student, or asking for any guest technology resource privileges, users implicitly agree to adhere to this policy and agree to adhere to the university "IT Security Manual."

(2) Users are responsible for any activity performed using their usernames and passwords except when account security is compromised by actions beyond the user's control.

(3) Users are responsible for any activity performed on university-owned technology devices assigned to them except when the device is compromised by actions beyond the user's control.

(4) There is no expectation of personal privacy when using university resources. See paragraph (G) of this rule.

(5) Potential violations regarding use of technology resources should be reported to the appropriate information technology services manager(s) or information security officer.

(6) Users are responsible for ensuring that critical data are backed up and available to be restored for systems not administered by information systems technology. This includes critical information contained on technology devices oriented to individual use (e.g., desktops, laptops, smart phones, and similar such devices).

(7) Users are responsible for maintaining data in compliance with the university records retention plan.

(8) Users are responsible for ensuring that sensitive information to which they have access is guarded against theft. (See university

policy 3356-4-13, “Sensitive information/information security”; rule 3356-4-13 of the Administrative Code.)

(9) Users are responsible for understanding whether the technology is in compliance with this policy prior to use.

(10) Personal use of computing resources not otherwise addressed in this policy or these procedures will generally be permitted if such use does not consume a significant amount of resources, does not interfere with the performance of an individual’s job or other university responsibilities, and is otherwise in compliance with university policies.

(11) Students are responsible for compliance with academic integrity policies. These policies may include further restrictions on technology use by colleges, schools, departments or instructors.

(G) No expectation of privacy.

(1) The university does not routinely monitor specific individual end-user usage of its technology resources. However, the university does routinely monitor technology resource usage in the normal operation and maintenance of the university’s computing, network and data resources. This monitoring includes the caching and backing up of data and communications, the logging of activity, the monitoring of general usage patterns, the scanning of systems and networks for anomalies and vulnerabilities, the filtering of malicious traffic, and other activities that are necessary for the rapid and efficient delivery of services. Technology users should be aware that there is no expectation of privacy associated with the use of university technology resources.

(2) When authorized by the office of the general counsel, the university may also specifically monitor the activity and accounts of individual end-users of university technology resources, including login sessions, file systems, and communications.

(3) When authorized by the appropriate university administrator (president, vice president, or associate vice president reporting to the president), the university may access active end-user accounts, files, or communications used for university business when needed

by a supervisor or assigned personnel for university business and the end-user is unavailable. For inactive end-users, such as retirees or terminated employees, the end-user's former supervisor or the individual currently holding the supervisor position may request access. For inactive student end-users the provost may authorize access. For all other inactive end-users, the general counsel may authorize access.

(4) 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, student conduct, or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

(5) Personal computing devices:

(a) Personal computing devices (laptops, desktops, tablets, cellular phones) are restricted to the campus wireless network or the residence hall network.

(b) No personal computing devices will be allowed to connect to the wired campus network (excluding the residence hall network).

(c) Personal computing devices must comply with university "IT Security Manual" when using the campus wireless network or other provided university technology resource.

(d) Personal computing devices used to conduct university business are subject to public records requests.

(e) Personal hubs, routers, switches, or wireless access points are prohibited from being connected to either the university's wired or wireless network.

(H) Email. University email (i.e. username@ysu.edu) is the only acceptable email for conducting university business. Email is an official means for communication at the university. Students, faculty, and staff are expected to check their official email address on a frequent and consistent basis in order to stay current with university communications.

(I) Security. The university employs various measures (i.e., the university's "IT Security Manual") to protect the security of information technology resources and user accounts; however, users should be aware that the university cannot provide full security measures without user participation. Users should increase their technology security awareness and fully employ access restrictions for their accounts, including using strong passwords, guarding passwords diligently and changing passwords regularly to help safeguard their use of technology.

Special procedures exist and must be followed to ensure that accounts for employees are secured with passwords known to only the account holder. Passwords may be changed at the request of the area supervisor and approved by the supervisor's vice president or the president.

(J) Additional policy ramifications. Users must abide by all applicable restrictions, whether or not they are built into the computing system, network or information resource and whether or not they can be circumvented by technical or other means. Individuals who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those states and countries and the rules and policies of those technology systems and information resources.

(K) Generative AI acceptable use guidance.

(1) Use of generative AI is encouraged for the purpose of advancing academic capabilities and university operations within the parameters set forth in the in the "YSU AI Principles Statement" (see OAA website) and potential further restricted by division, colleges or departments.

(2) Any use of generative AI not in accordance with university guidance or the framework defined by academic instruction is strictly prohibited.

