HLC Accreditation 2020-2021

Evidence Document

WSU Policies and Procedure Manual

Chapter 19 / Technology

Additional information: See the web page at:
https://www.wichita.edu/about/policy/ch_19/ (Accessed March 8, 2021).

Wichita State University

WSU Policies and Procedures

Chapter 19 - Technology

- **19.01 / Acceptable Use**
  Effective: July 1, 2003 | Revised: June 17, 2016
- **19.03 / Internet Statement**
  Effective: July 1, 2003
- **19.04 / University Web Sites**
  Effective: July 24, 2003
- **19.05 / University Information Technology Resources and Email**
  Effective: March 17, 1998 | Revised: June 17, 2016
- **19.06 / Digital Millennium Copyright Act**
  Effective: December 1, 2001 | Revised: September 21, 2020
- **19.07 / Cell Phone Usage**
  Effective: June 6, 2003 | Revised: May 7, 2004
- **19.10 / Retirement of Computing and Information Technology Resources**
  Effective: March 15, 2005 | Revised: September 21, 2020
- **19.12 / Anti-Piracy**
  Effective: January 1, 2009
- **19.13 / Utilization of University Network**
  Effective: May 1, 2009
- **19.15 / Software Copying**
  Effective: July 1, 1997
- **19.16 / Text Messaging While Driving**
  Effective: August 13, 2019

19.01 / Acceptable Use

Effective: July 01, 2003 Revised: June 17, 2016

I. Purpose

The purpose of this statement is to set forth guidance and policy with regard to acceptable use standards for University computing and information technology resources.

For purposes of this policy, University computing and information technology resources are used for the electronic transmission of information, and, include, by way of illustration and not limitation, telecommunications, wireless transmissions, all equipment (including laptop computers), software, networks, Internet access, data and modems provided by or otherwise made available through Wichita State University, whether leased or owned, and located in university libraries, computing centers, college and departmental computer labs, public access computers in student residence halls and remote centers.

II. Preamble

As a state educational institution, Wichita State University seeks to provide a learning environment that encourages the free exchange of ideas and the sharing of information. Such an environment includes usage of up-to-date computing and information technology resources providing access to local, national and international information sources. Access to University computing and information technology resources is a privilege and Wichita State University expects all users to use such resources in a responsible manner. This statement is intended to set forth University policy relative to such expected responsible usage.

III. Policy

A. The following policies, rules and conditions apply to all users of Wichita State University's computing and information technology resources (hereinafter "Users"). Additional policies from departmental systems within the University may also apply. Violations of these policies are unacceptable, unethical and possibly unlawful. Violations may result in disciplinary measures that may include immediate revocation of access, termination of employment or student status and/or legal action. (Access to the WSU Ethernet backbone is provided for the use of currently enrolled students, currently employed faculty and staff, and certain other designated affiliated users. Others shall be allowed limited access

to certain computing and information technology resources, i.e., library computers and remote access to the public components of the network, provided that said resources are used for academic purposes deemed to further the mission of the University.)

B. Computing and information technology resources provided by Wichita State University are made available to students, faculty, staff and others primarily as tools for enhancing and facilitating learning, teaching, scholarly research, communications and the operation and administration of the University. Uses which are not directly related to these purposes will be considered secondary activities and should such secondary activities in any way interfere with the activities primary to the operations of Wichita State University, they may be terminated immediately.
C. Computing and information technology resources are the property of Wichita State University and should be used for the primary purpose of benefiting, enhancing and furthering the mission of the University.
D. For the benefit of those using University computing and information technology resources, and to facilitate the protection of those computing and information technology resources and the security of information contained therein, all users of University computing and information technology resources (as defined in footnote 1) shall be required to complete a minimum of one (1) training session relating to the usage of said resources every twelve (12) months. Failure to complete such minimum training requirements will result in the loss of the privilege of access to, and use of, University computing and information technology resources.
E. University computing and information technology resources are to be used responsibly, ethically and legally. The University supports the rights of academic freedom and a campus and computing environment open to the free expression of ideas, including controversial or unpopular points of view. Employees must accept the responsibilities and limitations associated with such rights. The University will not limit access to any information based solely upon its content if said information meets any reasonable standard of legality. Prohibited communications include, but are not limited to, those that are libelous, obscene, threatening, that discriminate against or harass individuals protected by law or University policy or transmissions of child pornography.
F. Each User is solely responsible for the usage incurred at a workstation and individuals with an assigned account may not share the account or permit others to use. If the User believes that an unauthorized person[s] may have used the assigned account, the User should contact University Computing immediately. Users who intentionally abuse accounts and privileges, degrade system performance, misappropriate computer resources or interfere with the operation of the University's computing and information technology resources are subject to disciplinary actions pursuant to established University procedures, up to and including termination of employment or student status.

