

Purpose

The purpose of this policy is to establish rules for the use of the College Wireless Network, consequences for misuse, and connection with relevant governing authority regulations.

Definitions

The NSCC wireless network is in place for the purpose of academic pursuits and conducting college business. Tennessee State law and Federal law regulate the use of college networks.

Mobile devices and applications on the wireless network vary widely in numbers and types. These additional components and devices, such as a cell phone use of Voice over IP (VoIP) through local wireless, can add greatly to network traffic. NSCC has a robust system; however the network bandwidth through which all college digital traffic travels is limited by the capacity of carrier circuits.

Furthermore, the college must comply with all Federal, State and local laws noted in the Sources and Related Policies section of this policy. Illegal downloading and non-academic overuse have the capability of consuming resources which interfere with, limit or prevent the network's intended purpose.

For the above reasons, the NSCC campus wireless systems must operate with network controls in place and policies in order to maintain legal and technical standards while allowing digital information to flow freely and efficiently in support of academic studies and in the attainment of college goals.

Policy

1. It is illegal to download, use, or re-distribute copies of copyrighted material without first obtaining written permission to do so. If you download items such as music, films, or computer programs without proper licensing you can be held personally liable. The College is also liable if they allow their networks or computers to be used in this way. For this reason, such activities are **strictly prohibited**.
2. High-bandwidth and streaming applications (such as streaming audio, streaming video, real time phone/video conferencing) must be used thoughtfully, as they increase network traffic.
3. VoIP (Voice over Internet Protocol) telephony programs are allowed, but we ask you to use programs such as MSN Messenger, Google Talk, and OpenWengo, rather than Skype. Skype is able to divert other commercial internet traffic

through the College network even when you are not making a call, which is a violation of State law.

4. It is forbidden to run any P2P 'peer-to-peer' or 'file-sharing' torrent software such as BitTorrent, Limewire, or The Pirate Bay without prior permission. As well as being the main route for illegal downloads, these programs can consume large quantities of internet bandwidth and can adversely affect the performance of our network.
5. Tethering or mobile "Hot Spot" application using NSCC's network connection to create a wireless sub-network through phones or other devices is not allowed. Additionally, wireless access points and/or personal wireless routers that connect to the wired network may not be used. These present a security risk and may interfere with the College's main wireless system.
6. General computer use as set forth in the NSCC Policy 08-03-00 Acceptable Computer Use Policy must be observed in the wireless network as well. In particular, this policy forbids the use of NSCC's network for illegal, defamatory, or indecent purposes. Should the network administrator find a breach in the rules for use of the wireless system the following actions will be taken.
7. You will receive notification of a violation by email. You may respond to the administrator to offer explanation or to ask for assistance in mitigating the issue.
8. If the first notice does not result in compliance, the offending account and/or IP address may be throttled – bandwidth limited – to a level which the administrator feels appropriate for the situation.
9. In the third notice, students will be asked to see the AVP of Student Affairs or Extended Campus Director for possible disciplinary actions.
10. If compliance is not met, the account will be subject to disconnection from all network services until such time as the disposition of disciplinary actions are received from the AVP of Student Affairs or Extended Campus Director.

Sample Notices for "High Talkers" & Violators

1st Excessive Usage Warning Email Text

Dear :

Suspicious wireless activities have been detected through your college account.

A very large amount of data/network bandwidth usage has been traced to a device for which your credentials were used to access NSCC's wireless network. Due to this, your account and/or IP address has been flagged for abusive and possibly illegal activities by NSCC's network monitoring systems.

If you have not recently downloaded large files, or numbers of files, and feel that your account has been compromised, please contact the Technology Services Help Desk (615-353-3678) and let the technician who answers know that your account was flagged for suspicious activities on the wireless network. The technician will work with you to reset your passwords and provide you with tips to safeguard your portable wireless devices.

Please Note: If large amounts of data/network bandwidth usage continue to emanate from your account, the NSCC Wireless Network Administrator will either place connection limiting controls, or deny your account access to the NSCCWIRELESS network.

It is illegal to download, use, or re-distribute unlicensed copies of copyright material such as music, films, or computer programs. If evidence of illegal downloading is connected to your account, all network access, including the wired campus computer network, will be denied and evidence of this violation sent to the proper NSCC authority for disciplinary action.

Please refer to NSCC Policy 08-08-00 Wireless Network Policy.

2nd Excessive Usage Warning Email Text

You have been notified of suspicious wireless activities or bandwidth over usage. Large amounts of data/network bandwidth usage continue to be traced to your account.

Therefore, the NSCC Wireless Network Administrator has placed access limiting controls on your account and/or IP address connection to the NSCC wireless network. In order for these limits to be removed you must respond to the Help Desk and provide an explanation, which will be issued to the Network Administrator, as to what steps you have taken to correct excessive usage of network resources. The Network Administrator will make a determination based upon the results of your actions.

It is illegal to download, use, or re-distribute unlicensed copies of copyright material such as music, films, or computer programs. If evidence of illegal downloading is connected to your account, all network access, including the wired campus computer network, will be denied and evidence of this violation sent to the proper NSCC authority for disciplinary action.

3rd Excessive Usage Warning Email Text

This is your third notification concerning suspicious wireless activities or bandwidth over usage. Large amounts of data/network bandwidth usage continue to be traced to your account. Therefore, the NSCC Wireless Network Administrator has contacted the AVP of Student Affairs or Extended Campus Director for a disposition of disciplinary actions. Furthermore, connection limiting controls have been placed on your account and/or IP address access to the NSCCWIRELESS network. These limits will not be removed until the network administrator is contacted by the AVP of Student Affairs or Extended Campus Director. If we receive no notice within 48 hours your account and/or IP address will be denied access to all, wired and wireless, NSCC networks.

It is illegal to download, use, or re-distribute unlicensed copies of copyright material such as music, films, or computer programs. If evidence of illegal downloading is connected to your account, all network access, including the wired campus computer

network, will be denied and evidence of this violation sent to the proper NSCC authority for disciplinary action.

Sources

[Digital Millennium Copyright Act \(DMCA\)](#)

[Communications Assistance for Law Enforcement Act \(CALEA\)](#).

Related Policies

[NSCC Policy 08-03-00 Acceptable Use Policy](#)

Change Log

| Date | Change | By |
|-----------|---------------------------------|-----|
| 3/15/2021 | Formatted for new policy format | PAK |
| | | |

Approved by President's Cabinet 6/14/21