Nicolet College assigns and provides access to computer equipment, computing resources, and other electronic media to support College business. Use of computer equipment, computing resources, and other electronic media is limited to the purposes for which the access was provided.

Computer equipment, computer resources and other electronic media, employee accounts and transmissions, and all data stored on College systems are College property and subject to review and open records requests. Security analysis and maintenance systems may be used to identify and monitor unauthorized use of College computing equipment, systems and resources. With appropriate authorization, Information Technology staff may access data, accounts, and transmissions for troubleshooting, maintenance, or forensic purposes.

**Ethical Use of Computers and Electronic Media**

Employees hold a position of trust which imposes ethical obligations on the use of College computers, resources, and other electronic media.

- Employees will act as trusted agents in accessing, generating, and/or storing printed and electronic records/documents.
- Employees will use College computers and electronic media for College-related business. Use of College computers and electronic media for commerce, lobbying, or personal monetary gain is not permitted.
- Employees will not be a party to the misuse of computers, resources, or other electronic media.

**Inappropriate Use of Computers and Electronic Media**

Individuals using Nicolet computers and electronic media are prohibited from accessing/retrieving, saving, viewing, printing, disseminating, or displaying information including, but not limited to:

- Discriminating, harassing, insulting, or attacking others based on race, national origin, sex, sexual orientation, age, religion, disability, or any other legally protected status.
- Derogatory, demeaning, or offensive comments to or about any individual or group.
- Defamatory or threatening comments to or about any individual or group.
- Obscene, sexually oriented, pornographic, offensive, lewd materials, comments, or jokes. Any child pornography is a violation of law and will be reported to the appropriate authorities.
• Interference with computer or electronic media use or operations.
• Accessing or using College data that is available but not relevant to one’s current position, or manipulating College data for personal reasons.
• Conducting or participating in solicitations or promotions related to commercial ventures, religious or political causes, or solicitations or promotions other than those specifically approved by the President or a Vice President.
• Theft, accessing, copying, or saving electronic files without permission.
• Downloading, saving, or sharing music, videos, pictures, etc.
• Sending chain letters.
• Engaging in communications for any purpose contrary to College policy or interests or communicating on behalf of the College without consent.
• Use of another person’s password.
• Use which incurs any unauthorized expense to College.

The list above is intended to provide examples of communications or activities which are contrary to this policy and purposes. This list is not meant to be all-inclusive and may be modified at any time.

System Network Access and User IDs
Employees will be issued a User ID with network and system access and security appropriate to their duties. System credentials control access to valuable information and should be protected accordingly. System passwords should not be divulged to others.

Information Security

Incident Reporting
Any observed or suspected breach of this policy should be reported immediately to the supervisor, the Director of Human Resources, or the Chief Information Officer.

Disposal of Equipment
All College owned computer equipment disposals will be performed by the Information Technology department. Contact the Help Desk for guidance.

Clear Desk Clear Screen
In order to protect information that has been entrusted to the College by employees, students and the community, the College promotes a clear desk and clear screen approach. Unattended computers must be locked or logged out and any print materials or electronic media containing operational or confidential information which is not currently being used must be securely locked away.

Other Violations of Electronic Privacy
Access to electronic files, network communications, and related data is protected by various state and federal statutes. Unauthorized access to an employee’s electronic data or transmissions is prohibited and may also subject the individual to civil or criminal penalties. Examples of specifically prohibited behaviors include:
• Unauthorized access, interception, monitoring, or diversion of electronic transmissions of another employee or third party.
• Accessing clearly operational or confidential files unless specifically authorized to do so.
• Accessing confidential information about a person (e.g., education records, personal e-mail) without their consent or other authorization.
• Downloading or installing unauthorized software that does not support College business objectives.
• Disabling College anti-virus, anti-spam, or other filters.
• Breaching, testing, or monitoring computer or other electronic media security measures.

Data Storage
All public, operational, and confidential electronic data generated for College use must be stored on approved network locations or systems. Data should not be stored on a person’s local computer (C: Drive, Desktop or My Documents), as this area is not covered under the Enterprise Backup procedure.

Recognition of Copyrights
Employees and students must follow copyright laws. Copying proprietary software is theft and will not be tolerated. Illegally copied software subjects the College to risk of litigation and denies software authors the compensation they deserve.

Similarly, an employee must follow copyright law when using or making materials available for others to retrieve or use. In general, every document, image, or sound is covered by copyright upon creation and may only be used or redistributed with the permission of the copyright holder.

Disciplinary Action
Exceptions to this policy must have prior authorization from the President or designee. Any violations of this policy may result in disciplinary action up to and including termination of employment.