Student Information Technology Handbook

Academic Year 2023 - 2024

WILLIAMSON
COLLEGE of the TRADES
Founded 1888

106 S. New Middletown Road
Media, PA 19063-5299
610-566-1776 (phone)
610-566-6502 (fax)
info@williamson.edu
www.williamson.edu

FAITH • INTEGRITY • DILIGENCE • EXCELLENCE • SERVICE

TABLE OF CONTENTS

SECTION ONE: STUDENT ACCEPTABLE USE POLICY

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 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 using privately owned computers or electronic devices.

Network Resources in this document refers to all aspects of the college's owned or leased equipment, including, computers, printers, scanners, and other peripherals, as well as email, Internet services, servers, network files and folders, and all other technology-related equipment and services. These rules apply to any use of the college's network resources whether this access occurs while on or off campus.

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 educational 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, have been corrupted or damaged, or may threaten the integrity of the college's IT systems. In addition, files, e-mail, access logs (to include Internet browsing history), and any other electronic records may be subject to search at any time.

Students will:

A. Access the "Student" network system for educational purposes only. Student's may switch to the college's "Public" network after academic hours to access appropriate websites that may be restricted on the "Student" network. Students will always be held accountable for websites accessed.

B. Use appropriate language and be respectful of others. At no time will students engage in any form of Cyberbullying.

C. Observe and respect license and copyright agreements.

D. Keep passwords and personal information confidential (Student names, telephone numbers, and addresses should not be revealed to the system).

E. Return the laptops to the college IT Department when directed, or at the end of the college academic year for system updates and re-imaging.

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:
- Gaining access by willfully exceeding the limits of authorization.
- Attempting (even if unsuccessful) to gain unauthorized access through fraudulent means.
- Gaining access by using another person's name, password, access codes, or personal identification.
- Attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes.
- 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 college computer systems, including the laptop devices issued to a student, 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.

I. Use of the technology infrastructure to obtain or distribute racially or sexually offensive

material, to view pornographic or sexually explicit materials, to participate in hate groups or similar groups, or to engage or enable others to engage in gambling or any other illegal activity.

Privately Owned Devices Connected to the College Network

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

A. The only network students are authorized to connect to with a privately owned device is the "Public" Wi-Fi network. Under no circumstance are 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 device, and all network traffic to and from the device, whether the owner is aware of the traffic generated or not.

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 device will be disconnected from the network, and action will be taken with the appropriate authorities.

E. Any 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 or political 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 devices. 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 device, 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, because 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.

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 because 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 must 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

- USA Patriot Act
- Homeland Security Act of 2002, Section 225 (Cyber Security Enhancement Act of 2002)
- Prosecutorial Remedies and tools Against the Exploitation of Children Today Act, 18 U.S.C. § 2702 (PROTECT Act)
- 18 U.S.C. § 1029. Fraud and related Activity in Connection with Access Devices
- 18 U.S.C. § 1030. Fraud and related Activity in Connection with Computers
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C. § 2510 et seq. Wire and Electronic Communications interception and Interception of Oral Communications
- 18 U.S.C. § 2701 et seq. Stored Wire and Electronic Communications and Transactional Record Access
- 18 U.S.C. § 3121 et seq. Recording of Dialing, Routing, Addressing, and Signaling Information

SECTION TWO: STUDENTS LAPTOP POLICY

Computer Damages

- If a computer is damaged, the college must be notified immediately.

- The college reserves the right to hold the student accountable for all repair or replacement costs when the damage to the laptop is the result of gross negligence as determined by the administration. Examples of gross negligence include, but are not limited to:
  1. Leaving equipment unattended and unlocked.
  2. Lending equipment to others.
  3. Using equipment in an unsafe manner or environment.
  4. Violation of the college's acceptable use policy as outlined in Section One.

- A student awaiting a repair or replacement of their laptop may be offered a loaner device if available. If provided, the student will be held accountable, under this policy for the protection and return of any loaner device.

- If a laptop accessory (e.g., battery charger or pen) is damaged or lost, the student is responsible for replacing the item.

Student Use in Classrooms

- Students will comply with the specific course policy of each faculty instructor on the use of laptop devices within the classroom.

- The determination of when and how laptops may be used in the classroom is at the discretion of the course instructor.

- Students violating faculty use policy may be subject to disciplinary action, to include possible dismissal.

Student Access to Internet

- On campus, students will have access to the Internet through the college network server. When off-campus, students may access the Internet through their home or other onsite network access points.

Students Access & Monitoring

- At all times, the computer is the property of the college. As such, the laptop is subject to the college's policy requirements and stipulations as outlined in Section One.

- The college reserves the right to block inappropriate websites not conducive or aligned with Williamson's educational mission and code of conduct.

Downloading Programs & Personalizing the Computer

- Only the IT Department may download programs to the student computers.

- Stickers and other markings on the outside of the computer will NOT be allowed. Each computer and bag are easily identified by a specific numbering system ("Asset Tag") that is placed on the computer. This Asset Tag may not be tampered with or removed.

Student Printer Use

- Students will have access to the appropriate printers for their shop and throughout the network.

- Printers, unless approved by a college faculty or staff member, are for schoolwork use only.

