POLICY & PROCEDURE DOCUMENT

NUMBER: 5.5054

DIVISION: Information Technology

TITLE: Privacy of Electronic Information Policy

DATE: April 15, 2013

REVISED: September 15, 2013; November 3, 2014; July 1, 2016; April 20, 2017

AUTHORIZED: Gordon Johnson, VP for Information Technology

I. Purpose and Scope

This policy specifically addresses the issues of privacy and confidentiality related to *electronic information and email.* This policy covers, but is not limited to, the following:

- Any information that is created, stored, or transmitted electronically including all electronic data; documents and files; electronic mail; telecommunications and voice mails; faxes; databases; web pages; information submitted online; information stored on individual computers or voice mail accounts, on University-owned systems, devices, networks, or other technology resources; and information on hosted or cloud systems contracted by the University.
- University administrative or academic data and other University files on personally owned devices.

Privacy policy and statement related to how WKU collects, stores, manages, and releases *personally identifiable information* (maintained in all forms, not limited to electronic) is contained in the University's **Information Security Plan** under the section "Privacy Statement" and is not the focus of this policy. However, the Privacy Statement in the **Information Security Plan,** together with this policy, addresses the overall issue of privacy policy at the University.

II. Policy

PRIVACY OF ELECTRONIC INFORMATION

The University takes reasonable precautions to preserve user privacy and to secure its systems, but the University cannot guarantee the security of electronic data stored, sent, or received on equipment, networks, or systems that are owned by or hosted for the University.

The handling and treatment of all University electronic data should be done in accordance with the rules and guidelines in the University's "Information Security Plan." It is the responsibility of all users of University technology resources to read, understand, and abide by the University's **Information Security Policy** and **Information Security Plan** which are available online on the University's policies website (www.wku.edu/it/policies).

Personal use of University systems of any type (e.g. email, file storage, or web servers) is discouraged. Incidental and infrequent use is allowed, but it should be understood that any information or files of a personal nature on University-owned equipment or resources are considered property of the University and the University is under no obligation to retain, maintain, or secure them or to make them available to individuals during or after their employment or official affiliation with the University.

AUTHORIZED ACCESS TO ELECTRONIC INFORMATION

On occasion it may be necessary for authorized personnel to access electronic mail, files, and data stored on the University's computers or networks, including cloud or hosted systems, to ensure the orderly administration and functioning of information resources. The University does not routinely monitor electronic mail, files, network traffic, or data. The University does use automated tools and utilities that either scan network traffic or scan the information on University managed servers for security purposes. The University reserves the right to access user data on the University-owned devices when the University determines such access is necessary and appropriate, in accordance with all applicable state and federal laws, regulations, court decisions, and Attorney General's opinions. Examples of necessary and appropriate access include, without limitation, the following purposes:

- Troubleshooting hardware and software problems;
- preventing or investigating unauthorized access and system misuse;
- retrieving information in emergency circumstances where there is a threat to health, safety, or University property or if there is substantial risk of harm or liability;
- retrieving a former employee's email and files by the unit to which the employee was assigned, as necessary (e.g., to respond to students, customers, and vendors who may continue to send emails to that address);
- retrieving email and files of a deceased or incapacitated employee;
- providing access to email and files to a lawful representative (e.g., spouse, parent, executor, holder of power of attorney) of a deceased or incapacitated employee or student;
- investigating reports of violation of University policy or local, state, and federal law;
- investigating reports of employee or student misconduct; and
- complying with legal requests for information (such as subpoenas).

When accessing user data, the University will make reasonable efforts to notify the affected user except when such notification may be inappropriate, impractical, or unlawful.

Email System of Record

The WKU email systems (providing accounts ending in @wku.edu and @topper.wku.edu) shall constitute the official email systems of record. As such, all official University business requiring the use of email shall use the WKU email systems.

Email Record Retention

For purposes of e-discovery related to potential litigation, all student email is archived for a period of one year and all employee email is archived for a period of three years.

III. Procedure

IV. Related Policies

5.501X Information Security Policy
5.501X Information Security Plan

V. Reason for Revision

Revised to address retention, maintenance, and security of personal files and information. Also added date of last review.

This policy was last reviewed on June 28, 2018.