WICHITA STATE UNIVERSITY

WSU Policies and Procedures

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.