SECTION THREE: LAPTOP CARE

You are expected to follow all the specific guidelines listed in this document and take any additional **common-sense** precautions to protect your assigned computer. **Loss or damage resulting from failure to abide by the details below may result in full-financial responsibility.**

General Care

- Treat this equipment with as much care as if it were your own property.

- Do not attempt to remove or change the physical structure of the computer, including the keyboard keys, or the computer casing. If these actions are taken, students will be responsible for 100 percent of the repair. or replacement cost. Take extreme care to protect the charging port. Do not put any unnecessary stress on the port as this may render the computer unusable.

- Do not remove or interfere with the serial number or any identification placed on the computer.

- Keep the equipment clean.

- Do not eat or drink while using the computer.

- Do not do anything to the computer that will permanently alter it in any way.

- Back up your data. Never consider any electronic information safe when stored in only one location.

- Do not put stickers or use any type of markers on the computer.

- DO NOT charge your computer while it is in the bag or on a soft surface, such as a pillow or bedding. Ensure the computer has air circulation while charging.

- Close the lid of the computer when it is not in use, to save battery life and protect the screen.

- Do not walk from one location to another with an open computer. Any file or data saved on the local drive will be lost and is not retrievable upon reboot. It is recommended to use the Student server (H: Drive), Microsoft 365 One Drive Cloud storage, and / or a personal flash drive to save and back-up all pertinent data. There is also a Compact 32GB Flash Memory Card inserted in each laptop with the drive letter D. This should be used as a temporary storage location as needed, and any files saved here should be backed up as soon as convenient.

Keep Your Computer in a Safe Place

- The computer bag, with the computer and other equipment, must be stored in a safe place. Do not leave the computer on the floor where it might be stepped on, or within reach of small children or pets when at home. Do not leave it in a car or anywhere it might be exposed to extreme temperatures.

- Laptops left in bags in unattended classrooms or other areas are considered "unattended" and will be confiscated by faculty or staff as a protection against theft. If confiscated, the student will receive a warning before getting the laptop back. If the laptop is confiscated a second time, the student may receive disciplinary hours. Unattended and unlocked equipment, if stolen – including at college – will be the student's responsibility.

- If on an athletic team, never leave computers in college vans, in the gym, in a locker room, on playing field, or in other areas where it could be damaged or stolen.

- Avoid storing the computer in a car other than in a locked trunk. The locked trunk of a car would be an acceptable storage place if it is not excessively hot or cold.

Computer Bags

- Each student will be given a computer bag that they are required to use to carry their computer in during the college day and outside of college. It is important to keep the bag clean and take time to remove any items like paper clips that can scratch the exterior of your computer. Static electricity may develop in the bag during the cold, dry winter months, and a simple solution to reduce this problem and to keep your bag smelling fresher is to put a dryer sheet in your bag.

Keep Your Laptop Away from All Liquids.

- Exposure to liquids will severely damage a laptop and will result in large repair costs. Water, soda, juice, power drinks, coffee, etc. will all ruin your computer completely. Do not put a bottle of water/soda/etc. in your backpack with your laptop -- even if it is sealed.

Only One User

- Do not allow anyone else to use your computer. Loss or damage that occurs when anyone else is using it will be your responsibility.

Computer Problems

- It is the student's responsibility to maintain a working computer at all times.

- If the student's computer is not working properly, the student needs to talk to the instructor in the class to determine if some minor troubleshooting will take care of the problem. If the problem still exists, contact the Helpdesk. If the computer cannot be fixed immediately, the student will be issued a "Bench Stock" loaner computer to use on a temporary basis.

- If you are off campus and need assistance, send an email to helpdesk@williamson.edu. Even though a response will not be immediate, the IT department will be notified of the problem and take care of it as quickly as possible.

- Do not attempt to remove or change the physical structure of the computer, including keys, screen cover or plastic casing. Doing so will void the warranty, and the student will be responsible for 100% of the repair or replacement cost.

- When in doubt, ask for help.

Cleaning the Computer

- Use a soft, dry, lint-free cloth when cleaning the computer. If necessary, the cloth may be dampened slightly to assist in the cleaning areas that do not appear to be coming clean with the dry cloth. Never use cleaning products with acetone or ammonia.

Shutting Down the Computer

- Shut down the computer when it will not be used for an extended duration.

- Putting your computer to sleep and not using it for several days can drain the battery.

Closing the Computer

- The laptop lid/screen needs to be completely closed when moving it from one point to another.

Carrying the Computer

- Always store the computer in the laptop bag.

- Bring the provided laptop bag to classes and use the laptop bag whenever transporting.

- Do not store anything (e.g., cords, mice, pens, or thumb drives) in the area within the case designed for the computer other than the computer itself as this may damage the screen.

- Do not grab and squeeze the computer, as this can damage the screen and other components.

Personal Health and Safety

- Avoid extended use of the computer resting directly on your lap. The bottom of the laptop can generate significant heat and therefore cause temporary or permanent injury. Use a barrier—such as a book or devices made specifically for this purpose— when working on your lap. Also, avoid lap-based computing while connected to the power adapter as this will significantly increase heat production.

- Avoid lengthy use involving repetitive tasks (such as typing and use of the trackpad). Take frequent breaks as well as alter your physical position (typing while standing, sitting, leaning, etc.) to minimize any discomfort.