WINSTON-SALEM STATE UNIVERSITY

ACCEPTABLE USE OF COMPUTING & INFORMATION RESOURCES POLICY

I. EXECUTIVE SUMMARY

The Acceptable Use of Computing and Information Resources Policy (AUP) purpose is to help ensure an information infrastructure that supports the core missions of the University of teaching, learning, and research. Users of Winston-Salem State University (WSSU) information resources must respect copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource users.

II. POLICY STATEMENT

This policy covers the appropriate use of all WSSU information resources including computers, networks, and the information contained therein. Information resources are powerful enabling technologies for accessing and distributing the information and knowledge developed at the university and elsewhere. As such, they are strategic technologies for the current and future needs of the university. The AUP codifies what is considered appropriate usage and the responsibilities every user has with the use of WSSU information resources.

III. GUIDELINES

All individuals granted access to, or use of WSSU information resources must be aware of and agree to abide by the following acceptable use requirements.

a. General
    i. University Information Resources are provided for conducting the business of WSSU. However, Users are permitted to use University Information Resources for use that is incidental to the User's official duties, as permitted by this policy, if the following restrictions are followed:
        1. The use is lawful under federal or state law.
        2. The use is not prohibited by Board of Governors, University or departmental policies.
        3. The use does not overload the University computing equipment or systems, or otherwise, harm or negatively impact the system's performance.
        4. The use does not result in commercial gain or private profit or advertising on behalf of non-University organizations (other than allowable under University intellectual property policies).
        5. The use does not violate federal or state laws or University policies on copyright and trademark.
        6. The use does not state or imply University sponsorship or endorsement.

7. The use is not used for political activities where prohibited by University policy or federal or state laws.
8. The use does not violate state or federal laws or university policies against race or sex discrimination, including sexual harassment.
9. The User does not send, view or download fraudulent, harassing, obscene, threatening messages or material - including but not limited to cyberstalking, cyberbullying, threats of violence, obscenity, child pornography – that might contribute to the creation of a hostile academic or work environment. This provision applies to any electronic communication distributed or sent within the University Network or to other networks while using the University Network.
10. The use is not for chain letters, personal advertisements, or solicitations.
11. The use does not involve unauthorized passwords or identifying data that attempts to circumvent system security or in any way attempts to gain unauthorized access or attempt to bypass network security mechanisms.
12. The use does not involve the access or storage of sexually explicit materials that cannot be associated with instruction or research activities unless (1) such use is specific to work-related functions and has been approved by the respective manager or (2) such use is specifically related to an academic discipline or grant/research project.
13. The use of any Peer to Peer application (downloading of movies, music or other copyrighted material) by faculty, staff or students is prohibited on any University owned computers and information resources unless approved by the Office of Information Technology.

ii. Users have no expectation of privacy regarding any University Data residing on University owned computers, servers, networks, or other Information Resources belonging to, or held on behalf, of University. University may access and monitor its Information Resources for any purpose consistent with University's duties and/or mission without notice.
iii. Users have no expectation of privacy regarding any University Data residing on personally owned devices, regardless of why the Data was placed on the personal device.
iv. Users must clearly convey that the contents of any email messages or social media posts that are the result of incidental use are not provided on behalf of the University and do not express the opinion or position of University. An example of an adequate disclaimer is: "The views expressed are my own, and not necessarily those of my employer, Winston-Salem State University."
v. Users may not extend or share with public or other users the University Network beyond what has been configured accordingly by the Office of Information Technology (OIT). This includes connecting any network

Commented [BI1]: Camille may have some input on the EEO language

devices or systems to the University Network without prior consultation and approval by OIT.

vi. Users should report misuse of University Information Resources or violations of this policy to their supervisors or the OIT Information Security Officer at security@wssu.edu.

b. Email

i. Emails sent or received by Users in the course of conducting University business are University Data that are subject to state records retention and security requirements.

ii. Users are to use University provided email accounts, rather than personal email accounts, for conducting University business and communicating with students.

