WILLIAMSON
COLLEGE of the TRADES
Founded 1888

July 1, 2017

Office of the Senior Vice President/Chief of Staff

Policy Letter: Information Technology

Williamson's Information Technology Policy promotes the efficient, ethical, and lawful use of the college's information technology (IT) resources. The college's computing systems, networks, and associated facilities (*TRADEnet*) are intended to support its mission and to enhance the educational environment of its students. Any use deemed inconsistent with this mission will be considered a violation of this policy.

This policy applies to anyone who uses the college's IT resources. The resources covered by this policy include, but are not limited to computer hardware and software; mobile communication devices; telephone and data networks; and electronically stored data. Use of these resources includes access from off campus and on campus, as well as access from privately owned computers and electronic devices.

Rights & Responsibilities

Access to and use of Williamson IT resources and the Internet shall comply with federal laws, the laws of the Commonwealth of Pennsylvania, and the policies and procedures of the college. By use of the college's IT resources (including but not limited to computers, network, phones, tablets, etc.), all users agree to the rules, regulations, and guidelines contained in this policy. Computers and networks provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a revocable privilege and requires that individual users behave ethically and act responsibly. IT resources are primarily designated for instructional or administrative purposes. The college's IT resources are shared for use by all employees and students. Any activity that inhibits or interferes with the use of these resources by others is not permitted.

Users are responsible for all activities to and from their access accounts. Users must take every precaution to protect access accounts. Under no circumstances should a user allow someone else to share an access account or password. Users should change passwords whenever there is any indication of possible system or password compromise.

Users must satisfy the licensing requirements for all software installed or used on college IT resources (e.g. commercial software requiring a valid license for each user, etc.).

Users should not assume or expect any right of privacy with respect to the college's IT resources. While Williamson does not routinely monitor the communication of its employees or students, system

administrators or other authorized personnel may access or examine files or accounts that are suspected of unauthorized misuse, that have been corrupted or damaged, or that may threaten the integrity of the college's IT systems. In addition, files, e-mail, access logs, and any other electronic records may be subject to search under court order.

Prohibited Use of Information Technology Resources

It is a violation of this policy to:

A. Intentionally and without authorization, access, modify, damage, destroy, copy, disclose, print, take possession of, or disrupt in any way all or part of any computer, computer system, network, software, data file, program, database, or any other IT resource. This includes:

    1. Gaining access by willfully exceeding the limits of authorization

    2. Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means

    3. Gaining access by using another person's name, password, access codes, or personal identification

    4. Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes

    5. Attempting to disrupt any resource from being available to other users

B. Give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, network or e-mail account, database, or any other IT resource. All users must identify themselves on request of administration by presenting a valid Williamson identification card.

C. Load any third-party software on computer systems in the computer labs, unless authorized by a member of IT staff or administration

D. Transfer copyrighted materials to or from any system, or via the network, without the express consent of the owner of the copyrighted material.

E. Use any IT resource for commercial, political, or illegal purposes; personal financial gain; or harassment of any kind.

F. Display obscene, lewd, or otherwise offensive images or text.

G. Intentionally or negligently use computing resources in such a manner as to cause network congestion and performance degradation.

H. To remove materials (e.g. printouts, manuals, flash drives, etc.) belonging to other users or the college.

Private Owned Devices Connected to the College Network

The following applies to anyone connecting a privately owned device to the network. A devise is defined as any instrument capable of connecting to a network.

A. The only network that employees or students are authorized to connect to with a private computer is the public Wifi network. Under no circumstance are employees or students authorized to connect to alternate networks unless specifically approved by the college IT staff.

B. The owner of the device is responsible for the behavior of all users on the devise, and all network traffic to and from the device, whether or not the owner is aware of the traffic generated.

C. A private device connected to the network may not be used to provide network access for anyone not authorized to use the college's IT resources. The private device may not be used as a router or bridge between the network and external networks, such as those of an Internet Service Provider (ISP).

D. Should the IT or administrative staff have any reason to believe that a private device connected to the college network is using the resources inappropriately, network traffic to and from that device will be monitored. If justified, the system will be disconnected from the network, and action will be taken with the appropriate authorities.

E. Any residential student with an authorized network account may use the dormitory connection for scholarly purposes, for official college business, and for personal use, so long as the usage (1) does not violate any law, regulation, or this policy; (2) does not involve extraordinarily high utilization of resources or substantially interfere with the performance of the network; (3) does not result in commercial gain or profit; and (4) is not in violation of any part of this policy.

