CHAPTER 4	SECTION NO.
College Operations	4.17
REFERENCE	*Adopted: October 12, 2010*
4.17 Use of Information Technology, Facilities & Resources	*Reviewed: October 12, 2012; July 17, 2012, August 9, 2022; August 12, 2025*
	Revised: July 17, 2012, August 9, 2022; August 12, 2025

Kishwaukee College provides employees with information technology equipment and systems that allow them to perform their duties as efficiently and effectively as possible in order to serve students, employees, employers, and community members. The Board of Trustees recognizes that each employee should have access to the College's information systems to serve these stakeholders. However, the College's information systems provide access to sensitive and confidential data and must be safeguarded to the highest degree. Therefore, College employees must be held to the highest degree of confidentiality and ethical standards in their use of the College's information systems and provided resources. Additionally, the importance of cybersecurity cannot be overstated in protecting these resources.

Scope
This policy sets forth the responsibilities of each employee as they utilize the College's information systems and technology resources. This policy is designed to protect the integrity of these systems from unauthorized, inappropriate, unethical, and criminal use. It applies to all employees, contractors, and any other individuals who have access to the College's information systems.

General Users Responsibilities Users are responsible for using College technology and resources responsibly and appropriately, adhering to the following guidelines:

- To use information, resources, tools, and systems for legal and authorized purposes to support College business and activities.
- To learn, understand, and follow the guidelines for each type of computer, lab, software, or other electronic resource.
- To comply with all College, federal, state, and local regulations regarding access and use of information resources, including the safeguard of confidential and proprietary information.
- To share proprietary information only to the extent authorized and necessary to carry out an employee's assigned duties.
- To only access those computing and information technology resources and data for which they have authorization and only in the manner and to the extent authorized.
- To ensure that persons to whom an individual account is issued are responsible at all times for its proper use. Passwords are assigned to approved users and may not be shared or transferred to someone else.
- To change system passwords in accordance with platform and current IT recommendations.
- To store work in network storage space. Files will be retained according to the College's Record Retention Policy.
- To connect devices to the College's secure network through approved and proper channels.
- To install software on College-owned systems only with authorization.

- To acknowledge that all content located anywhere on equipment, software, programs, or networks owned or maintained by the College may be reviewed by the College, its agents, and designees at any time for the purpose of investigating possible violations of Board Policies. Users have no reasonable expectation of privacy with regard to any such search of contents of files located anywhere on the computer or network equipment owned or maintained by the College.
- To log out or lock the desktop before leaving a computer unsecured.
- To complete annual cybersecurity training and be an active contributor to the protection of campus computing resources and cybersecurity.
- To report any suspicious activities or potential security breaches to the IT department immediately.

Generative Artificial Intelligence (AI)

AI technologies have the potential to significantly improve workplace efficiency and productivity but also carry risks. To ensure responsible and ethical use of AI, users are expected:

- To recognize that AI does not replace human involvement and to use it to apply critical thinking and thoughtful review of generated content for any content development in which AI is used as an aid.
- To protect confidentiality by refraining from inputting or otherwise sharing personally identifiable information (PII) (i.e. names, dates of birth, social security numbers, contact information) of employees, students, or other members of the College community or proprietary content belonging to the College into AI tools.
- To avoid misrepresenting ownership of AI-produced content and to disclose the role AI played in the development of work products as applicable.
- To ensure that all AI tools utilized are accurate, appropriate, unbiased, and comply with all applicable College policies, and any applicable federal, state or local laws or regulations, including but not limited to the Family Educational Rights and Privacy Act (FERPA).
- To verify that AI tools comply with data protection policies and do not store or share sensitive information without authorization. Consult IT for guidance when handling data.
- To stay updated with AI advancements and best practices, encouraging continuous learning and adaptation.
- To comply with the rules, guidelines, and procedures specific to their job function, role, or department when using AI technologies including but not limited to employees' respective duties and responsibilities as set forth in Chapter 2 of the Board of Trustees Policy Manual.

As technologies evolve, employees are expected to remain flexible, stay informed about changes, and adapt their practices to align with any new standards or requirements.

All employees will receive a copy of this policy and will acknowledge they received and understand the contents of the policy annually. This policy is also applicable to the Kishwaukee College Board of Trustees.

Failure to abide by the terms of this policy may result in disciplinary action, up to and including discharge and possible prosecution of the employee for any criminal usage of the systems.