Wilson Community College Acceptable Use Policy for Students

Section 1. Application

The WCC Acceptable Use Policy (AUP) for Students applies to any student (individual enrolled in any class on or off campus) who uses any device, whether college-owned or personal, to connect to the wired or wireless College Network, or to access any college-supported system.

Section 2. Requirements

1. Users may not connect personal devices to the wired College Network without express written permission from Technology Support Services. This requirement does not apply to users who connect through a college-supplied Wi-Fi network. Personal devices include, but are not limited to, smart phones, tablets, laptops, smart appliances or lighting, wearable devices, Amazon Echo, Google Home or other "Internet of Things" or similar technologies. Users may not place their own personal wireless access point or switching device under any circumstance on the college network without express written consent from Technology Support Services.
2. All devices connected to the College Network must have updated malware/anti-virus protection.
3. Users must not attempt to access any data, documents, email correspondence, or programs contained on systems for which they do not have authorization. This includes, but is not limited to attempting (even if unsuccessful) to gain unauthorized access by circumventing system security, uncovering security loopholes, or guessing passwords/access codes.
4. Users must not share their account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or other similar information or devices used for identification and authorization purposes.
5. Users must not make unauthorized copies or share copyrighted or college-owned software.
6. Users may not download, install, or distribute software to college-owned devices unless it has been approved by Technology Support Services.
7. Users must ensure all files downloaded from an external source, such as the Internet, to the College Network or any device connected to the College Network are scanned for malicious software such as viruses, Trojan horses, worms or other malicious code. Students are encouraged to use cloud storage (Microsoft One Drive) provided by the College.
8. Users must not purposely engage in activity that is illegal according to local, state or federal law, or activity that may harass, threaten or abuse others, or intentionally access, create, store or transmit material which may be deemed to be offensive, indecent or obscene.
9. Users accessing the College Network must only access Internet-streaming sites as consistent with the mission of the institution, for the minimum amount of time necessary.
10. Users must not engage in activity that may degrade the performance of information resources, deprive an authorized user access to resources, obtain extra resources beyond those allocated, or circumvent information security measures.
11. Users must not download, install or run security programs or utilities, on college-owned devices or devices connected to the College Network, such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of information technology resources unless approved or overseen by Technology Support Services or an authorized instructor.
12. Information technology resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorized fund raising, personal business ventures, or for the solicitation of performance of any activity that is prohibited by any local, state or federal law.
13. Access to the Internet from college-owned devices must adhere to all acceptable use policies. Students must not share their college-issued credentials or allow any other non-authorized person to access their College account(s).

14. Users must report any weaknesses in computer security to Technology Support Services for follow-up investigation. Weaknesses in computer security include unexpected software or system behavior, which may indicate an unauthorized disclosure of information or exposure to security threats.
15. Users have a responsibility to promptly report any incidents of possible misuse or violation of the Acceptable Use Policy, along with the theft, loss, or unauthorized disclosure of information.

Section 3. Violations

Any violation of these regulations is unethical and may constitute a criminal offense. Should a student commit any violation of this policy, access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

Section 4. Privacy Disclaimer

Wilson Community College implies no expectation of user privacy when connecting any device (college owned or personal) to the College Network or accessing a college-supported system. All users of the College waive any right to privacy of any stored content or email communications. The College has a right to monitor suspected unethical behavior. Accordingly, the College reserves the right to access and disclose the contents of email messages and stored files on a need-to-know basis. Confidential information will only be disclosed in accordance with federal, state, and local requirements, i.e. FERPA, GLBA, PCI compliance. 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 email or stored files.

Wilson Community College is not liable for loss or damage to files or the functionality of a personally owned device when connected to the College Network or a college-supported system.

Section 5. Acknowledgement of Policy

Wilson Community College publishes this AUP for Students on the College website, in the College catalog, and in Moodle classes. Use of the College Network, wired or wireless, or accessing a college-supported system through a college-issued account represents implied agreement to abide by this Acceptable Use Policy for Students.