FingerLakes
COMMUNITY COLLEGE

Success. It's In Our Nature.

Policy Name: FLCC Technology Device Management and Use **Policy Number:** J-2

Functional Area(s) Responsible: Information Technology

Owner(s) of Policy: Information Technology

Most Recent BOT Approval Date: September 2011

Most Recent Review Date: Spring 2025

Most Recent Review/Revision Type: ☐ none ☒ minor/non-substantive ☐ substantive/extensive

Policy Statement:

Individual computing devices which utilize Finger Lakes Community College's networks must be managed and used in a manner which conforms to essential best practices.

Reason(s) for Policy:

To protect the FLCC computing environment from operational disruptions and security breaches while ensuring a quality IT experience for all users.

Applicability of Policy:

This policy applies to all technology which accesses the College's internal data networks.

Definitions:

Best Practices

For the purposes of this policy, essential Best Practices consist of the following:

- All operating systems and applications software must be of a current, supported version and receiving periodic updates.
- All devices which support Anti Malware must be equipped with an IT sanctioned updated version and scanned on a routine basis for the presence of viruses and malware.
- Personally owned devices may access the FLCC network through guest wireless networks only – they cannot be connected directly to hard-wired network ports except as specifically authorized by the Network Administrator.
- Users of devices on the College's networks must adhere to all relevant IT policies including the J8 - Responsible Network Use and J9 - Security of IT Systems and Data.
- Local storage of data on computing devices should be synchronized with OneDrive to avoid any loss of data in case of a computer crash. Generally, it is expressly disallowed for information which is regarded as sensitive by the Security of IT Systems and Data Policy to leave a college own storage device.
- Users who are assigned individual accounts may not share those accounts under any circumstances. In addition, they are responsible for keeping their passwords secure, utilizing an alphanumeric mix with a minimum of 14 characters or longer with required use of special characters for complexity requirements. Passwords should be changed no less than annually.
- All portable devices and laptops will have their hard drives encrypted by IT prior to release to the college community.
- All FLCC equipment will have standard security related software loaded

- If a college owned or managed cell phone is found to be compromised, IT has the ability factory reset as needed to protect college systems.

Related Documents:

- Security of IT Systems and Data Policy
- Network Usage Policy

Procedures:

Users of IT supported computing devices should adhere to the following standards– failure to do so can result in suspension of access to FLCCs technology.

- Employees should not load software on the device without prior IT approval. Requests for local admin rights may be granted on a temporary basis for this purpose.
- In the case where specialized software is approved, the user may have to assume the responsibility for periodic updates of the software.
- IT should be consulted before connecting any non-college owned device to a college owned or managed system, such as a network port, local PC or Laptop, printer, Audio/Video System, etc.
    - This does not apply to typical activities such as connecting your phone or personal laptop to the public Wi-Fi, your computer or thumb drive to a classroom or conference room device for instructional and/or administrative purposes/presentations.
- Any external storage device, such as thumb drives or external hard drives, must first be encrypted before storing any college data.
- Anyone that needs to move a desktop computer system or network printer from one location to another within the college needs to work with IT in advance. Devices are secured in relation to their physical location and may not work in the new location.

Personally-Owned Devices

Personally owned devices are not allowed to interact with college enterprise systems as it is not possible for IT to manage their security.

Oversight of Policy Implementation

The IT area is responsible for implementation of this policy. In that effort it may inspect software loads on individual systems, examine the effectiveness of password use, monitor cases where multiple users may be logged on to a single account, and to the extent possible determine the degree of adherence to the policy across the institution. In the event that a device is identified as being non-compliant with the policy, the IT Division may deny access for the device or user’s account until the problem is rectified.

Forms/Online Processes:

None

Appendix:

None