Acceptable Use Policy

It is the policy of North Central Missouri College to maintain access to local, national, and international sources of information and provide an atmosphere that encourages free exchange of ideas and promote learning. Use of the College's electronic information systems is a privilege and not a right. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and comply with all relevant laws, College policies and procedures, and contractual agreements.

NETWORK DEFINITION

The College network is defined to include any and all computer and electronic based communication facilities (voice, data, and video) and/or equipment which are owned or operated under the supervision of North Central Missouri College.

CRIMINAL OR ILLEGAL ACTS

Electronic information systems of the College, which include hardware, software, and network environment, shall not be used for illegal or criminal activities. Such activities may involve, but are not limited to, unauthorized access, intentional corruption or misuse of resources, theft, defamation, obscenity, pornography, child pornography, and harassment based upon ethnicity, disability, age, religion, or sex. The College will cooperate with all branches of law enforcement (local, state, federal, or international) in investigations of a criminal nature by making available transmissions and files within the College's network.

COPYRIGHT LAW

North Central Missouri College treats copyright infringement very seriously. It is illegal to violate the copyright law, including downloading or sharing music and videos without permission from the copyright owner. Copyright owners have begun using software to aggressively search for people who are providing copyrighted materials to others over the Internet without the copyright owner's permission.

INFORMATION SECURITY

Employees must understand and follow the information security policies. All data that is collected must be secure. Secure Data Elements also known as personal identifiable information must never be released to any entity outside of the college without your supervisor's approval. Employees that fail to follow the Information Security policies are subject to the sanctions of the North Central Missouri College's Electronic Information System Use Policy.

Secure Data Elements

Although commonly stored, these data elements are protected and must not be made available. This information should not be released verbally. Electronic or paper reports containing this data must be approved before release. First name (or first initial) and last name in combination with any of the following:

- Social Security Number
- Driver's license number, Student ID, or other unique number assigned or collected by a government body.
- Financial Account, credit card, or debit card number
- Unique electronic Identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account.
- Medical Information
- Health Insurance Information

Never Store Data Elements

Never store these elements electronically or on paper.

- Full Credit Card Numbers (last 4 digits acceptable)
- Credit Card Card-Validation codes (3 or 4 digit code on front or back of card used to verify card no present transactions)
- Credit Card PIN Numbers

FERPA

Employees of North Central Missouri College are expected to maintain the confidentiality of all educational records, as outlined in the Family Educational Right and Privacy Act (FERPA). FERPA is a federal act designed to protect the privacy of educational records, to establish the right of students to inspect and review their educational records, and to provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings. The College Catalog and website state the policy regarding academic records at North Central Missouri College. Academic records are open to members of the faculty and staff who have a legitimate educational interest in seeing the records. Information should not be viewed unless it is required to fulfill job responsibilities at NCMC. Under the terms of FERPA, certain directory information may be released to third parties without the written consent of students, however students have the right to restrict release of directory information. All third-party requests for academic information should be cleared through the offices of the Dean of Student Services or the Registrar at North Central Missouri College.

SMART PHONE / MOBILE DEVICE

All portable devices that use the college network or resources to synchronize or store data must have an automated lock configured to prevent unauthorized access. All devices must be

updated to insure the highest level of security. IT Services must be notified of missing or stolen devices no later than the next business day.

FLASH DRIVES

College employees must use an approved password protected encrypted flash drive. Lost or stolen storage devices must be reported to IT Services no later than the next business day.

NOTEBOOKS

All notebook computers used for administration of college business must have the hard drive encrypted and be a member of the domain. IT Services must be notified of missing or stolen computers no later than the next business day.

OFF CAMPUS IT SERVICES

Cloud or Off Campus Provider

Contracting with or the use of services such as Cloud or any type of remote services not provided by the IT Services department is prohibited.

Data Storage

The use of personal or cloud base (hosted) storage such as, but not limited to, SkyDrive, Dropbox, and Google Documents not provided by the IT Services department is prohibited.

EMAIL

Email containing private data elements must only be sent off campus in an encrypted transmission. Users must comply with the CAN-SPAM Act that deals with sending bulk/commercial messages that are unsolicited. Contact the helpdesk before sending messages to recipients with which you do not have a prior working relationship.

ACCEPTABLE AND UNACCEPTABLE USES

Acceptable and unacceptable uses of College electronic information systems are outlined below. Note: this list is not all inclusive.

ACCEPTABLE USES

- A means for authorized users to have legitimate access to email, network resources, and/or Internet access.
- Any use necessary to complete research or coursework assigned to a College employee or student.

- Communication for professional development.
- Other administrative and/or academic communications or activities in direct support of College projects and missions.
- Limited personal use may be allowed when such use meets the following criteria: it does not interfere with College operations, it does not compromise the functioning of the College network and computing resources, it does not interfere with the user's employment or other obligations to the College, and it does not violate any other laws, regulations, or College policy.

UNACCEPTABLE USES

- Any commercial or for-profit use
- Attempting to gain or gaining unauthorized access to the computer system or files of another
- Including use of another individual's identification, network, email or other College-based account and/or related passwords
- Any use that causes unauthorized network disruption, system failure, or data corruption
- Any use related to achieving, enabling, or hiding unauthorized access to network resources, College-owned software, or other information belonging to North Central Missouri College
- Unauthorized or excessive personal use
- Use of computing facilities or network resources to send obscene, harassing, abusive, or threatening messages or computer viruses or worms
- Use of all peer to peer file sharing sites such as uTorrent, Bittorrent, qBittorrent, Transmission, Bitport.io, FrostWire, Deluge, Folx, Webtorrent.io, Shareaza, eMule, and many more are considered peer to peer file sharing sites.

USER RESPONSIBILITY AND ACCOUNT OWNERSHIP

Users may not allow other individuals to use their College-assigned network, email, or other College-based account. Employees and students are individually responsible and accountable for the proper use of their assigned accounts. Users should take proper security measures to ensure the integrity of their accounts and should also report any notice of unauthorized access. All network shares on individual's computers must be properly password protected. The college will use email to communicate important information, so all users are encouraged to check their email on a regular basis.

ADDITIONAL POLICIES

North Central Missouri College is required by contract with MOREnet to abide by and therefore enforce their policies and procedures. For more information about MOREnet's policies, procedures, and security measures, visit them online. Visit More.net

USER CONDUCT AND SANCTIONS

Abuse of the College's electronic information system or violation of any local, state, or federal telecommunication law or regulation, or College policy, is not allowed and may subject the individual to criminal, civil, and institutional penalties and liabilities.

Penalties for violation of college policies including unauthorized peer-to-peer file sharing, illegal downloading or unauthorized distribution of copyrighted material using the College's information technology system can include, but not be limited to, loss of all College computer network privileges, probation, suspension from the College, and/or referral to law enforcement for prosecution, including criminal or civil action. Employees can also be subject to termination.

Penalties for violation of federal copyright laws and copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505. Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, visit the US Copyright Office.

FERPA is enforced by the Family Compliance Office, which is part of the U.S. Department of Education. Violations may result in NCMC's loss of ability to offer federal financial aid programs, institutional fines, personal law suits, termination of employment, and other sanctions. All employees shall read and become familiar with the "Guidelines for Release of Education Records" as posted on the NCMC website. More information is available online at ncmissouri.edu/registrar.

UPDATES

Email notifications will be made available as changes affect this policy.