G. When an employee is terminated, resigns, retires, or is no longer performing duties on behalf of the University, access to administrative/informational systems, University provided devices and employee email will be terminated immediately. Access to online payroll history and tax related forms will be provided to the employee. In these instances, or when a University employee changes positions or moves to another University department or unit, the employee's supervisor will be given access to the computing and information technology resources provided to that employee. A University employee or the employee's supervisor, in consultation with Human Resources, may ask the University's Chief Information Officer to provide access to the employee's computing and information technology resources to someone other than the employee's supervisor.
H. Retired employees will have their firstname.lastname@wichita.edu email account closed. Retirees may request a Wichita State email address in the format of firstname.lastname@shockers.wichita.edu. No data will be transferred from the email account @wichita.edu to the @shockers.wichita.edu email account.
I. Users must abide by and comply with all applicable software licenses, WSU copyright and intellectual property policies, and applicable federal and state laws.
J. Users shall not intentionally seek, provide or modify information in files or programs, or obtain copies of files or programs belonging to other computer users without permission. This includes all system files and accounts.
K. An account and a password are intended as entrance keys to the University's computing and information technology resources. They should not be used by anyone other than the assigned user.
L. The University's computing and information technology resources are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, destructive programs, political material or other unauthorized purposes or uses.
M. Users should refrain from acts that waste University resources and from usage that prevents others from using the University's computing and information technology resources in accord with this policy.
N. Users shall not intentionally develop or use programs that infiltrate the University's computing and information technology resources and/or damage the software or hardware components of said resources.
O. University computing and information technology resources should not be used for private or commercial gain. The posting of chain letters, representing oneself electronically as another user, or configuring hardware or software to intentionally allow access by unauthorized users are prohibited and will lead to appropriate disciplinary action.
P. The use of the University's computing and information technology resources to send, upload, download, post, transmit or store fraudulent, harassing, sexually explicit or pornographic materials (unless reasonably related to a faculty

member's research), child pornography (as defined by state or federal law), profane, libelous, threatening, intimidating or other unlawful messages is specifically prohibited. Exceptions to this will be for the University Police Department or Office of General Counsel engaged in legal investigations. Faculty or researchers engaged with such content must contact Information Technology Services to provide a secure storage medium.

Q. Access to the University's computing and information technology resources at any given time cannot be and is not guaranteed. While reasonable efforts will be made to provide access, Users must understand that access will sometimes be down due to power failures, system testing, maintenance and other special circumstances as determined by Information Technology Services.

R. The University employs various measures to protect the security of its computing and information technology resources and its User's accounts. However, Users should be aware that the University cannot guarantee security and confidentiality and that their use of University computing and information technology resources is not completely private.

S. The storage of social security numbers and credit card information on University provided devices is prohibited. Storage of any personal information is discouraged. This is in an effort to minimize identity theft for University constituents (e.g. students, employees, community partners and affiliates) and to be compliant with credit card industry security protocols. The University's information technology personnel are required to perform electronic scans to identify and remove social security numbers or credit card data stored on University provided devices. Exceptions to this policy may be made only with the approval of the Chief Information Officer in consultation with the General Counsel.

T. Users should understand that delivery of email cannot be assured and that recovery of lost email may not be possible.

U. Users should understand that authorized University personnel must have access to email and related information stored on University computing and information technology resources. This access is required for reasons that include retrieving business-related information, trouble-shooting hardware and software problems, preventing unauthorized access and system misuse or abuse, assuring compliance with software distribution policies and complying with legal and regulatory requests for information.