(L) Examples of unacceptable use:

(1) As a further aid to policy compliance, the following non-exhaustive list is provided of activities that are prohibited.

(a) Using technology resources to engage in fraud, defamatory,

abusive, unethical, indecent, obscene, pornographic and/or unlawful activities is prohibited.

(b) Using technology resources to procure, solicit, or transmit material that is in violation of sexual, racial or other harassment or hostile workplace laws is prohibited.

(c) Any form of harassment by electronic means (e.g., email, videoconferencing, web access, phone, paging), whether through language, content, frequency or size of messages is prohibited. (Refer to university policies 3356-2-03, "Discrimination/harassment," 3356-2-05, "Title IX sexual harassment policy," and 3356-4-21, "Campus free speech"; rules 3356-2-03, 3356-2-05, and 3356-4-21 of the Administrative Code.)

(d) Making fraudulent offers of products, items or services using any university technology resource is prohibited.

(e) Using technology resources for unauthorized or inappropriate financial gain, unauthorized solicitation, or activities associated with a for-profit business, or engaging in an activity that involves a conflict of interest. (Refer to university policies 3356-7-01, "Conflicts of interest and conflicts of commitment" and 3356-7-19, "Access to campus for purposes of commercial solicitation or advertising"; rules 3356-7-01 and 3356-7-19 of the Administrative Code.)

(f) Creating or forwarding chain letters, Ponzi, or other pyramid schemes is prohibited.

(g) Broadcasting of unsolicited mail or messages is prohibited. Examples include chain letters, virus hoaxes, spam mail, and other email schemes that may cause excessive network traffic. Sending large numbers of electronic mail messages for official university purposes necessitates following the university's procedures for the electronic distribution of information.

(h) Sending junk mail or advertising material to individuals

who did not specifically request such material (email spam) is prohibited.

(i) Violations of the rights of any person or company 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 is prohibited.

(j) Unauthorized copying and downloading of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and films and the installation of any copyrighted software for which an active license has not been procured is prohibited.

(k) Circumventing user authentication or security of any host, network or account is prohibited. This includes, but is not limited to, monitoring by use of keylogging or session logging.

(l) Revealing your account password to others or allowing use of your account by others is prohibited. This prohibition extends to family, other household members, friends and/or co-workers.

(m) Attempting to log onto another user's account (secured or otherwise) is prohibited.

(n) Sending electronic communications in such a way that masks the source or makes it appear to come from another source is prohibited.

(o) Personal use beyond limited responsible use is prohibited.

(p) Digital recordings of any sensitive nature, such as manager-employee personnel discussions/interactions or any discussions that email sensitive or protected data (i.e., FERPA, HIPAA, etc.), as well as recording of any meeting or conversation without full disclosure that the interaction

is being recorded. All recordings become subject to the public records law of Ohio, university policy 3356-9-07, "Public records" and 3356-9-09, "Records management" (rules 3356-9-07 and 3356-9-09 of the Administrative Code).

(q) Use of TikTok, or any other social media application that freely harvests device and/or network data, is prohibited on YSU-owned devices.

(r) Submission of private institutional data to an open generative AI system.

(2) Under no circumstances is an employee of Youngstown state university authorized to engage in any activity that is unethical or illegal under local, state or federal law while utilizing university-owned resources.

(M) Enforcement.

(1) The office of the chief information officer (CIO) may suspend and/or restrict either an individual's or a device's access to the university network resource if:

(a) It is deemed necessary to maintain the security or functionality of the network resource.

(b) It is deemed necessary to protect the university from potential liability.

(c) The account, system, or device is believed to have been either compromised or is in violation of this policy.

(2) The office of the CIO must immediately report the enforcement action and the justification for the action to the vice president of student affairs, vice president for finance and administration, or provost (or their designee), as applicable. The university may permanently suspend all technology access of anyone using the university network resource until due process has been completed by student conduct, employee administrative discipline and/or law enforcement agencies.

(N) Exceptions.

(1) The chief information officer, or designee, may approve exceptions to this policy on a case-by-case basis (with written authorization according to the university "IT Security Manual").

(2) Faculty and staff who have a legitimate business or academic case for using TikTok or other prohibited applications can request an exception.

Approved exceptions require a departmental purchase of a dedicated YSU-owned device that does not comingle university data.

(3) In regards to generative AI, faculty and staff can apply for exceptions by email to the CIO and provost. All exceptions will be reviewed by both parties and the submitter will receive a response within a reasonable amount of time.

(O) Violations: An employee may be held financially liable for a data breach when using non-university storage or email. In addition, in the event of a data breach, the university may not defend or support any employee who uses unsupported information technology or unacceptable use of generative AI.