F. Users are responsible for the security and integrity of their systems. In cases where a device is "hacked into," the user shall either shut down the system or remove it from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. If you suspect electronic intrusion or hacking of your system and would like assistance, contact the IT department immediately (helpdesk@williamson.edu)

G. Personal servers and network equipment should never be connected to the college network without prior authorization.

Electronic Mail

The College e-mail system is not a private secure communications medium. As such, e-mail users cannot expect privacy. By using the Williamson's e-mail system, each user acknowledges:

A. The use of electronic mail is a privilege not a right. Transmitting certain types of communications is expressly forbidden. This includes messages containing chain letters, pyramids, urban legends, and alarming hoaxes; vulgar, obscene, or sexually explicit language; threatening or offensive content; derogatory, defamatory, sexual, or other harassment; and discriminatory communication of any kind. As with other information technology resources, the use of e-mail for commercial or political purposes is strictly prohibited.

B. Under the Electronic Communications Privacy Act, tampering with e-mail, interfering with the delivery of e-mail, and using e-mail for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.

C. All users of the e-mail system waive any right to privacy in e-mail messages and consent to the access and disclosure of e-mail messages by authorized personnel. Accordingly, Williamson reserves the right to access and disclose the contents of e-mail messages on a need-to-know basis. Users should recognize that under some circumstances, as a result of investigations, subpoenas, or lawsuits, the college may be required by law to disclose the contents of e-mail communications.

D. Any user who suspects that his/her e-mail account has been compromised is required to contact the IT staff immediately (helpdesk@williamson.edu).

E. The college e-mail system for employees is not authorized for personal use. Students are authorized, through their assigned Williamson e-mail address, to use the e-mail system for personal use.

File Sharing and Copyright Infringement

Federal copyright law applies to all forms of information, including electronic communications. Users should be aware that copyright infringement includes the unauthorized copying, displaying, and/or distributing of copyrighted material. All such works, including those available electronically, should be considered protected by copyright law unless specifically stated otherwise.

Williamson complies with all provisions of the Digital Millennium Copyright Act (DMCA). Any use of the Williamson network, e-mail system, or website to transfer copyrighted material including, but not limited to, software, text, images, audio, and video is strictly prohibited.

Anyone using College IT resources to commit acts of copyright infringement will be subject to the College's due process. Acts of piracy are violations of state and federal laws, and as such, may result in criminal charges.

Indemnification/Liability Statement

Williamson makes absolutely no warranties of any kind, either express or implied, for the IT services it provides. The college will not be responsible for any damages suffered by users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The College is not responsible for the accuracy or quality of information obtained through its IT services, including e-mail. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

The user agrees to indemnify and hold harmless Williamson, the Board of Trustees, and college employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the college's hardware, software, and network facilities. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.

Reporting Violations of IT Acceptable Use Regulations

Violations of this policy should be reported immediately to college administration. The administration will make every effort to maintain confidentiality to the extent possible consistent with other obligations.

Disciplinary Action

Violations of these regulations will result in the appropriate disciplinary action, which may include loss of computing privileges, suspension, termination, expulsion, and criminal prosecution.

Pennsylvania Law

It is a violation of Pennsylvania law to access, alter, or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. It is also unlawful to knowingly and without authorization, disclose a password to any computer system, network, or to gain unauthorized access to a computer or to interfere with the operation of a computer, network, or to alter, without authorization, any computer software. Violations of these sections of the law are punishable with up to $15,000 fine and seven years imprisonment. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine up to $10,000 and imprisonment of up to five years.

Federal Law and Legislation

A. USA Patriot Act

B. Homeland Security Act of 2002, Section 225 (Cyber Security Enhancement Act of 2002)

C. Prosecutorial Remedies and tools Against the Exploitation of Children Today Act, 18 U.S.C. § 2702 (PROTECT Act)

D. 18 U.S.C. § 1029. Fraud and related Activity in Connection with Access Devices

E. 18 U.S.C. § 1030. Fraud and related Activity in Connection with Computers

F. 18 U.S.C. § 1362. Communication Lines, Stations, or Systems

G. 18 U.S.C. § 2510 et seq. Wire and Electronic Communications interception and Interception of Oral Communications

H. 18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Record Access

I. 18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information

If you have any questions regarding this policy letter, please contact the IT Staff or the Senior Vice President/Chief of Staff

//Signed//
Senior Vice President/Chief of Staff