V. Users should understand that while the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing and information technology resources require the backup and caching of data and communications; the logging of activity; the monitoring of general usage patterns; and other such activities that are necessary for the rendition of service. The University may also specifically monitor the activity and accounts of individual users of University computing and information technology resources, including individual login

sessions and the contents of individual communications, without notice to the User; provided, however, that any such individual monitoring must be authorized in advance by the University's Chief Information Officer in consultation with the University's General Counsel.

W. Users should understand that the University, in its discretion or as required by law, judicial or regulatory order, may disclose the results of any general or individual monitoring, including the contents and records of individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings.

X. Users should understand that communications made using University computing and information technology resources are considered to be non-confidential communications and that they should have no expectation of privacy regarding such communications. Such communications may be subject to disclosure through legal proceedings and/or may also be subject to access and disclosure pursuant to the Kansas Open Records Act.

Y. By using University computing and information technology resources, individuals and other entities agree to abide by all applicable policies and procedures adopted by the University, the Kansas Board of Regents, the state of Kansas, and the usage guidelines of other networks linked to the University's computing and information technology resources.

IV. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.03 / Internet Statement

Effective: July 01, 2003

I. Purpose

The purpose of this statement is to set forth University policy and to set forth various disclaimers regarding access to and usage of the Internet through University computing and information technology resources.

II. Preamble

Internet users should understand that the Internet is a developing electronic environment that may be insecure and unreliable. The ability of the University to provide access and services is totally dependent upon the Internet and equipment, software, systems, data and services provided by various telecommunications carriers, equipment manufacturers, firewall providers and encryption system developers and other vendors or third parties. Users of the University's computing and information technology resources should understand the developing nature of the Internet and must accept certain obligations and responsibilities for usage.

III. Policy

A. Wichita State University is not responsible and makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb or other such computer program.
B. Wichita State University is not responsible for the quality, accuracy or validity of information found on the Internet.
C. Wichita State University is not responsible for Internet materials accessible on the web.
D. Ultimate responsibility for Internet usage through University computing and information technology resources by individuals under the age of eighteen shall be with that individual's parent or guardian.

IV. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.04 / University Web Sites

Effective: July 24, 2003

I. Purpose

The purpose of this statement is to set forth University policy with regard to Web Sites and Servers affiliated with Wichita State University.

II. Preamble

The increased usage of the Internet and Web Sites as convenient and productive means of communicating information and as vehicles to relay and receive information requires that policies be developed to govern and enhance such usage relative to Web Sites affiliated with Wichita State University.

III. Policy

A. Definitions and Terminology for Purposes of this Policy

1. Advertising

   Promotional information provided in exchange for consideration, including, but not limited to, messages containing qualitative or comparative language, price information or other indication of savings or value; endorsements; or inducements to purchase, sell or use certain products or services.

2. Official University Web Sites

   Represent official views and opinions of the University, and display official web site certification. Official University Web Sites are hosted and maintained on Wichita State University servers.

3. Sponsorship

   Includes providing sponsor name, address, telephone numbers and Internet address; use of logos and slogans that do not contain comparative language; sponsor brand name or trade name; value-neutral description of sponsor product; or display of sponsor product.

4. Unofficial Web Sites

   Do not represent official views or opinions of the University and must carry a disclaimer. Examples of Unofficial Web Sites may include, but are not limited to: personal sites of faculty, staff, students and Wichita State University organizations.

5. Web Site

   A collection of linked web pages containing text, graphics, sound files, etc. residing on a web server.

6. Wichita.edu

   Registered Internet domain name owned and controlled by Wichita State University.

7. Wichita State University Servers

   Any web server owned and administered by Wichita State University.

B. Information Posted to Official University Web Sites (Wichita.edu)

1. Official University Web Sites (sites using "Wichita.edu") represent the official views and opinions of the University. Such sites will carry the following official certification:

   Certification of Official Status

   This Web Site is created and maintained by Wichita State University and is certified as an official Web Site of Wichita State University.