~~iii. Users should not click on suspicious links or attachments, especially from unknown sources.~~

~~iv.~~iii. The following email activities are prohibited when using a University provided email account:

1. Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
2. Accessing the content of another User's email account except
   a. as part of an authorized investigation,
   b. as part of an approved monitoring process,
   c. for other purposes specifically associated with the User's official duties on behalf of University.
3. Sending or forwarding any email that is suspected by the User to contain computer viruses.
4. Any Incidental Use prohibited by this policy.
5. Any use prohibited by applicable University policy.

c. Confidentiality & Security of Data

i. Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users must not attempt to access data on systems they are not expressly authorized to access.

ii. Users shall not disclose Confidential Data except as permitted or required by law and only as part of their official duties.

iii. Whenever feasible, Users shall store Confidential Information or other information essential to the mission of University on a centrally managed server, rather than a local hard drive or portable device.

iv. In cases when a User must create or store Confidential or essential University Data on a local hard drive or a portable device such as a laptop computer, tablet computer, or, smartphone, the User must ensure the data is encrypted in accordance applicable requirements.

v. The following University Data must be encrypted during transmission over an unsecured network: Social Security Numbers; personally identifiable Medical and Medical Payment information; Driver's License

Commented [BI2]: Should or may? Are we disciplining because someone knows but does not report?

Commented [CR3]: Changed to should…

Commented [BI4]: This is subjective; not necessariliy wrong, but subjective. "Suspicious" can vary by the User.

Commented [CR5]: Recommend removing, was inserted based on conversation with Gartner.

Commented [BI6]: I changed it to lower case before to make it generic, but it can be capitalized if Incidental Use is defined somewhere

Commented [CR7]: Added definition to policy.

Numbers and other government issued identification numbers; Education Records subject to the Family Educational Rights & Privacy Act (FERPA); credit card or debit card numbers, plus any required code or PIN that would permit access to an individual's financial accounts; bank routing numbers; and other University Data about an individual likely to expose the individual to identity theft. The Office of Information Technology will provide tools and processes for Users to send encrypted data over unsecured networks to and from other locations.

vi. Users who store University Data using commercial cloud services must use services provided or sanctioned by WSSU, rather than personally obtained cloud services.

vii. Users must not use security programs or utilities except as such programs are required to perform their official duties on behalf of University.

viii. All computers connecting to a University's network must run security software prescribed by the Information Security Office as necessary to secure University Resources properly.

ix. The University may immediately disconnect devices determined by University to lack required security software or to otherwise pose a threat to University Information Resources from a University network without notice.

x. All material prepared and utilized for work purposes and posted to or sent over University Information Resources must be accurate and must correctly identify the creator and receiver of such. Any creation of a personal home page or a personal collection of electronic material that is developed for academic purposes and/or student organizations and is accessible to others must include a disclaimer that reads as follows: "This is a personal web page. Opinions or views expressed are those of the author and do not represent the official views of Winston-Salem State University."

xi. Users must respect the integrity of information resources. Users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others, without proper authorization.

d. Copyright and Licenses

Users must respect copyrights and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.

i. Licensed Software

Most software is available for use on computers at Winston-Salem State University is protected by the United States Copyright Law of 1976, as amended. Educational institutions are not exempt from the laws covering copyrights. Also, software is protected by a license agreement between the purchaser and the software seller. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses. It is the policy of the University to respect the copyright protection given to

software owners by federal law. It is against University policy for faculty, staff or students to copy or reproduce any licensed software on University computing equipment, except as expressly permitted by the software license. Also, faculty, staff, and students may not use unauthorized copies of software on University-owned computers or personal computers housed in University facilities. Unauthorized use of the software is regarded as a serious matter, and any such use is without the consent of Winston-Salem State University and subject to disciplinary action.

ii. Downloading of Music, Movies & Other Copyrighted Material
Use of any Peer to Peer application (downloading of movies, music or other copyrighted material) by faculty, staff or students is prohibited on any University owned computers unless approved by the CIO or their designee. Students are prohibited from configuring their personal systems to participate in the hosting of files for access by Peer to Peer applications. If the application cannot be reconfigured to disable hosting, it must be removed from the computer. IT IS THE SOLE RESPONSIBILITY OF THE STUDENT TO DISABLE THIS FUNCTION BEFORE CONNECTION TO THE UNIVERSITY'S NETWORKS. If identified by internal security mechanisms or if an artist, author, publisher, the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), or a law enforcement agency notifies the University of a violation of copyright laws, the Office of Information Technology will provide to the Office of Legal Affairs and the Vice Chancellor for Student Affairs information in the form of Internet Protocol (IP) address information, MAC address, appropriate log entries, location of computer, and any identifying information needed to assist in the investigation of the complaint or in response to a court order for identification of the user. The Office of Legal Affairs will advise any user identified under a lawfully ordered subpoena of the date for submitting identifying information to the court or the attorney designated in the subpoena. Neither the Office of Legal Affairs nor the North Carolina Attorney General can represent any employee or student identified who has illegally downloaded copyrighted material.

