OTTERBEIN UNIVERSITY

UNIVERSITY POLICIES

Section 800: Information Technology	Policy Number: 803.0 Acceptable Use Policy
New: ____ Revised: __X__	Effective Date: 01/01/2004 Last Revised: 01/07/2022
Scope: Faculty, Staff, Students, Contractors, Guests	Authority: Chief Information Officer Approved by:

803.0 Title Acceptable Use of Information Technology Resources

803.1 Philosophy Technology resources provided by Otterbein University are made available to students, faculty, staff and approved guests primarily as tools for enhancing and facilitating teaching, learning, and scholarly research. This policy establishes outlines the acceptable use of those information technology resources at Otterbein University (OU). The intent of this policy includes:

1. Protecting the confidentiality and integrity of electronic information and privacy of its users to the extent required or allowed under federal and state law.
2. Ensuring that the use of electronic communications complies with the provisions of OU policy and state and federal law; and
3. Allowing for the free exchange of ideas and support of academic freedom.

This policy applies to all users of, and information technology resources owned, operated, or provided by Otterbein University.

"Users" includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling OU information technology resources.

Information transmitted or stored on University IT resources is the property of Otterbein University unless it is specifically identified as the property of other parties.

803.2 Statement Each User of Otterbein University resources must be familiar and comply with all University policies governing the use of OU resources as well as with the Procedures specified in this Acceptable Use Policy. Activities involving these resources must also be in accord with the University policies found in faculty and staff handbooks, the Campus Life Handbook; all relevant local, state, federal laws and international agreements, and all contracts and licenses.

Acceptance of this policy is assumed if a User accesses, uses, or handles University resources.

803.3 Definitions

1. UNIT: An operational entity such as a school, division, or department.
2. USERS: Includes but is not limited to students, faculty, staff, contractors, agents, representatives, and visitors accessing, using, or handling OU information technology resources.
3. SENSITIVE INFORMATION: Information that is protected against unwarranted disclosure. Protection of sensitive information may be required for legal, ethical, privacy, or proprietary considerations. Sensitive information includes all data that contains: Personally Identifiable Information, Protected Health Information, student education records, card holder data, or any other information that is protected by applicable laws, regulations, or policies. (See the Otterbein Personally Identifiable Information Policy.)

803.4 Procedure

1. User Privacy

a. Users of Otterbein University information technology (IT) resources have no right to privacy attendant upon their use of University IT resources, nor should they have any expectation of privacy in their use of such resources.
b. As required by state law, Otterbein University hereby notifies users that email may be viewed as a public record and open to public inspection under the Ohio Open Records Act (Section 149.43 of the Ohio Revised Code)--unless the email is covered by an exception to the Act, by containing personally identifiable information, proprietary information, or other such covered information.
c. Similarly, any activity on OU resources, systems, and networks may be monitored, logged, and reviewed by OU-approved personnel or may be discovered in legal proceedings. All documents created, stored, transmitted, or received on OU computers and networks may be subject to monitoring by office of Information Technology Services (ITS) systems administrators.

2. Users WILL

a. Comply with all Otterbein University policies to ensure confidentiality, integrity, and availability of OU resources under their control
b. Only use OU resources for which the User has authorization
c. Be responsible for using OU-approved resources for electronic data and understanding the back up and retention policies associated with those resources
d. Control and secure physical and network access to OU resources, including data
e. Lock screens when leaving their desks and log out of sessions when

finished

f. Monitor access to their accounts (If a User suspects unauthorized activity or that their account has been compromised, they must report the compromise to ITS and change passwords immediately.)
g. If you have administrator rights to a machine, install, use, and regularly update virus protection software
h. Use only supported and patched applications and operating systems on OU-owned devices (Exceptions must be documented and approved by ITS.)
i. Abide by the password protection best practices specified for each University resource
j. Use only the passwords and privileges associated with their computer accounts and use those accounts only for their authorized purpose
k. Respect the rights of others with regard to intellectual property, privacy, freedom from harassment, academic freedom, copyright, and use of University resources;
l. Use University-provided software in a manner that strictly adheres to all licensing provisions, including installation, use, copying, number of simultaneous users, and other terms of the license

3. Users WILL NOT

a. Share access codes or passwords
b. Use accounts, access codes, privileges or IT resources for which they are not authorized
c. Tamper, modify, or alter any restrictions or protections placed on their accounts, OU systems, or network facilities
d. Physically damage, vandalize, or compromise University IT resources
e. Commit copyright infringement, including file sharing of video, audio, or data without permission from the copyright owner
f. Use University resources to introduce, create, or propagate SPAM, PHISHING email, computer viruses, worms, Trojan

horses, or other malicious code

g. Eavesdrop on or intercept other Users' transmissions
h. Attempt to degrade the performance or availability of any system or to deprive authorized Users access to any OU resources
i. Misrepresent their identity with actions such as IP address "spoofing," email address falsification, or social engineering
j. Send email chain letters or mass mailings for purposes other than official University business
k. Use OU resources as an email relay between non-OUemail systems (routing email through OU email systems between two non-OU systems)
l. Engage in activities that violate state or federal law, a University contractual obligation, or another University policy or rule including but not limited to Human Resources policies and Standards of Conduct for students
m. Comment or act on behalf of OU over the Internet without authorization
n. Connect devices (such as switches, routers, hubs, computer systems, and wireless access points) to the network without prior approval from ITS.
o. Use without authorization any device or application that consumes a disproportionate amount of network bandwidth
p. Include or request that Sensitive Information be included in unprotected electronic communication (e.g., email, instant message, text message)

