POLICY & PROCEDURE DOCUMENT

NUMBER: 5.5023

DIVISION: Information Technology

TITLE: Information Technology Acceptable Use Policy

DATE: April 15, 2013

REVISED: September 15, 2013; November 3, 2014; July 1, 2016

AUTHORIZED: Gordon Johnson, VP for Information Technology

I. Purpose and Scope

The purpose of this policy is to define and set forth the standards of conduct and acceptable use regarding WKU Information Technology resources. This policy is in force in conjunction with the Kentucky Commonwealth Office of Technology's (COT) Acceptable Use Policy (referenced below) which applies to all state institutions and agencies. While the KY COT policy specifically deals with acceptable use of Internet and email, this policy augments and expands the scope of the COT policy to include any and all WKU Information Technology resources.

CIO-060 – Commonwealth Office of Technology
Internet and Electronic Mail Acceptable Use Policy
http://gotsource.ky.gov/docushare/dsweb/Get/Document-5282/

II. Policy

The general standards of conduct expected of a member of this educational institution also apply to the use of WKU information technology resources. These resources include networks, systems, services, applications and any respective hardware, software, and data associated with such. It is expected that users will cooperate with each other so as to promote the most effective use of resources and will respect each other's rights and property (tangible or intellectual). User(s) for purposes of this document refers to University employees, students, authorized affiliates, or any other valid constituency that utilizes WKU information technology resources.

WKU information technology resources are the property of Western Kentucky University and are made available to authorized individuals to assist in the pursuit of activities necessary to the University's mission and operation. Personal use of such resources should be incidental and infrequent. University officials, upper management, or appointed delegate under the direction of University General Counsel, can access, seize, and/or commandeer any and all physical or electronic WKU resources as deemed necessary to address a given situation, in accordance with all applicable state and federal laws, regulations, court decisions; and Attorney General's opinions. Personally owned digital resources (i.e. resources purchased by an employee or a student) may not be seized without a court order. Users shall have no expectations of privacy associated with email transmissions or of other data, content, and information stored, transmitted, or accessed on University systems and resources.

Protection of Rights and Acceptable Use

The University seeks to protect the civil, personal, and property rights of those constituents utilizing its information technology resources and the confidentiality of University records stored on its computer systems from unauthorized access. Rules prohibiting theft or vandalism apply to software and data as well as to physical equipment. Prohibited conduct involving use of WKU Information Technology resources, includes but is not limited to the following:

- Invading the privacy of an individual by using electronic means to ascertain confidential information;
- copying or altering another user's software or data without permission;
- knowingly accepting or using software or data that have been obtained by illegal means;
- abusing or harassing another user through electronic means, as defined by applicable state and federal laws, regulations, and court decisions; and Attorney General's opinions;
- using the University's computing resources in the commission or attempted commission of a crime;
- accessing data residing on University systems not related to the user's responsibilities;
- intruding (hacking) into or attempting to intrude into University systems for the purpose of accessing or altering data or systems operations in any unauthorized manner;
- using another individual's accounts or credentials or providing one's computer identity to another individual so that individual can impersonate you;
- copying University-owned or licensed software or data to another computer system for personal or external use without prior written approval;
- attempting to modify University-owned or licensed software or data files without prior written approval by the employee responsible for its maintenance;
- attempting to damage or disrupt operation of any technology resources or services;
- allowing or enabling access by unauthorized persons, even if they are members of the University community;
- using WKU information technology resources in external consulting, except for occasional or incidental professional activities, unless approved in accordance with University procedures. When approved, such use is limited to the specific resources allocated for the purpose, and fees may be charged for such use;
- illegally obtaining or sharing copyrighted files outside of the "fair use" guidelines or without the author's permission;
- sharing copyrighted digital data or files, including but not limited to music, movies, software, and games without the consent of the copyright holder is against federal law and is expressly prohibited under this policy; and
- removing University owned technology equipment of any type from University premises without prior approval from the proper University management.