e. Portable and Remote Computing

i. All electronic devices including personal computers, smartphones or other devices used to access, create or store University Information Resources, including email, must be password protected by University requirements, and passwords must be changed whenever there is a suspicion that the password has been compromised.

ii. University Data created or stored on a User's personal computers, smartphones or other devices, or in databases that are not part of University's Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University Information Resources

iii. University issued mobile computing devices must be encrypted.

iv. Any personally owned computing devices on which Confidential University Data is stored or created must be encrypted.
v. University Data created and/or stored on personal computers, other devices, and/or non-University databases should be transferred to University Information Resources as soon as feasible.
vi. Unattended portable computers, smartphones, and other computing devices must be physically secured.
vii. All remote access to networks owned or managed by University must be accomplished using a remote access method approved by OIT.

f. Password Management
   i. University issued or required passwords, including digital certificate passwords, Personal Identification Numbers (PIN), Digital Certificates, Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes shall be maintained securely and shall not be shared or disclosed to anyone.
   ii. Each User is responsible for all activities conducted using the User's password or other credentials. Sharing of user passwords is not permitted.

g. Locally Defined and External Conditions of Use
   i. Individual units within the University may define "conditions of use" for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Where the use of external networks is involved, policies governing such use also are applicable and must be adhered.
   ii. A User's incidental personal use of Information Resources does not extend to the User's family members or others regardless of where the Information Resource is physically located.

h. Application of Public Records Law
   i. All information created or received for work purposes and contained in University computing equipment files, servers or electronic mail (e-mail) depositories are public records and are available to the public unless an exception to the Public Records Law applies. This information may be purged or destroyed only by the University records retention schedule and State Division of Archives regulations.

i. Consequences of Misuse of Computing Privileges
   i. Any violation of this policy by a University student is subject to the Student Code of Conduct in the Student Handbook.

ii. For employees, any violation of this policy may be "misconduct" under EHRA policies (faculty and EHRA non-faculty) and "unacceptable personal conduct" under SHRA policies, including any appeal rights stated therein.
iii. Violations of law may also be referred for criminal or civil prosecution.
iv. Violations of this policy may result in termination or suspension of access, in whole or in part, to University information systems at the discretion of OIT where such action is reasonable to protect the University or the University information infrastructure.
v. The University, in consultation with its legal counsel, may also refer suspected violations of applicable law to appropriate law enforcement agencies to investigate any matter at its sole discretion.

Commented [BI8]: "is" or "may be"? Consider the way iii is written about how violations of law may be referred for prosecution.

Commented [CR9]: Changed to 'may be'

IV. APPLICABILITY

The AUP applies to all active members of the University community, including faculty, students, staff, and affiliates, and to authorized visitors, guests, and others for whom University technology resources and network access are made available by the University. This policy also applies to campus visitors who avail themselves of the University's temporary visitor wireless network access service and to those who register their computers and other devices through Conference and Event Services programs or through other offices, for the use of the campus network.

V. COMPLIANCE

Users must acknowledge the terms of this policy prior to initial access is granted and afterward at least annually. Only users in compliance with this AUP are authorized to use and/or access University computing and information resources.

VI. DEFINITIONS

- **Confidential Data or Confidential Information:** All University Data that is required to be maintained as private or confidential by applicable law.
- **Incidental Use:** The personal use of information technology resources that do not relate to university employment or studies or to other activities involving and approved by the university, does not result in any measurable cost to the university, and benefits the university by allowing personnel to avoid needless inconvenience.
- **University:** Winston-Salem State University
- **University Information Resources**: All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf.
- **University Data:** All data or information held on behalf of University, created as result and/or in support of University business, or residing on University Information Resources, including paper records.
- ~~**Confidential Data or Confidential Information:** All University Data that is required to be maintained as private or confidential by applicable law.~~
- **User:** Any individual granted access to University Information Resources.

Formatted: Font: Bold

Formatted: Font: Not Bold

VII. RESPONSIBLE DIVISION

The Office of Information Technology

VIII. AUTHORITY
Board of Trustees

IX. HISTORY

Adopted: September 21, 2007
Amended: November 30, 2016

X. RELATED RESOUCES

WSSU Student Code of Conduct
WSSU Faculty Handbook
WSSU SHRA Employee Grievance Policy
WSSU EHRA Non-Faculty Employees

Effective Date: This policy becomes effective upon adoption.

_____

Chancellor
Winston-Salem State University

_____

Chair, Board of Trustees
Winston-Salem State University

_____

Secretary, Board of Trustees
Winston-Salem State University