Wilson Community College Acceptable Use Policy

Section 1. Application

This policy applies to any college employee, contractor or third party who uses any device, whether state-owned or personal, to connect to the wired or wireless College Network.

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.
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.
4. Systems administrators and authorized users must not divulge remote connection information or other access points to information technology resources to anyone without proper authorization.
5. 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.
6. Users must not make unauthorized copies of copyrighted or college-owned software.
7. Users may not download, install, or distribute software to college-owned devices unless it has been approved by Technology Support Services.
8. Users must ensure all files downloaded from an external source to the College Network or any device connected to the College Network, including a CD/DVD/Blu-ray, USB flash drive, or any other electronic medium, is scanned for malicious software such as viruses, Trojan horses, worms or other malicious code.
9. Users must ensure that the transmission or handling of personally identifiable information (PII) or other sensitive data is encrypted or has adequate protection.
10. Users must not download College data to personally owned devices unless approved by Technology Support Services.
11. Users must comply with the State's Data Retention Guidelines located at https://archives.ncdcr.gov/documents/colleges-north-carolina-community-college-system-retention-and-disposition-schedule.
12. 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.
13. Users accessing the College Network must avoid unnecessary network traffic and interference with other users. Specific prohibitions include, but are not limited to, the following:

    (a) Unsolicited commercial advertising by public employees and College Network users. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission initiated by a vendor, provider, retailer, or manufacturer of goods, products, or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer that describes goods, products, or services. This prohibition does not include the following:

        (i) discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer, or manufacturer, or related to or affiliated with the vendor, provider, retailer, or manufacturer);

        (ii) responses to questions, but only if such responses are direct replies to those who inquired via electronic mail; or

(iii) mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.

(b) Any other type of mass mailing by employees and others accessing the College Network that does not pertain to college business or a college-sponsored activity.

14. Users accessing the College Network must only access Internet-streaming sites as consistent with the mission of the agency for the minimum amount of time necessary.
15. 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.
16. Users must not download, install or run security programs or utilities 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.
17. 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.
18. Access to the Internet from college-owned devices must adhere to all acceptable use policies. Employees must not allow non-employees to access nonpublic accessible information systems.
19. 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.
20. 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. Technology Support Services Handbook
More detailed information regarding Technology Support Services can be found in the electronic version of the Technology Support Services Handbook located in the Technology Support Services section of the Intranet through Moodle. The Technology & Distance Learning Committee is responsible for making users aware of any updates to the TSS Handbook. It is the user's responsibility to regularly review the TSS Handbook and follow the established guidelines and procedures.

Section 4. Violations
Violation of this policy and/or the guidelines in the TSS Handbook may result in disciplinary action, termination, loss of information resources and/or criminal prosecution.

Section 5. Acknowledgement of Policy
Wilson Community College employees and contractors must acknowledge in writing that they have received a copy of this policy prior to accessing the College Network.

I have read, understand, and will abide by the above Acceptable Use Policy when using computer and other electronic resources owned, leased, or operated by Wilson Community College. I further understand and will abide by the above Acceptable Use Policy when using personal computing devices not owned leased, or operated by Wilson Community College that connect to the College Network. I further understand that I have no expectation of privacy when connecting any device to the College Network and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

_____ _____

User Signature *Date*

Adopted by the WCC Technology and Distance Learning Committee on 10/09/19
Approved by College Council on 11/12/19