WINTHROP UNIVERSITY

Policy Number/Title:	7.1.14 Acceptable Use Policy
Effective Since:	01/01/2025
Last Revision Approved:	11/20/2024
Responsible Office:	Computing and Information Technology

1. Scope:

This policy applies to all Users of university information technology assets.

2. Definitions:

Specific meanings of terms seen throughout this policy can be found below.

2.1. University information technology assets: University owned, operated or maintained workstations, servers, printers, copiers, telephones, switches, routers, wiring and hubs; wireless and cellular components; mobile devices such as smart phones, tablets, laptops and other portable computing devices; or any university owned, operated or maintained technology, software, components or devices that store, process, or transmit information or data.

2.2. Users: all Winthrop faculty, staff, students, contractors, vendors, and guests who have been authorized and provided access to information technology assets by the University.

3. Policy:

Access to and utilization of information technology assets owned or operated by Winthrop University (hereinafter termed "University") imposes certain responsibilities and obligations on authorized Users. Users are subject to state government policies and local, state, and federal laws.

3.1. Acceptable use is always ethical and reflects honesty. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, the appropriate protection of students' and employees' personal and health-related information, and the individual's right to freedom from intimidation, harassment, and unwarranted annoyance.

3.2. Users may be subject to limitations on their access to and the use of information technology assets as determined by the appropriate supervising authority.

3.3 Exceptions to Policy

Specific exceptions may be allowed for:

3.3.1. Information Technology personnel, Winthrop University Police Department, or other authorized personnel while performing system maintenance, troubleshooting, or participating in potential criminal or misconduct investigations.

3.3.2. Users performing bona fide teaching, research, classroom, or scholarly activities. Bona fide teaching, research, classroom, or scholarly activities shall have prior written approval from the Dean in the respective academic college of the University.

3.4 Terms of Permitted Use, Privacy, and Monitoring

3.4.1. Access to information technology assets is provided as a tool for the University's Users. Use of information technology assets is subject to monitoring and/or recording for security, legal compliance, protecting the integrity of University resources, protecting the rights of Users, network management, or other purposes deemed appropriate by the University. At all times, the University has the right, but not the obligation, to access, monitor, and record information technology assets' usage. There are systems currently in place to monitor and/or record information technology assets' usage, as well as the files, information, and location of all sites accessed by Users.

3.4.2. Users should have no expectation of privacy in anything that they access, view, create, store, transmit, or receive on or through University technology assets, even during limited personal use of University information technology assets (see section 5.2), all of which may remain, be accessed, or be viewed on the information technology assets and may be retrieved and monitored by the University.

3.4.3. The University reserves the right to investigate all activity, without limitation, on or through the information technology assets, and to permit Information Technology and other appropriate personnel to access material for such investigation. Generally, any such access will be made only by those University representatives who have a need to know for legitimate business reasons, compliance with legal processes and federal procedures, or when necessary to protect a property right or other legal interest of the University.

3.4.4. No individual is provided any right to maintain a University e-mail address or other University associated account, including social media accounts, once the decision to eliminate that address or account is made by the appropriate supervising authority.

3.5 Permissible Uses

In making acceptable use of resources, Users covered by this policy must take the

following actions.

3.5.1. Use the information technology assets, including e-mail and access to the Internet, in a manner consistent with all other applicable University policies and legal requirements.

3.5.2. Comply with software licenses, copyrights, and all other state, federal, and international laws, including those governing intellectual property and online activities.

3.5.3. Be guided by reasonable judgment.

3.5.4. It is recognized that Users may occasionally use information technology assets for limited incidental personal use during non-working time.

3.5.5. Such personal use may be acceptable if other usage policies are followed, the use does not result in additional University expense, and the use does not interfere with a User's work or negatively impact the information technology assets productivity, such as through large attachments or audio/video segments.

3.5.6. The following are examples of incidental personal uses of the information technology assets.

a) Sending and receiving necessary or occasional personal communications;

b) Using voice communications for occasional and brief personal calls; and

c) Accessing the Internet for brief personal searches and inquiries, provided Users adhere to all other usage policies.

3.6 Impermissible Uses

Unless specifically included in section 3.3, the following activities are expressly prohibited on University information technology assets and electronic communication platforms. Refer to section 3.3 for exceptions.

3.6.1. Using information technology assets to create a hostile learning or work environment that unreasonably interferes with the ability of a person to

a) Perform employment responsibilities, or

b) participate in academic activities or programs.

3.6.2. Engaging in immoral, illegal, or unlawful activities, violating the policies and procedures of the University, or encouraging others to do so. Examples include, but are not

limited to the following.

a) Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned User accounts, valid passwords, file permissions, or other legitimate access and authentication methods.

b) Granting another individual access to any University accounts authorized to the User or using another individual's account or credentials.

c) Viewing, uploading, printing, copying, filing, transmitting, downloading, or searching for illegal or otherwise objectionable non-business-related web content.

d) Accessing other Users' folders, files, work, networks, or computers without express permission.

e) Intercepting communications intended for others.

f) Downloading or transmitting the University's confidential information without proper authorization.

3.6.3. Transmitting Confidential or Restricted university information using unsecured networks and systems. This includes, but is not limited to, unencrypted transmission methods and unencrypted email.