2. All official University Web Sites are hosted and maintained on Wichita State University Servers.
3.

C. Information Posted to Unofficial Web Sites

1. Unofficial Web Sites are the sole and exclusive responsibility of the author/creator. Such Unofficial Web Sites must display the following disclaimer:

Disclaimer of Official Status

This Unofficial Web Site is created and maintained by ***[insert name and email address]****. The views and opinions expressed on this site are strictly those of the site author/creator and in no way represent the views and opinions of the State of Kansas, the Kansas Board of Regents, or Wichita State University.*

2. Wichita State University is not responsible for links from Unofficial Web Sites to non-university Web Sites.

D. Hosting of Web Sites on Wichita State University Servers for External Entities

Web Sites for external entities such as professional associations, consortiums and/or academic or professional journals may be hosted on Wichita State University Servers only when the external entity has a relationship with Wichita State that supports the University's mission. Such a relationship may be demonstrated by one or more of the following criteria:

1. The University is a member of the external entity.
2. The external entity is an organization of which a member of the University faculty or staff is a member, and the appropriate department chair, director or vice president approves the hosting as being in support of the University's mission.
3. The University has a contractual obligation for the hosting of a Web Site for the external entity.
4. The President of the University or the President's designee determines that the external entity is one appropriate for the University to host that entity's Web Site.

E. Approval of Unofficial Web Sites on Wichita State University Servers

1. Web Sites related to professional activities of faculty, staff and/or affiliated corporations of the University may be hosted on Wichita State University Servers.
2. Applications for hosting such Web Sites must be registered with and approved by the University's Chief Information Officer.
3. An approved outside employment form covering the activity must be on file with the appropriate vice president, if applicable, as a component of the registration and approval process for Unofficial Web Sites.

F. Advertising, Underwriting and Recognition on Official University Web Sites

1. Official University Web Sites may not be used for commercial purposes, for personal financial gain or any other use inconsistent with this policy.
2. Unofficial Web Sites maintained on Wichita State University Servers may not contain Advertising.

3. A division, college, department, unit or program of the University may display information and provide links to sponsors that underwrite an activity to indicate Sponsorship.

G. Use of Marks, Logos and the University Seal

1. University marks, logos and the University seal may be used on Official University Web Sites. (See Use of the University's Name, Seal, Logos or Marks Policy at Section 20.11 of this manual.)
2. University marks, logos and the University seal may not be used on Unofficial Web Sites without permission. (See Use of the University's Name, Seal, Logos or Marks Policy at Section 20.11 of this manual.)

IV. Enforcement

A. The University maintains final and absolute discretion with regard to what appears on or in connection with Official University Web Sites or for Unofficial Web Sites that are maintained or accessed on Wichita State University Servers.
B. The University does not actively monitor content of Web Sites, but it does reserve the right to remove a web site from Wichita State University Servers reasonably determined to be in violation of federal, state or local law, or in violation or contradiction of any rules, policies, procedures or regulations of Wichita State University or the Kansas Board of Regents.
C. Users who violate this policy may be denied further access to University computing and information technology resources and may be subject to disciplinary action.
D. The University may temporarily suspend, block or restrict access to an account when it reasonably appears appropriate or necessary to do so to protect the integrity, security or functionality of University computing and information technology resources or to protect the University from liability.
E. The University may also refer suspected violations of applicable law to appropriate law enforcement or investigative agencies.
F. Enforcement of this policy shall be the responsibility of the Chief Information Officer.

V. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.05 / University Information Technology Resources and Email

Effective: March 17, 1998 Revised: June 17, 2016

I. Purpose

To state University policy with regard to the use of University information technology systems relative to email.

II. Preamble

Technology resources provided by Wichita State University are made available to students, faculty, staff and others primarily as tools for enhancing and facilitating teaching, learning, scholarly research, communications and the operation and administration of the University. Uses which are not directly related to these purposes shall be considered secondary activities and should such secondary activities in any way interfere with the primary activities, access to university technology resources may be terminated immediately. Access to and usage of such resources is a privilege and is not a right; it is therefore deemed appropriate and necessary that certain guidelines for the usage of the email component of the University's technology resources be set forth and explained.