4. Rights of Otterbein University

The University reserves the right to access, monitor, review, and release the activity of an individual User's accounts as well as of personal Internet accounts used for OU business. Otterbein University reserves the right to access any OU-owned resources and any non-University-owned resources on OU property, connected to OU networks, or containing OU data. This action may be taken to maintain the network's integrity and the rights of other authorized Users. Additionally, this action may be taken if the security of a computer or network system is threatened, misuse of University resources is suspected, or the University has a legitimate business need to review activity or data. This action will be taken only after obtaining

approval from an authorized OU office (e.g., Office Risk Management or Compliance Office), or in response to a subpoena or court order.

5. Copyright and Licenses

a. Violation of copyright law or infringement is prohibited by OU policy and state and federal law. Any unauthorized use of copyrighted material may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct in the Human Resources Policy and Procedures.
b. Software may not be copied, installed, or used on University resources except as permitted by the owner of the software and by law.
c. Users will properly license software and strictly adhere to all licensing provisions, including installation, use, copying, number of simultaneous users, and terms of the license.
d. All copyrighted information, such as text and images, retrieved from University resources or stored, transmitted, accessed, or maintainedwith University resources must be used in compliance with applicable copyright and other laws.
e. Copied material must be properly credited using applicable legal and professional standards.
f. Each Unit is responsible and accountable for maintaining records of purchased software licensure. Information Technology Services is responsible for maintaining records and information related to centrally provided software. These records are subject to audit for compliance.

6. Personal Use

a. Otterbein University resources are provided for use in conducting authorized University business. All users are prohibited from using these resources for personal gain, illegal activities, or obscene activities.
b. The prohibition against using University IT resources for personal gain does not applyto:
    i. Scholarly activities, including the writing of textbooks or preparation of other teaching materials by faculty members;
    ii. Consulting and other activities that relate to a faculty member's professional development or as permitted under OU policy;

c. Incidental or casual personal use of these resources is permitted by this policy, except when such use:
   i. Is excessive or interferes with the performance of the User's University responsibilities.
   ii. Results in additional incremental cost or burden to University resources;
   iii. Violates any state or federal law or is otherwise in violation of this or any other OU policy;
   iv. Results in additional risk to the confidentiality, integrity, and availability to OU resources.
d. University IT resources may not be used for commercial purposes, except as specifically permitted under other written University policies or with the written approval of the appropriate University vice president.
e. Any commercial use of University IT resources must be properly related to University activities and provide for appropriate reimbursement of taxes and other costs the University may incur by reason of such use.
f. The ".edu" domain on the Internet has rules restricting or prohibiting commercial use. Activities not appropriate for the ".edu" domain but otherwise permissible using OU resources must use other domain designations.

7. Misuse of IT Resources

a. Users must report all suspected or observed illegal activities to the appropriate OU administrative office. Examples include theft, fraud, copyright infringement, illegal electronic file sharing, sound or video recording piracy, hacking, and viewing or distribution of child pornography.
b. Abuse of networks or computers at other sites through the use of OU resources will be treated as an abuse of resource privileges.
c. Otterbein University prohibits the use of resources by employees for campaign or political advertising on behalf of any

party, committee, agency, or candidate for political office. This does not prohibit use of University resources to discuss or examine political topics or issues of public interest, so long as such use does not advocate for or against a particular party, committee, agency, or candidate.

8. Violations of Policy

Student violations of this policy, such as computer time/theft/abuse (as included in the Campus Life Handbook located on the student conduct page), will be addressed through the Student Affairs Office. Employee violations of this policy are addressed in the Policies and Procedures Manual for Salaried and Hourly Staff or in the Union Contract. Violations of this policy by administrative staff, non-exempt staff and union employees are handled through the Office of Human Resources. Faculty violations are handled through the Office of the Provost. Violations of local, state, or federal laws will be reported to the appropriate authorities. The University may temporarily suspend or block access to an account or remove files, when reasonably necessary to do so in order to protect the integrity, security or functionality of University or other computing resources or to protect the University from liability. Any such suspension or blocking of access to an account, other than as required by law or necessary to respond to perceived emergency situations, must be authorized in advance by the Chief Information Officer.

803.5 Related Policies

Data Classification Policy
Personally Identifiable Information Policy
Data Access Policy

803.6 History Enacted: 01/07/2022
Revised: