Fort Hays Tech | North Central

Information Systems Use Policy

The use of Information Systems, personal or college (computers, laptops, networking equipment, network resources, PDA's, servers, smartphones, tablets, telephones, etc.) on either the College's guest or private networks requires the acceptance of the Fort Hays Tech | North Central'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 building. 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 Any violation of this policy, a virus, malware or spyware infection of an Information System, outdated or no security (antivirus) software, attaching servers or additional networking equipment, or any copyright infringement; may result in the interruption of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 for students, dismissal from the College and or legal action without prior notification.

NOTICE: Fort Hays Tech | North Central reserves the right to update or change the posted Information Systems Use Policy at any time. 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 Fort Hays Tech | North Central'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. 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 Fort Hays Tech | North Central deems this necessary. If there is evidence that an end-user is not following Fort Hays Tech | North Central'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 for students, and dismissal from the College and/or legal action.
4. End-users' personal devices (computers, laptops, tablets, PDA's, iPods, smartphones, etc.) may connect to the College's guest wireless network (Campus or Campus Guests) as long as they meet and follow Fort Hays Tech | North Central'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. * Fort Hays Tech | North Central 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 user's personal devices, technical support or damages that may occur from the end-users connecting to the Internet (malware, spyware, viruses,) via the College's guest wireless network.

5. End users are to refrain from installing any software onto any college Information Systems without prior approval from Fort Hays Tech | North Central's IT Department. Non-approved software may be removed from college Information Systems, and loss of use or other rights may occur.
6. End users are not permitted to change, add, remove, or modify any college Information Systems hardware, software, or operating system settings.
7. End users are not permitted to change, add to, remove from, or modify the College's network infrastructures in ANY manner without Fort Hays Tech | North Central's IT Department 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 Fort Hays Tech | North Central's IT Department.
8. End users should understand that offsite, cloud-based data storage, or backup sites such as carbonite, drop box, I Drive, Mozy, SkyDrive, Google drive, etc., 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-user's data. Fort Hays Tech | North Central is not responsible for any data loss from using these sites. With respect to Google drive, your account may be completely suspended for a violation of this policy.
9. 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.
10. 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).
11. 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.
12. End users are to refrain from purposefully connecting, removing, damaging, destroying, modifying, or changing any college Information Systems hardware, software, or operating systems settings.

13. 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.
14. 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.
15. End users are to refrain from sending or forwarding messages or attachments belonging to another user without first acquiring permission from the original sender.
16. End users are to refrain from installing, creating, distributing, or using unauthorized copies of licensed software, music or literature, videos, or other copyrighted materials. 66 Fort Hays Tech | North Central Board of Trustees Policy Handbook (Approved 7.22.24)
17. End users are to refrain from using college information systems and network connections for frivolous activity, non-educational use, personal, or business/monetary gain.
18. Social media is to be used to promote the mission, visions, values, and programs of the institution.
19. Information Systems passwords are required to gain access to various resources on the College computer/telephone network and are considered private. These passwords will be reset once a semester. End users (you) are not to disclose your account information to anyone other than IT Administration for tech support. In certain circumstances, employees may be required to share account information during an absence in order for college work to continue. Any such instances must be approved in advance by the College President or designee. If, for any reason, you believe that your Fort Hays Tech | North Central account or password has been compromised, immediately inform the College's IT Department so that preventative
20. Measures may be taken to protect you and your Fort Hays Tech | North Central account. End users are required to log off or shut down all Information Systems after use.
21. AI Tools and Generators (ChatGPT, Meta, Co-Pilot, Dall-E, etc.) may be used in the academic setting, but have limits in their use as described below. Please review the following as to when AI tools and AI generated content is permissible to use in both the workplace and classroom settings.
    a. **Students**
        i. Students may use AI where permitted for class work and content generation. Students are responsible to check their course syllabi for individualized instructions in how AI use is permitted per course. Please be aware the use of AI generated content may result in misinformation or inaccuracies. Students should use with caution and double check generated content. Submitting AI generated work as your own, without attribution, will be considered academic dishonesty.
        ii. The use of AI tools to create content enabling harassment, defamation, stalking, or sexual exploitation is not permitted. AI generated content is not permissible to break laws, institutional policies or licensing agreements.
    b. **Faculty/Staff**
        i. AI usage is permitted in the following applications:

1. Lesson planning
2. Professional development and training presentations
3. Personalized student support
4. Administrative assistant – automating tasks, drafting/revising communications, transcribing meetings
5. Event planning

ii. Ai usage is not permitted in the following applications:
1. Using AI generated code within institutional IT systems or services without permission from system administrators.
2. Using AI tools to create content enabling harassment, defamation, hostile environment, stalking or illegal discrimination.
3. Using AI to summarize and/or grade student work
4. Using AI tools to infringe copyright or other intellectual property rights
5. Uploading FERPA protected information, HIPPA protected information, Intellectual property, and information related to employees and their performance into AI tools for data analysis

iii. Faculty/Staff should work with their supervisor. The College reserves the right to limit and/or prohibit the use of AI.