III. Policy

A. Computers and other electronic media are the property of Wichita State University and should be used for the primary purpose of benefiting, enhancing and furthering the mission of the University.
B. By using University-supplied information technology facilities and resources, individuals and other entities agree to abide by all applicable policies and procedures adopted by the University, the Kansas Board of Regents, the state of Kansas, and the usage guidelines of other networks linked to the University's networks or computer systems.
C. By using University-supplied information technology facilities and resources, individuals and other entities agree to abide by and/or with current state and federal laws, including, but not limited to those relating to trademarks, service marks and copyright, defamation and discrimination.
D. Users should understand that email transmissions are considered to be non-confidential communications and that they should have no expectation of privacy regarding such communications. Email transmissions may be subject to

disclosure through legal proceedings or otherwise through various laws which may be held to apply to such transmissions.

E. Users should understand that authorized University personnel must have access to email and related information stored on University owned equipment. This access is required for reasons that include retrieving business-related information, trouble-shooting hardware and software problems, preventing unauthorized access and system misuse, assuring compliance with software distribution policies, and complying with legal and regulatory requests for information. The University's Chief Information Officer will be responsible for approving any such access.

F. Users should understand that individual access to the University's information technology resources may be terminated at any time due to a violation of this policy.

G. Users should understand that delivery of email cannot be assured and that recovery of lost email may not be possible.

H. Users should respect the right of privacy of others and email should not be used to harass, intimidate or interfere with the work of the recipients of email.

I. Users should refrain from acts that waste University resources and prevent others from using the University's information technology resources in accord with this policy.

J. Email should not be used for private (does not include or cover consulting activities pursued in accord with applicable University policies) or commercial gain, posting of chain letters, representing oneself electronically as another user, or configuring hardware or software to intentionally allow access by unauthorized users.

K. Users should understand that the University's information technology resources are intended to facilitate the work of the University and personal usage by Users should be limited and should not interfere with or delay University matters.

L. All University employees will be assigned an employee email address for University business use based on the following format: firstname.lastname@wichita.edu. First and last name may be modified in the case of multiple employees with the same name. Retired employees will have their firstname.lastname@wichita.edu email account closed. Retirees may request a Wichita State email address in the format of firstname.lastname@shockers.wichita.edu. No data will be transferred from the email account @wichita.edu to the @shockers.wichita.edu email account.

M. Users should understand that while the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing and information technology resources require the backup and caching of data and communications; the logging of activity; the monitoring of general usage patterns; and other such activities that are necessary for the rendition of service. The University may also specifically monitor the activity and accounts of individual users of University

computing and information technology resources, including individual login sessions and the contents of individual communications, without notice to the user, provided, however, that any individual monitoring must be authorized in advance by the University's Chief Information Officer in consultation with the University's General Counsel.

N. The use of email to send, upload, download, post, transmit or store fraudulent, harassing, sexually explicit or pornographic materials (unless reasonably related to a faculty member's research), child pornography (as defined by state or federal law), profane, libelous, threatening, intimidating or other unlawful messages is specifically prohibited.

IV. Implementation

The Chief Information Officer shall have primary responsibility for the publication and implementation of this University policy.

19.06 / Digital Millennium Copyright Act

Effective: December 01, 2001 Revised: September 21, 2020

I. Initiating Authority

The Chief Information Security Officer serves as the initiating authority.

II. Purpose

The purpose of this statement is to set forth University policy with regard to institutional responsibilities as an online service provider and claims of copyright infringement.

III. Policy

A. Wichita State University respects the rights of holders of copyrights, their agents and representatives and will implement appropriate policies and procedures to support these rights without infringing upon the legal use, by individuals, of those materials. Legal use can include, but is not limited to, ownership, license or permission, and fair use under the U.S. Copyright Act. Employees and students need to be aware of the rights of copyright owners. Information on copyright law and these rights can be found in a number of places, but general information can be found by going to the following sites:

1. Section 3.36, Copyright
2. Section 9.10, Intellectual Property Policy and Institutional Procedures

B. Persons who are found to intentionally or repeatedly violate the copyright rights of others may be denied access to all University computing and networking facilities and resources. All instances of reported copyright violations will be reported to the appropriate University authority in accordance with the following policies for possible additional disciplinary actions:

1. Section 4.06, Statements on the Professional Rights and Responsibilities of Faculty
2. Section 8.05, Student Code of Conduct
3. Section 19.01, Acceptable Use
4. Section 19.05, University Information Technology Resources and Email

