Success. It's In Our Nature.

Policy Name: Responsible Network Use **Policy Number:** J-9

Functional Area(s) Responsible: Information Technology

Owner(s) of Policy: Information Technology

Most Recent BOT Approval Date: Fall 2011

Most Recent Review Date: Spring 2025

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

Policy Statement:

Finger Lakes Community College provides network resources for the purpose of facilitating the academic and administrative work of College employees, students and authorized visitors. All users who are granted access to these resources are expected to utilize these networks in a manner which respects the operational integrity and efficiently of the College's user community. In addition, usage of these resources must be consistent with local, state, and federal laws. Failure to comply with this requirement for responsible network use, and the following specific policy guidelines can result in the loss of network access privileges. In enforcing these and related computer use policies, as well as in complying with the enforcement of federal, state, and local laws, the Division of Information Technology may monitor, inspect, and retain the contents of any data that flows on the college network.

Disclaimer

The information provided in this privacy policy should not be construed as giving business, legal, or other advice, or warranting as fail proof, the security of information provided through FLCC.

Reason(s) for Policy:

To establish formal compliance with the Higher Education Opportunity Act and the SUNY Information Security Guidelines.

Applicability of Policy:

All users of FLCC Network Resources should be familiar with this policy.

Definitions:

Unacceptable Use - includes, but is not limited to the use of FLCC's network resources:

- to interfere with the privacy, security, and legitimate work of others
- to intentionally interfere with the performance of the network
- to perform unauthorized copying or transmission of copyrighted material
- to attempt to violate any connected computer system's security
- to access data being transferred through the network or files on any computer connected to the network without the owner's permission
- to spread computer Malware designed to violate security, interfere with the proper operation of any computer system, or destroy another user's data
- in any manner which violates any federal, state, or local law

- involving the use of a username or account belonging to another individual
- for the transmission of material that is harassing or unlawful
- Writing down your username and password down on a sticky note
- Sharing your password with someone else

Related Documents:

The use of FLCC's network resources must also be consistent with the policies governing other IT resources connected to the network, including:

- Employee Computer Use policy
- Student Computer Use policy
- Security of IT Systems and Data policy
- Electronic Messaging and Acceptable Use policy
- Copyright Infringement Notification and Takedown Procedures Policy

Procedures:

In addition to the Responsible Network Use guidelines, network users should observe the following specific policy guidelines:

Efficiency of Network Use

It is the responsibility of the individual network user to utilize network bandwidth efficiently to avoid a negative impact on other users.

Security

Users must protect their personal accounts and passwords from unauthorized use.

Networked Devices and Software

Only authorized IT staff can connect or configure devices that are physically wired to the college network. Except as authorized by IT, personally owned devices may utilize the College network through wireless access only. Only authorized IT staff may install any form of network services software, including Peer to Peer (P2P) or other remote networking applications, on a system or server wired to the network. To enable compliance with the monitoring requirements of the Higher Education Opportunity Act, peer to peer file sharing software may not be used on the College network except when IT-installed or authorized.

In accordance with the Digital millennium Copyright Act, College policy also forbids the unauthorized copying, distribution, downloading and uploading of copyrighted materials on any device utilizing the College network or computing resources. Owners of wireless devices utilizing the College Network should note that the use of file share programs on the College network involves not only a violation of this policy, but can also create considerable personal liability. As of 2008, pre- litigation settlements offered by such copyright holders as the Recording Industry Association of America (RIAA) have started at $3,000 per incident. For personally owned devices utilizing P2P software, the file sharing component should be disabled. Details on disabling file sharing for P2P software are available on the Cornell University website at: https://it.cornell.edu/how-uninstall-filesharing-software

Use Consistent with the Operational Integrity of the Network

It is a violation of this policy to make any efforts to disrupt the security of the College's networks or other interconnected network such as the Internet. Examples include attempts to: initiate a denial-of-services attack; spread computer mailware or any other program designed to violate system or network security, and otherwise interfere with the proper operation of any computer system or destroy others' data. Also included as a violation of this specific policy guideline is the use of subterfuge to avoid being identified while using the network or any computer systems attached to it.

Intercepting or Scanning of Network Traffic

Except for the purposes noted under Responsible Network Use (above) it is a violation of this policy to attempt to access data being transferred through the network or files on any computer connected to the network without the owner's permission. This includes situations where the available data may not be adequately protected or secured. Any unauthorized efforts at scanning or intercepting network traffic will be treated as a violation of this provision of the network usage policy.

Forms/Online Processes:

None

Appendix:

None