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*
	Revised: July 17, 2012, August 9, 2022

<u>**Kishwaukee College Board of Trustees Policy Manual – 4.17 (Use of Information Technology, Facilities & Resources - Page 1 of 3)**</u>

It is the policy of Kishwaukee College, hereafter referred to as the College, to provide employees with information technology equipment and systems that allow them to carry out 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 in order 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 in their use of the College's information systems. This policy sets forth the responsibilities of each employee as they utilize the College's information systems. This policy is designed to protect the integrity of these systems from unauthorized, inappropriate and criminal use. All employees will receive a copy of this policy and will acknowledge that they received and understand the contents of the policy. This policy is also applicable to members of the Board of Trustees.

Internet and E-mail Access

Internet access and E-mail services have become extremely useful tools for conducting College business and delivering services. Internet access and E-mail services, while providing instant access to information, people, databases and courses, also presents a significant threat to the College's information systems as many criminals and computer hackers use the Internet and E-mail systems to gain unauthorized access.

General Principles

Internet, E-mail and text messaging privileges provided by the College's information systems, networks and equipment are considered College resources and are intended to be used for College purposes. Employees that have access to any of these resources are expected to use them in a manner that is consistent with common sense, common decency and the general guidelines in this policy. Usage may be monitored for unusual or unacceptable activity.

- The College E-mail systems and the information transmitted and stored within them are the property of the College. **Employees have no expectation of privacy or confidentiality in any of their E-mail or text messages or in connection with use of the College's technology systems except to the extent a user's confidential information is otherwise protected by federal or state law. Employee E-mail and text messages may be monitored for policy, security or network management reasons from time to time and are subject to inspection at any time.**

- The distribution of any information through the information and E-mail systems is subject to the scrutiny of the College and its auditors.

- External transmission of non-public student information without the student's authorization should not be performed unless sufficient encryption of a minimum of 128-bit strength is used. Contact the Information Technology Department or the Registrar for information on requirements for data encryption and for details on FERPA regulations, respectively

Cybersecurity and Training

Use of the information and communication systems provided by the College have become essential for business and security of these systems is imperative. In order to maintain the highest levels of security employees are required to complete assigned cybersecurity training.

Conditions of Use

Users will not:
- Knowingly visit Internet sites that contain obscene, hateful or other objectionable materials unless they are related to specific curricular objectives.
- Conduct College business using an E-mail account other than a College account.
- Use the information and E-mail systems for any illegal purpose.
- Use the information and E-mail systems to solicit non-College business for personal gain or profit.
- Use the information and E-mail systems to share offensive or vulgar messages that violate the College's policies against harassment and discrimination.
- Use the information and E-mail systems to participate in political activities excluding College-related union and retirement plan communications.
- Use the information and E-mail systems to represent personal opinions as those of the College or purport to represent the College when not authorized to do so.
- Use the information and E-mail systems to reveal or publicize confidential or proprietary information which includes, but is not limited to, financial information, confidential student information, marketing strategies and plans, databases and any information contained therein, student lists, computer software source code, computer and network access codes and business relationships.
- Share via social networking sites (i.e., Twitter and Facebook) confidential or proprietary information which includes, but is not limited to, financial information, confidential student information, marketing strategies and plans, databases and any information contained therein, student lists, computer software source code, computer and network access codes and business relationships.
- Transfer sensitive or confidential data files or E-mail messages to any non-College computer or portable storage device, including, but not limited to, personal E-mail accounts and USB flash drives, without authorization.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic, which substantially hinders others in their use of the network.
- Connect any computer workstation, notebook computer or other device to the College's secure network without authorization.

- Duplicate, upload, download or otherwise transmit shareware, freeware, commercial software or any copyrighted materials belonging to parties outside of the College without authorization.
- Install software of any kind on College-owned systems without authorization.
- Examine, change or use another person's files, output or username for which they do not have explicit authorization.
- Share passwords with any other person without authorization.
- Leave passwords exposed or easily accessible.
- Leave a computer unsecured without first logging out or locking the desktop.

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.