C. The Designated Agent for complaints under the DMCA is:

Chief Information Security Officer
1845 Fairmount
Wichita State University
Wichita, KS 67260-0098
(316) 978-3456

D. A notice of alleged copyright infringement to the Designated Agent concerning information residing on the University's systems or networks at the direction of the user must have the following:
    1. A description of the works claimed to be infringed.
    2. A description of the allegedly infringing works or location site sufficient to enable the Designated Agent to find them.
    3. Sufficient information to enable the Designated Agent to contact the complaining party.
    4. A statement that the complaining party believes in good faith that the use of the material is not authorized by the copyright owner, the owner's agent, or the Copyright Act.
    5. A signed statement that the information provided by the complaining party in the notice is accurate and, under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner of one or more of the exclusive copyright rights.
    6. A physical or digital signature of the owner of an exclusive copyright right or the owner's authorized agent with accompanies the statement.

E. When properly notified of the potential copyright infringement, the Designated Agent will make a reasonable effort to contact the site or page owner of the materials in question. There will be an attempt to secure the voluntary take down of the work, but, if not, then the University will immediately disable access to the work unless it is immediately determined that the work is lawful under the copyright law. The owner of the site or page of the alleged infringing material may exercise their counter notice procedure rights set forth below. The Designated Agent may, but need not, undertake to determine if the work complies with copyright law.

F. After voluntary take down or the site is involuntarily disabled, the University may, but need not, proceed to counter notification on its behalf or on behalf of its employees and students, or the owner of the site may provide counter notification to the Designated Agent. Counter notices can claim only that either the copyright owner is mistaken and that the work is lawfully posted or that the work has been misidentified. A site owner may assert that use of another's work is fair use, which falls under the provision that the copyright owner is mistaken in characterizing the work as infringing. Various University officials may be consulted in arriving at a fair use determination.

G. Counter notices to the Designated Agent must contain the following:
    1. A physical or digital signature of the site or page owner.
    2. A description of the materials removed and its location before it was removed.
    3. A statement that the owner believes in good faith that the material was removed by mistake because the work is not infringing or that it was misidentified.
    4. Sufficient information to enable the Designated Agent to contact the owner who is filing the counter notice, e.g., name, address, phone number, email address, and his or her consent to jurisdiction of the federal district court with proper jurisdiction for any court actions arising from the infringement.
    5. A statement that the owner will accept service of process from the complaining party.

H. Access to the materials in question will be restored within ten to fourteen business days after the date the Designated Agent receives the counter notice unless the Designated Agent first receives a notice from the complaining party that he or she has filed an action seeking a court order to restrain the page owner.

I. The Designated Agent will promptly send a copy of any substantially conforming counter notice to the complaining party indicating that the site will be restored within ten to fourteen business days unless the Designated Agent receives a notice of court action.

IV. Possible Penalties For Violating WSU Copyright Policies Or Copyright Law

Wichita State University prohibits the unauthorized distribution of copyrighted materials, including the use of peer-to-peer (P2P) networks. Members of the University community who use these networks to share copyrighted media files are subject to appropriate disciplinary action or sanction ranging from loss of access to the relevant University services or property (including computing privileges) to dismissal or removal from the University as determined by applicable employment or student disciplinary policies. In addition, unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject a student or employee to serious civil and criminal liabilities (e.g., 17 U.S.C. 504, et seq.). Some of these liabilities include, but are not limited to the following:

A. Civil penalties of actual damages suffered by the copyright owner from the infringement; or
B. Civil penalties of statutory damages of up to $30,000.
C. Civil penalties for willful infringement of up to $150,000, and

D. Criminal penalties for willful criminal infringement from 1 to 5 years of imprisonment and fines of up to $250,000 per offense.

V. Applicable Laws And Additional Resources

A. 17 U.S.C. 101 et seq./U.S. Copyright Act
B. WSU Policy 3.35/Copyright
C. WSU Policy 9.10/Intellectual Property
D. WSU Policy 4.06/Statements on the Professional Rights and Responsibilities of Faculty
E. WSU Policy 8.05/Student Code of Conduct
F. WSU Policy 19.01/Acceptable Use
G. WSU Policy 19.05/University Information Technology Resources and Email

VI. Implementation

A. This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.
B. The General Counsel shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.07 / Cell Phone Usage

Effective: June 06, 2003 Revised: May 07, 2004

I. Purpose

The purpose of this statement is to set forth University policy with regard to the use of cellular phones.