3.6.4. Online gambling.

3.6.5. Stocks, bonds, and securities trading.

3.6.6. Using the network, email, or Internet for commercial activities.

3.6.7. Using the network, email, or Internet for the purpose of supporting candidates for public office in a partisan election; using official authority or influence to interfere with or affect the results of an election or nomination; directly or indirectly coerce contributions from subordinates in support of a political party or candidate; using the network or Internet for disseminating political campaign material to another employee.

3.6.8. Using the network, email, Internet, or other University information technology assets for personal gain such as selling access to the network, or by performing work for profit with University resources in a manner not authorized by the University.

3.6.9. Vandalizing or using the network to disrupt network Users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of viruses, harmful components, or corrupted data.

3.6.10. Deliberately or intentionally destroying or manipulating files or emails inconsistent with the General Records Retention Schedule for State Colleges and Universities in South Carolina.

3.6.11. Attempting to circumvent or subvert system or network security measures.

3.6.12. Intercepting network traffic for any purpose unless engaged in authorized network administrative duties.

3.6.13. Making or using illegal copies of copyrighted software or content, storing such copies on University information technology assets, or transmitting them over University networks.

3.6.14. Using any information technology assets in the commission of a crime.

3.6.15. Using, transmitting, receiving, or seeking suggestive, offensive, inappropriate, fraudulent, vulgar, profane, obscene, pornographic, abusive, harassing, belligerent, threatening, defamatory, or misleading language or materials. Displaying any kind of sexually explicit image or document on any University-owned information technology assets.

3.6.16. Using or installing software not licensed or approved by the University's Computing and Information Technology Department.

3.6.17. Installing or using hardware or peripheral equipment not specifically approved and authorized by the University's Computing and Information Technology Department or using approved equipment in a manner inconsistent with the approved purpose for which the equipment was installed.

3.6.18. Encouraging others to view, download, or search for materials, files, information, software, or other vulgar, profane, obscene, defamatory, misleading, infringing, or illegal content.

3.6.19. Sending, soliciting, printing, or copying any of the following:

3.6.19.1. Text, images, or jokes (text or images), that disparage others based on their race, color, religion, sex, national origin, age, protected disability, veteran status, sexual orientation, gender identity, or other characteristic protected under federal, state, or local law.

3.6.19.2. Messages or images that are defamatory, alarming or may imply a threat, defame the University, or negatively impact student or employee productivity.

3.6.19.3. Sexually oriented messages or images.

3.6.19.4. Images that contain foul, obscene, or adult-oriented language.

3.6.20. Using a User's University e-mail address to register for personal email subscriptions, publications or notifications. The sharing of University e-mail addresses make the company susceptible to phishing attempts, spam, and other security breaches.

3.6.21. Using a personal e-mail address or electronic account to conduct University business.

3.6.22. Forwarding messages from University e-mails to personal e-mail accounts or otherwise outside of the University's information technology assets. Forwarding e-mails to third parties as necessary and appropriate to carry out User's assigned job responsibilities is permitted.

3.7 Lost or Stolen Devices

All Users are responsible for reporting lost or stolen information technology assets to the IT department. Users must report lost or stolen information technology assets to the Service Desk as soon as possible, and always within 12 hours of the last known possession of the device. Service Desk at servicedesk@winthrop.edu or call 803/323-2400.

3.8 Policy Compliance

All Users are responsible for complying with this policy and established information technology standards and procedures. Users are responsible and accountable for all activity initiated or conducted through assigned access credentials. Violation of any portion of this policy may result in immediate loss of access to University information technology assets, initiation of legal action by the University, and/or disciplinary action according to employee and student discipline policies.

3.8.1. Additionally, the University may suspend access to its information technology assets at any time for technical reasons or for any other reason the University deems necessary.

3.8.2. If Users find that they have inadvertently or accidentally connected to a website that contains offensive material, they must immediately disconnect from the website.

3.9 Policy Infractions

Failure to comply with the terms of this policy may:

a) result in the termination of access to University information systems and resources,

b) subject the employee to disciplinary action,

c) be grounds for the termination of vendor access or in some cases, termination of the contract with the University, and

d) result in the reporting of potentially illicit or criminal behavior by Users to the proper authorities for prosecution.

3.10 Reporting policy violations or inappropriate use of University information technology assets.

3.10.1. Violations of the Acceptable Use Policy or any inappropriate use of information technology assets should be reported to the Assistant Vice President for Computing and Information Technology (803) 323-2148 or the Vice President for Finance and Business Affairs (803) 323-2205.

3.10.2. Non-Users engaged in improper access and use of University information technology assets will be reported to the proper authorities and fully prosecuted.

3.11 Reporting Potential Incidents.

3.11.1. Users are responsible for immediately reporting any actual or suspected violation of this policy to the University's Computing and Information Technology Department.

3.11.2. If Users receive e-mail that contains offensive material, they should immediately report the email to the Service Desk. Service Desk at servicedesk@winthrop.edu or call 803/323-2400.

4. Procedures:

This section was intentionally left blank.

5. Resources:

This section was intentionally left blank.

WINTHROP UNIVERSITY

6. History of Revisions:

11/20/2024	Various Revisions
01/01/1996	Policy first established