ADMINISTRATIVE POLICY
Policy Section: Information Technology

Policy Title: **ACCEPTABLE USE OF COMPUTERS AND ELECTRONIC DEVICES**

Purpose

The use of the Fox Valley Technical College (FVTC) network, computers, systems, and other electronic devices (e.g. desktop computers, laptops, tablets, cell phones) is a privilege provided by FVTC to support employment consistent with business objectives and to promote the interests of the College. Inappropriate use exposes FVTC to risks, including virus and malware attacks, compromise of network systems and services, and possible litigation. The purpose of this policy is to outline the acceptable, ethical, and lawful use of FVTC systems. This policy applies to all FVTC staff, faculty, as well as all personnel affiliated with third-party contractors and consultants. This policy applies to all College owned or College leased information systems, computers, and devices.

FVTC information technology resources, including College-owned equipment on and off campus facilities, computers attached to the network, and any associated resource or service are for the use of persons affiliated with the College, including authorized faculty and staff and students. Information technology resources are provided to further FVTC's mission of providing high-quality education and training that supports student goals, a skilled workforce and the economic vitality of our communities. The use of these resources should be consistent with this mission, this policy, other use and security policies, and other applicable regulations.

Users must only access information systems they are authorized to use, and are permitted to use them only in the manner and to the extent authorized. Ability to access such systems does not, by itself, imply authorization to do so. While the College makes its information systems available primarily for use in College-related instruction, learning, enrichment, and administrative activities, it realizes the need for personal use for the convenience of the campus community. Computer resources may be used for personal use to the extent that personal usage does not interfere with assigned responsibilities, and any personal use of College systems may not violate any College practice or policy. By using FVTC technology, all individuals, including, but not limited to, employees, customers, volunteers, and third parties, unconditionally accept the terms of this policy.

Acceptable use of FVTC information technology resources is based on common sense, decency, ethics, civility, and security applied to the computing environment. Authorized users may expect reasonable privacy with regard to all computer files and email. However, authorized personnel may access College-owned or networked computers, accounts, and data transmissions for maintenance and upgrades and to monitor or troubleshoot networks for related security, network audits, investigations, and/or legal requirements. If there is reasonable suspicion of misuse, accounts and transmissions may be accessed for investigative purposes when authorized by all three of the following positions: The Executive Team member responsible for the unit, the Vice

President of Human Resources, and the Vice President for Information Technology Services. Security analysis and maintenance systems whose purpose is to identify unauthorized use of a system may be used to monitor computer use. All data stored on FVTC systems is considered College property and is subject to review.

The College reserves the right to limit or restrict any authorized user's usage of the College's information systems; to copy, remove, or otherwise alter any information/data or system that may undermine the authorized use of the College's information systems; and to do so with or without notice to the user in order to protect the integrity of the College's systems against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage.

Authorized users of the College's information systems recognize that when they cease to be formally associated with the College (e.g. no longer an employee, student, faculty member, or contract of the College), their information/data may be removed from the College's information systems and equipment without notice.

Acceptable Use

General guidelines for the acceptable use of FVTC information systems are based on the following best practices and authorized users are expected to:

- Behave in a manner consistent with the College's mission and comply with all applicable laws, regulations, and policies, as well as applicable licensing and contractual agreements.
- Behave responsibly and respect the reputation of the College, and the integrity and security of College information systems and data at all times.
- Use information technology resources they are authorized to use and only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.
- Comply with information technology security policies and associated controls implemented by FVTC and protect credentialed accounts and non-public/sensitive data from unauthorized access.
- Only share data with others as allowed by applicable policies and procedures, and dependent on their assigned role.
- Accept responsibility for the content of their personal communications and may be subject to any personal liability resulting from that use.

Unacceptable Use

Any actions that compromise the integrity of the College, data facilities, networks, services, or resources are strictly prohibited. Examples of unacceptable uses include, but are not limited to, the following:

- Using the resources for any activity that violates federal or state laws.
- Using excessive data storage or network bandwidth or transferring unusually large or numerous files or messages.
- Introducing malicious software into any College information systems.
- Compromising sensitive or non-public information or allowing the unauthorized use of College information systems.
- Attempting to breach, disrupt, or circumvent the security of, or otherwise tamper with the network, communications or systems, or the devices of others at the College.
- Sending or storing harassing, intimidating, or abusive material.
- Misrepresenting your identity or affiliation while using information technology resources.
- Using someone else's identity and password for access to any information technology resources.
- Using the resources for political activities, including organizing or participating in any political meeting, rally, demonstration, soliciting contributions or votes, distributing material, surveying or polling for information connected to a political campaign, completing political surveys or polling information, and any other activities prohibited under the ethics act and/or other state/federal laws.
- Using the resources for personal commercial or for for-profit activities.
- Providing, loaning, or reallocating College information systems without approval.

This policy extends to networks and information technology resources outside of the College accessed via the Internet. Networks or information technology resource providers outside of the College may, in turn, impose additional conditions of appropriate use, which the user is responsible to observe when using those resources. Certain violations of this acceptable use policy may be reported to external agencies or law enforcement for investigation.

In a case where unacceptable use severely impacts performance or security, in order to sustain reasonable performance and security, Information Technology Services will immediately suspend an individual's access privileges.

Disciplinary Action

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

Adopted: 05/23/88
Reviewed: 04/12/2021
Revised: 04/12/2021