II. Preamble

As a state educational institution of Kansas, Wichita State University must be concerned about the appropriate usage of state resources and about the safety of its employees and others who perform services for the University. With the increasing prevalence of cellular phone usage, this policy statement is intended to provide information and guidance about University expectations regarding such usage.

III. Policy

A. Usage of a state-provided cellular phone is a privilege and is provided to improve University operations and service and to enhance operating efficiencies. It is intended that a state-provided cellular phone be used for business purposes only.
B. Use of a state-provided cellular phone should not be a primary mode of communication, but should be used only when such usage is the most cost-effective way to conduct state business. The telephone card provided by the University is the preferred method for long distance communications.
C. Justification for a state-provided cellular phone is left to the determination of department heads or budget officers with the understanding that regular audits by the state of Kansas are to be expected. No University employee may approve his/her own service plan for a state-provided cellular phone.
D. More than minimal personal usage of a state-provided cellular phone without advance written authorization from the appropriate Vice President or the President is not allowed. Employees must confirm review of the monthly statement by signing the final page of the statement/invoice and will reimburse the University for all additional charges resulting from personal calls.
E. Misuse of a state-provided cellular phone will result in revocation of its use and forfeiture of the cellular phone**.**
F. Excessive use of a personal cellular phone for personal business during work hours is considered outside an employee's scope of employment.

G. Employees are not expected to use a personal cellular phone for official University business. Employees will not be reimbursed for the cost of using a personal cellular phone for official University business without the advance written authorization of the appropriate Vice President or the President.
H. Anyone operating a state-owned vehicle should not use a cellular phone while operating such vehicle.
I. Anyone using potentially hazardous equipment while working for the University should not use a cellular phone while operating such equipment.
J. Violation of this policy will be grounds for disciplinary action, up to and including termination. Such disciplinary action will be taken in accord with applicable University policies.

IV. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The General Counsel shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.10 / Retirement of Computing and Information Technology Resources

Effective: March 15, 2005 Revised: September 21, 2020

I. Initiating Authority

The Chief Information Security Officer serves as the initiating authority.

II. Purpose

The purpose of this statement is to set forth University policy with regard to required practices for retirement of University computing and information technology resources.

III. Preamble

It is an unacceptable practice for personal data and information to remain on University computing and information technology resources upon the cessation of use of those resources by a University department, office or group. Additionally, it may be a violation of a software license to permit software to remain on such resources upon their retirement.

IV. Policy

A. No University computing and information technology resources may be forwarded to the University Physical Plant Warehouse for salvage, sale or redistribution until and unless Information Technology Services or departmental technical personnel has determined that all data, information and/or software has been permanently deleted from said resources (in accordance with Department of Defense standards relating to deletion of information from computing and information technology resources).

B. All University computing and information technology resources forwarded to the University Physical Plant Warehouse for salvage, sale or redistribution shall be accompanied by a written statement that all data, information and/or software has been permanently deleted.

C. Data destruction will follow NIST 800-88 guidelines for media sanitization. The Chief Information Security Officer will be notified if NIST 800-88 guidelines cannot be utilized for media sanitization.

V. Implementation

A. This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

B. The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.12 / Anti-Piracy

Effective: January 01, 2009

I. Purpose

The purpose of this statement is to set forth University policy with regard to the unauthorized downloading and distribution of copyrighted material over the University's computing and information technology resources.

II. Preamble

The Higher Education Opportunity Act of 2008 requires that certain universities comply with specific anti-piracy provisions directed at the unauthorized downloading and distribution of copyrighted material over college and university computer networks.

III. Policy

The University shall, at least annually, inform students that the unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject them to criminal or civil liability and to discipline under the University's Student Code of Conduct. The annual advisory shall include, as a minimum, the following information:

A. A summary of the penalties for violation of federal copyright laws.
B. A review and description of University policies regarding unauthorized peer-to-peer file sharing utilizing the University's computing and information technology resources.
C. A review of the deterrents put in place by the University to combat the unauthorized distribution of copyrighted material.
D. A review of alternatives to illegal downloading that are offered by the University.