22. Fort Hays Tech | North Central 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 - using the guest wireless or any other college networks to access the Internet.

23. Fort Hays Tech | North Central and its employees will neither be held responsible nor 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.

Student Housing Internet Access

For students living in campus housing (Beloit campus only), a secured wireless Internet connection is available for laptops, tablets, and gaming consoles.

In order for the Internet in housing to function properly, the following rules MUST be followed:

- Each resident is allowed up to 3 devices (laptop, tablet, gaming console, or smartphone) to connect to the housing's wireless Internet.
- No personal wireless routers are allowed in student housing.
- No personal wireless access points, bridges, or repeaters are allowed in student housing.
- Residents are encouraged not to share their wireless key with any visitors, as doing so reduces available bandwidth to that housing unit.
- Residents are encouraged not to turn on smartphone Hotspots in order to help reduce disruptive and unnecessary wireless signals and traffic.
- Residents are required to read and adhere to the Student Housing Acceptable Use Policy: http://home.ncktc.edu/documents/Dorms_AUP.pdf Additional Acceptable Use Policy for Dorms. All acceptable use rules set forth above continue to apply to use of college information systems in student housing, in addition to the following:
- All computers connecting to the student housing's network are required to have current and up-to-date security software and patches.
- Internet activity over student housing's network may be monitored at any time without prior notification. If there is evidence that a resident is not following this acceptable use policy, the College reserves the right to take appropriate disciplinary action, including, but not limited to, loss of network privileges, cancellation of housing contracts, dismissal from the College, and/or appropriate legal action.

Service provided "AS IS." The student housing's network provides access to the Internet on an "AS IS" basis with all the risks inherent in such access. The College makes no warranty that the student housing's network or that any information, software, or other material on the student housing's network is free of viruses, worms, Trojan horses, spyware, malware, or other harmful components. By connecting to the student housing's network, residents (end users) acknowledge and accept the risks associated with public access to the Internet and use of the student housing's network.

Service provided "AS AVAILABLE." The student housing's network is provided on an "AS AVAILABLE" basis without warranties of any kind, either express or implied, that the dorms' network will be uninterrupted or error-free, including but not limited to vagaries of weather, disruption of service, acts of God, warranties of title, non-infringement, nor implied warranties of merchantability or fitness for a particular purpose. No advice or information given by the College, affiliates, or employees of the College shall create such a warranty.

Indemnity.

Under no circumstances shall the College, the provider of the student housing's network, or affiliates, agents, or employees thereof, be liable for any direct, indirect, incidental, special, punitive or consequential damages that result in any way from the residents' use of or inability to use the student housing's network or access to the Internet or any part thereof, or the residents' reliance on or use of information, services or merchandise provided on or through the student housing's network, or that result from mistakes, omissions, interruptions, deletion of files, errors, defects, delays in operation or transmission, or any other failure of performance. Residents agree to indemnify and hold harmless the College, the provider of the student housing's network, including affiliates, agents, and employees thereof, from any claim, liability, loss, damage, cost, or expense (including without limitation reasonable attorney fees) arising out of or related to the residents' use of the student housing's network, any materials downloaded or uploaded through the student housing's network, any actions taken by the residents in connection with the residents' use of the student housing's network, any violation of any third party's rights or any violation of law or regulation, or any breach of this policy.

Connection Assistance

The College's IT department will provide technical support for internal student housing network issues only, such as locked up access points or failed network switches. Any college hardware failures will be addressed and repaired as soon as possible. The College's IT department is NOT responsible for and will NOT provide technical support for residents' personal devices.

Student housing network support times are Monday through Friday, 8:00 A.M. to 4:00 P.M. Residents should schedule assistance requests during these hours. For after-hour issues, residents should contact the Dean of Student Experience or complete the Student Housing Assistance form on the College's Intranet to receive assistance on the next business day.

Information Systems Use Policy Signature Page

_____	_____	_____
*EU Printed Full Name – Must Be Legible	Department	Campus

_____	_____
*EU's Signature	Date

_____

Network Administrator or Designee Signature

* EU = End User