Information Systems Use Policy

The use of Information Systems, personal or college (computers, laptops, networking equipment, network resources, pda’s, servers, smart phones, tablets, telephones, etc.) on either the college’s guest or private networks requires the acceptance of the North Central Kansas Technical College’s Information Systems Use Policy. End users (you) are independently and solely responsible for complying with all applicable laws and policies in all of your actions related to your use of personal or college information systems and network resources, regardless of the purpose of the use.

Certain information systems are prohibited due to their potential to cause harm or damages, such as decreased network performance, introduction of viruses or complete information system outages for a building or multiple buildings. End users (you) do not want to be responsible for information systems disruptions or outages, and with the availability of college-wide wireless access and college computers, end users (you) should have no reason to use a prohibited device. Any violation of this policy, a virus, malware or spyware infection of an Information System, outdated or no security (antivirus) software, attaching servers or additional networking equipment, or any copyright infringement; may result in the interruption of services and or loss of network privileges, the cancellation of housing contracts, the dismissal from the college and or legal action without prior notification.

NOTICE: North Central Kansas Technical College reserves the right to update or change the posted Information Systems Use Policy at any time without notice. All college Information Systems are business devices and should not be used as personal use systems. Please keep all college Information Systems use related to college business or research and not to a personal or home business type of use. This includes but is not limited to the following practices:

1. It is the responsibility of all college Information Systems end users to read, understand and follow NCK Tech’s Information Systems Use Policy.
2. Only authorized college faculty, staff, students or guests (end users) are allowed to use college Information Systems and network resources.
3. End users personal devices (computers, laptops, tablets, pda’s, iPods, smart phones, etc.) may connect the college’s guest wireless networks (NCK Tech Guests) or (NCK Tech Campus) as long as they meet and follow NCK Tech's Information Systems Use Policy. These devices are NOT permitted to connect to any other college network. For more information on the college’s guest wireless service, please refer to our Wi-Fi Warning and Disclaimer posted on our public web and within each department.
   * NCK Tech reserves the right to refuse or deny network services to any personal device if for any reason that device has questionable functionality or may be in violation of the Information Systems Use Policy.
   ** The college is not responsible, liable or accountable for any end users personal devices, technical support or damages that may occur from the end users connecting to the Internet (malware, spyware, viruses, etc.) via the college’s guest wireless network.
4. End users are to refrain from installing any software on to any college Information Systems without prior approval from NCK Tech's IT staff. Non-approved software may be removed from college Information Systems and loss of use, or rights may occur.
5. End users are not permitted to change, add, remove or modify any college Information Systems hardware, software or operating system settings.
6. End users are not permitted to change, add to, remove from or modify the college’s network infra-structures in ANY manner without NCK Tech’s IT staff approval. This includes all Information Systems, network switches, access points, routers and servers of any kind (examples include, but are not limited to: FTP, SMTP, DHCP, P2P (peer to peer), DNS, Remote Terminal Connections, IIS, NAT devices, distributed transaction servers, LAN\network scanners, wireless analyzers, proxies, packet analyzers, protocol analyzers, denial of service attacks, network discovery or brute force password cracking software, key loggers, locks, viruses or other harmful content) or other related networking hardware or software deemed to be malicious or harmful by NCK Tech’s IT staff or the IT industry.
7. End users are to refrain from using any offsite, cloud-based data storage or backup sites such as carbonite, dropbox, idrive, mozy, skydrive, etc. These sites and services are not supported by the college. The college provides onsite data storage to faculty, staff and students, if requested.
   * The college’s data storage is NOT intended for use as primary data storage, but rather a secure replica of the end users data.
8. End users are solely responsible for the content, retention and compliance with all applicable laws and policies of any electronically generated material created in any format while using a college or personal device or networked service provided by the college.
9. All Information Systems use must be legal, ethical, reflect academic honesty and community standards, and show restraint in the consumption of shared Information Systems resources (computers, network access and network bandwidth).

PO Box 507
Beloit, KS 67420
http://www.ncktc.edu
10. End users are to refrain from invading another person’s privacy including viewing, copying, modifying, or destroying another person’s data without explicit permission from the creator/owner of the data.

11. End users are to refrain from purposefully connecting, removing, damaging, destroying, modifying or changing any college Information Systems hardware, software or operating systems settings.

12. End users are to refrain from using Information Systems to harass, defame or send any harmful, malicious, slanderous, unsolicited or fraudulent chat, email, text, IM or spamming messages to others.

13. End users are to refrain from posting, displaying, viewing, sending, forwarding or otherwise distributing libelous, defamatory, offensive, racist or obscene materials over the college’s network and guest wireless networks.

14. End users are to refrain from sending or forwarding messages or attachments belonging to another user without first acquiring permission from the original sender. Attachments should be limited to 10MB or less.

15. End users are to refrain from installing, creating, distributing or using unauthorized copies of licensed software, music or literature, videos or other copyrighted materials.

16. End users are to refrain from using college Information Systems and network connections for frivolous activity, non-educational use or personal business/monetary gain, such as with stock market or commodities trading, Internet or email messaging commerce, etc.

17. Social media is to be used to promote the mission, values and programs of the institution. Personal use of social media while on contracted time is forbidden.

18. Information Systems passwords are required to gain access to various resources on the college computer/telephone network and are considered private. End users (you) are not to disclose your account information to anyone at anytime. If for any reason you believe that your NCK Tech account or password has been compromised, immediately inform the college’s IT staff so that preventative measures may be taken to protect you and your NCK Tech account. End users are required to log off or shut down all Information Systems after use.

19. NCK Tech uses “filtering” to make sure our employees, students and guests do not view sites that contain or display objectionable material. Filtering can only be accomplished at an "all or nothing" level. We cannot turn on a site only for one person and no one else. Please understand that these filtering protocols apply to everyone-guests, students and employees’ alike-using the guest wireless or any other college network to access the Internet.

20. There should be no expectation of privacy as all information, including personal information, placed or sent over the college's network is logged and may be monitored. Internet activity, email messages and attachments may be monitored without prior notification if NCK Tech deems this necessary. If there is evidence that an end user is not following NCK Tech’s Information Systems Use Policy, the college reserves the right to take disciplinary action, including the loss of network privileges, the cancellation of housing contracts, and dismissal from the college and or legal action.

21. NCK Tech and its employees will neither be held responsible or liable for any criminal, civil, illegal or illicit activity conducted by an end user misusing any personal or college Information System and network resources. End users (you) are independently and solely responsible for complying with all applicable State, Federal and International laws and policies in all of your actions related to your use of personal or college information systems and network resources, regardless of the purpose of the use.

____________________________________________________  ____________________________  ____________________________
End Users (printed name – MUST BE LEGIBLE)  Department  Campus

____________________________  ____________________________
End Users Signature  Date

____________________________  ____________________________
Network Administrator or Designee Signature  Check here if you would like an NCK Tech Email Account _______