Acceptable Use of Technology Resources Guidelines

Approved by: Timothy Hopkins, Chief Information Officer
Last updated: 2/4/2025 – *Included prohibition on sharing sensitive data with Artificial Intelligence-enabled software.*

1. Purpose

McHenry County College (MCC) provides a technology environment that promotes student success, teaching, research, and the efficient operation of MCC business and services. The College requires all Users of its Technology Resources adhere to standards of academic and professional ethics, codes of conduct and policies, and all applicable laws and regulations.

This document details the College's administration, ownership, and monitoring of its Technology Resources, as well as the proper use of those resources. The requirements contained within this document apply to all persons and all devices accessing or using any College information system or service.

2. Definitions

A. Authorized Users (Users): Students; employees (faculty, staff, and administrators); invited guests; community members; contractors and temporary employees; and all other persons granted authorized access or user privileges.

B. College Technology Resources: College-owned, operated, leased, licensed, or contracted networks, telephones, devices, systems, and services, whether local or hosted, individually controlled or shared, including:

- Wired and wireless networks
- Student and employee information systems and databases
- College provided email accounts and related services
- Networked and local storage systems and devices
- Telephone, smart devices, and other communication systems
- Accounts operated by the College, including social media and other hosted platforms
- College data maintained in electronic format

Users of College Technology Resources agree to abide by the requirements contained herein and in applicable guidelines and policy and procedure manuals, as well as state and federal laws, including but not limited to:

- Board Policy Manual
- Administrative Manual
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bailey Act (GLBA)
- Legal Hold directives
- Defamation

- Discrimination
- Fraud
- Harassment
- Identity theft

3. Requirements

McHenry County College recognizes that free expression of ideas is central to the academic environment. For this environment to flourish, all Users must adhere to the requirements contained herein.

The College voluntarily provides Technology Resources, with their primary purposes to meet the academic, research, administrative, and communications needs of its stakeholders. The use of these resources for other purposes is tolerated if usage is kept to a minimum, does not interfere with the function of any Technology Resource, and does not violate [a] any federal, state, or local law, [b] the College mission, Board policies, or Administrative procedures, and [c] requirements stipulated in this guidelines document. Users who make incidental personal use of College Technology Resources do so at their own risk. The College cannot guarantee the security or continued operation of any Technology Resource.

Access to any McHenry County College-owned and/or operated Technology Resource is a privilege and not a right. Individuals who refuse to follow these requirements will not be granted user accounts and/or may not be granted access to services/systems. Acceptable use is based on common sense, common decency and civility, and Users are subject to all policies, procedures, and processes which operate within the College.

4. Confidential Data

All Users should take all appropriate precautions to maintain the accuracy, integrity, and confidentiality of confidential data and ensure that no unauthorized disclosures occur. All Users must refrain from sharing confidential data with anyone not authorized to view or possess such data; this includes using sensitive data as part of an Artificial Intelligence prompt or any other software that will process and potentially store the data. All Users must comply with the provisions of any signed Confidentiality Agreement and all federal/state/local privacy laws and regulations, including GLBA and FERPA. No one, unless it is a function of their job position, may collect, store, disseminate, or disclose Personally Identifiable Information (PII) data. No PII data may be disclosed outside of the College unless there is legal, regulatory, or functional requirement to do so. PII data must be encrypted in transit and at rest.

5. College Ownership/ Monitoring

Technology Resources are the property of McHenry County College. The College's ownership of a file, record, data, or a message does not transfer ownership to the College of any intellectual property therein. Incidental

personal uses are permitted as provided herein. Records of electronic communications pertaining to the business of the College are considered Technology Resources.

The College President, College Legal Counsel, or Vice President of Human Resources may grant access to the account of a User to other College employees or designated individuals. Request for such access must be in writing and include:

1. What access/user account is being requested?

2. Why is this being requested?

3. Who is going to access this information and for what duration?

The College President, Legal Counsel, or Vice President of Human Resources will provide written authorization granting requested access.

6. Expectation of Privacy

All Technology Resources, including email accounts and shared storage, are provided by McHenry County College in furtherance of its mission. No representation has been made to Users as to the privacy of any communication or data stored on or sent through College Technology Resources. Users should have no expectation of privacy while using the College network or any other Technology Resource. Email and files that are sent, received, or stored using College Technology Resources are the property of the College. Email is not a secure form of transmission and must not be used to transmit sensitive data, including files with PII. MCC reserves the right, without notice, to limit or restrict any individual's use of any Technology Resource, and to inspect, copy, remove or otherwise alter any data, file, or system resource. MCC also reserves the right to periodically examine any system and any other rights necessary to protect its Technology Resources.

The College may monitor the activity and accounts of Users of Technology Resources, with or without notice, when:

- The user has voluntarily made information accessible to the public, as by posting to a blog or a web page
- It is necessary to protect the integrity, security, or functionality of any Technology Resource, or to protect the College from liability
- There is reasonable cause to believe that the user has violated, or is violating, the Acceptable Use requirements contained herein, or other College policies, procedures, or guidelines, or laws/regulations
- An account appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns
- It is otherwise required or permitted by law

The College, in its discretion, may also disclose the results of such monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies, and may use those results in appropriate College disciplinary proceedings.