IV. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.13 / Utilization of University Network

Effective: May 01, 2009

I. Purpose

The purpose of this statement is to set forth University policy with regard to utilization of the University's network infrastructure.

II. Preamble

Because of security, utilization and operational requirements, it is necessary and appropriate that the University, acting through Information Technology Services (ITS), control usage of University computing and information technology resources with regard to what hardware/software is used; what data is transported; and what devices are connected to the University network infrastructure.

III. Policy

A. ITS shall supply and manage all wired and wireless computer networking equipment connected to the University network infrastructure. The connection of non-ITS-managed networking equipment, including, but not limited to, equipment to share a network connection with more than one device, is specifically prohibited.
B. ITS shall control and manage use of the University's network infrastructure addresses and names.
C. ITS shall support only current hardware/software platforms and the connection of older-version workstations to the University network infrastructure is prohibited.
D. Servers not registered and approved by ITS shall not be connected to the University network infrastructure.
E. The use of a virtual private network (VPN) connection is required to connect to campus PC's from off-campus.
F. The Chief Information Officer shall develop and enforce specific guidelines regarding the nature of data that can be moved to local devices and/or mobile devices.

IV. Implementation

This policy shall be included in the *WSU Policies and Procedures Manual* and shared with appropriate constituencies of the University.

The Chief Information Officer shall have primary responsibility for publication, dissemination and implementation of this University policy.

19.15 / Software Copying

Effective: July 01, 1997

I. Policy

Wichita State University endorses the Software Copying Policy developed by Educause, a nonprofit consortium of over 450 colleges and universities as follows:

"Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to work of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

II. Background

Some related background as provided by Educause relative to software copying are:

- Unauthorized copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors. Persons possessing illegal copies of software may be subject to legal action by the publisher.
- Unauthorized copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on campus, the institution may incur a legal liability.
- Unauthorized copying of software can deprive developers of a fair return for their work, increase prices, reduce the level of future support and enhancement, and inhibit the development of new software products.

19.16 / Text Messaging While Driving

Effective: August 13, 2019

I. Purpose

The purpose of this statement is to set forth University policy regarding text messaging while driving.

II. Preamble

Due to the safety risks associated with texting while driving, Kansas law prohibits text messaging while operating a motor vehicle. Because many University employees are required to operate a motor vehicle in the course of their employment, this policy statement is intended to provide information and guidance about the University's expectation about text messaging while driving.

III. Policy Statement

A. Text Messaging Prohibited

Employees shall not engage in "text messaging" on a personal or state-provided cellular phone when:

1. driving a state owned, leased, or rented vehicle;
2. performing University work or on University business while driving a privately-owned vehicle, or
3. using any equipment supplied by the state or federal government while driving.

B. Text Messaging Defined

For purposes of this policy, "text messaging" means reading from or entering data into any handheld or other electronic device, including for the purpose of short message service texting, e-mailing, instant messaging, obtaining navigational information, or engaging in any other form of electronic data retrieval or electronic data communication. The term does not include glancing at or listening to a navigational device that is secured in a commercially designed holder affixed to the vehicle, provided that the destination and route are programmed into the device either before driving or while stopped in a location off the roadway where it is safe and legal to park.

C. Exceptions

This policy shall not apply to:

1. The use of a device which is voice-operated and which allows the user to send or receive a text message without the use of either hand, except to activate or deactivate a feature or function; or
2. A law officer or emergency service personnel acting within the course and scope of the law enforcement officer's or emergency service personnel's employment.

D. Consequences of Violation. Violation of this policy will be grounds for disciplinary action, up to and including termination. Such disciplinary action will be taken in accord with applicable University policies.

IV. Implementation

This policy shall be included in the WSU Policies and Procedures Manual and shared with appropriate constituencies of the University.

The General Counsel shall have primary responsibility for publication, dissemination and implementation of this University policy.

V. Applicable Laws

- FAR 52.223-18
- KSA 8-15,111; 8-296 & 8-2,101
- Wichita Ord. No. 48-806, § 1
- VI. Policy Owners
- Federal Contracts Compliance, Research Compliance