Accessing University Resources

WKU Information Technology resources are appropriately designed with capacity to handle expected levels of system and network access. Any conduct which jeopardizes system and network performance or compromises security is considered a misuse of information technology resources. Examples include:

- Operating an unauthorized/unregistered server connected to the campus network. See WKU policy 5.5010, Information Security Policy and related Information Security Plan.
- Conducting or attempting to conduct denial-of-service attacks in any form.
- Sending harmful computer viruses or malware of any type.
- Any intentional or unintentional activity that degrades the quality of the WKU information technology infrastructure.

Access to WKU information technology resources includes, but is not limited to, the Internet, email systems, learning management systems, ERP systems, online registration systems, network file storage systems, computer labs, website hosting, and wired and wireless network services. Use of these resources is a privilege that may be revoked at any time for inappropriate conduct. Examples of inappropriate conduct include:

- Using WKU information technology resources for personal gain or personal business activities in a commercial connotation such as buying or selling of commodities or services with a profit motive.
- Engaging in illegal activities or using the Internet for any illegal purposes, including initiating or receiving communications that violate any federal or state laws and regulations.
- Purposely accessing (or sharing) information which you are not authorized to access or which you have no legitimate business reason to access.
- Using abusive or harassing language in either public or private messages or content.
- Knowingly visiting pornographic or illegal sites; and/or disseminating, soliciting, or storing sexually oriented messages or images that are not required as part of educational requirements.
- Misrepresenting, obscuring, suppressing, or replacing a user's identity. This includes the use of false or misleading subject headers and presentation of information in the distribution of email.
- Sending or forwarding chain letters, phishing emails, spam emails, malware, or viruses.
- Distributing or forwarding unsolicited commercial email.
- Using WKU's email system, which is a resource of the University, for political campaign or solicitation purposes. Such use is prohibited, except for university elections.
- Copying, disseminating, or printing copyrighted materials (including articles, images, games, or other software) in violation of copyright laws.

Technology Accounts

Where pertinent, University constituents are issued credentials in order to access various information technology resources that require authentication. A user's account credentials constitute a unique identity that controls levels of access to University systems and networks. Users are required to manage their accounts securely, protect their account credentials at all times. Sharing one's account credentials is prohibited.

Websites on University Resources

Websites using University computing resources or utilizing the University Internet connectivity or web address domain (wku.edu) may only be used for instruction, research, public service, or administrative and professional purposes. Websites must follow the guidelines and policies set

forth by the **Office of Legislative and Public Affairs** (www.wku.edu/policies/legislative_pubaffairs.php).

With the exception of certain types of consulting which qualify as University public service, use of University computing resources to promote for-profit enterprise or activity is not acceptable. For instance, while faculty members who provide private consulting services related to their disciplines might briefly describe these on their personal or professional pages and provide information for direct personal contact, enterprises that fail to meet this definition should not be promoted through the University network. In no case would public description of specific service offerings and prices be appropriate on a University subsidized website or other system utilizing WKU information technology resources.

Individuals and organizations are expected to maintain their websites in an appropriate and professional manner. Any statement, act, or offer which could lead to criminal or civil action if made in public, over a telephone, or through the mail should be viewed as equally subject to legal action if made over the WKU network or Internet.

Violations

Any violation of this policy may lead to suspension of access to Information Technology resources, with the possibility of revocation of privileges, or other action as provided by disciplinary provisions applicable to faculty, staff, or students. Confirmed or suspected violations of local, state or federal laws will be turned over to the University General Counsel and/or the appropriate law enforcement agency.

III. Procedure

IV. Related Policies

5.501X Information Security Policy
5.501X Information Security Plan

V. Reason for Revision

Revised to make minor changes to grammar, spelling, and diction as part of an annual review process.

This policy was last reviewed on April 20, 2017.