The College reserves the right to access its Technology Resources, including current and archival files of Users' accounts if:

- That access would be imperative to conducting College business;
- There is strong evidence of improper usage; or
- There is strong evidence of impropriety.

Under the Illinois Freedom of Information Act, electronic files are treated the same way as paper files. Any inspection of electronic files, and any action based upon such inspection, will be governed by all applicable federal and state laws, and by College policies and procedures. Strong evidence would consist of a substantiated report or claim that could include, but is not limited to, physical evidence.

Under certain circumstances, the College may access and modify the contents of an email account. In cases concerning the health, safety, or welfare of any member of the College community, as determined by authorized College officials, the College may authorize accessing or modifying an employee's email account. In cases where personally identifiable information may have been inappropriately disclosed, authorized College officials may authorize modification of the email accounts of both senders and recipients.

MCC's Technology Resources are private, and all information stored on College-owned or contracted equipment is the property of the College (exceptions noted in Faculty Handbook).

The College may use tools to block electronic content and shape or restrict network bandwidth. These tools, such as anti-spam, anti-virus, and firewalls, will be used to ensure the security of the technology environment. Web sites and internet services may be blocked if they are known to spread viruses, spyware, adware, or other types of malicious software or service, harm or attempt to harm any College Technology Resource, or illegally host copyrighted material made available for download. Additional security measures may be implemented to protect the College technology environment.

User Responsibilities

MCC Users are responsible for all activity that happens on their accounts. All Users have the responsibility to use College facilities and all forms of Technology Resources in an ethical and legal manner. Users are expected to follow usage guidelines, and when necessary, receive and participate in training in the use of Technology Resource, including Confidential Information Training when hired.

All Users must:

- Maintain the privacy and security of all data
- Keep passwords confidential
- Comply with all information security policies and procedures
- Be responsible for the data stored on their own system, or in a shared network drive, by ensuring backups are maintained and controlling access, when appropriate
- Adhere to all laws and regulations regarding copyright and intellectual property
- Report any security incident or suspected misuse of any technology resource to the Chief Information Officer or designee.

All Users must not:

- Use any Technology Resource in any way that degrades any Technology Resource, including the network, or alters or makes inaccessible any other Technology Resource for any user or service
- Share passwords with anyone or otherwise grant access to another person (except IT personnel) to their own account, computer, or other resource provided by the College
- Obtain extra electronic resources or access to accounts for which they are not authorized

- Misuse, alter, or otherwise damage any data, computer equipment, or any other Technology Resource
- Engage or attempt to engage in any activity designed to spy on network traffic, to access other Users' accounts, passwords, files, or programs, or to introduce malicious or unauthorized programs into the Technology Resources environment
- Send, display or cause to display pornographic, obscene, abusive, racist or inappropriate language or material to any user or any Technology Resource. (NOTE: The College reserves the right to judge the appropriateness of displayed material on a case-by-case basis.)
- Install or uninstall software on any computer without prior written authorization or assistance from Information Technology
- Use College Technology Resources to send unsolicited Junk mail, relay mail, or forge or mislead the source and or destination of mail
- Install networked or other technology hardware (including wireless access points, cameras, IoT devices, smart speakers, etc.) without prior written authorization from the Chief Information Officer. Unauthorized equipment will be confiscated.
- Use any Technology Resource to support political or non-College related business interests
- Represent the College on social media unless authorized to do so by the Vice President of Marketing, Communications, and Development/Office of Marketing and Public Relations
- Disable, remove, or uninstall software designed to provide a secure computing environment, (e.g., anti-virus software, patches of existing software, etc.), on any College information system without prior approval from Information Technology.
- Sell, rent, or provide access to College's Technology Resources to outside individuals, groups, or businesses except as authorized by the Chief Information Officer for authorized College business relationships
- Engage in personal activities using College Technology Resources to the extent that it interferes with job performance

7. Enforcement

McHenry County College retains unfettered discretion to monitor, authorize, control, or stop the use of any Technology Resource at its sole discretion. Alleged violations of the Acceptable Use of Technology Resources Guidelines will be referred to the Vice President of Human Resources for investigation and action through the established disciplinary processes of the College. Violations may result in disciplinary action up to and including expulsion or separation from the College and legal action. In addition, the College may:

- Delete files or programs
- Inactivate user access privileges
- Inactivate or remove the user account.

8. Compliance with Legal Holds

All Users must comply with any legal hold directive from legal counsel, the Chief Information Officer or designee, the College President, or the Vice President of Human Resources. Users acknowledge that they

may be required to save and preserve, or conduct an exhaustive search, for certain electronic records pursuant to a legal hold.

9. The Freedom of Information Act and Illinois Local Records Act

This Acceptable Use of Information Technology Resources Guidelines does not amend or supersede any obligation under the Freedom of Information Act or the Illinois Local Records Act.