SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **PEER-TO-PEER FILE SHARING**	Procedure 8.07.01

I. PROCEDURE

The purpose of this policy is to establish guidelines for the use and management of peer-to-peer (P2P) file-sharing applications and protocols on the College's network. This policy ensures compliance with state and federal laws while protecting the integrity, confidentiality, and availability of the College's information systems and data.

II. SCOPE

This procedure applies to all users, including employees, students, contractors, and third-party vendors, who access the College's network, systems, or devices. It governs the use of P2P file-sharing applications or any other technology that facilitates the sharing of files between devices.

III. DEFINITIONS

A. **Peer-to-Peer (P2P) File Sharing:** A decentralized file-sharing technology that allows devices to share files directly without the need for a central server. Examples include BitTorrent, LimeWire, and similar software.
B. **Unauthorized Content:** Any material that violates copyright laws, College policies, or state and federal regulations.
C. **Bandwidth:** The amount of data transmitted over a network connection in a given time, often affected by P2P applications.

IV. ROLES AND RESPONSIBILITIES

A. **Vice President for Information Technology:** Oversee the implementation of this policy and ensure compliance with applicable laws and standards.
B. **IT Division:** Monitor the network for unauthorized use of P2P applications. Implement technical controls to restrict or block P2P traffic as necessary. Report violations to the appropriate College authorities.
C. **Users:** Refrain from using unauthorized P2P applications on College networks. Ensure compliance with copyright laws and College policies. Report any suspected misuse of P2P applications to the IT Department.

V. POLICY REQUIREMENTS

A. **Prohibited Use:** The use of P2P file-sharing applications on the College's network is prohibited unless explicitly authorized by the IT Division for academic or administrative purposes. The sharing or downloading of copyrighted or illegal content is strictly forbidden and may result in legal consequences.
B. **Authorized Use:** Authorized use of P2P applications for legitimate academic or administrative purposes must be documented and approved by the IT Division. Users must ensure that such usage complies with applicable laws, regulations, and licensing agreements.
C. **Technical Controls:** The IT Division will employ firewalls, intrusion detection systems (IDS), and other network monitoring tools to identify and block unauthorized P2P activity. Bandwidth management techniques will be used to prevent P2P applications from degrading the performance of critical College systems.
D. **Compliance with Copyright Law:** All users are required to comply with copyright laws, including the Digital Millennium Copyright Act (DMCA). Any notices of copyright

infringement received by the College will be promptly addressed, and violators may face disciplinary action.

VI. ENFORCEMENT AND PENALTIES

Unauthorized use of P2P applications may result in disciplinary action, up to and including termination of employment, expulsion, or contract termination. Violations of copyright laws may result in legal penalties, including fines and criminal charges.

VII. REVIEW AND REVISION

This policy will be reviewed annually and updated as necessary to reflect changes in technology, laws, and best practices.

Legal References:

- North Carolina Statewide Information Security Manual, SCIO-SEC-316 - System and Communications Protection
- Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512
- CIS Controls v8, Controls 9, 13 (Limitation and Control of Network Ports; Data Protection)

Cross References:

- Policy 8.02 - Acceptable Use Policy
- Policy 8.10 - Information Security Program
- Policy 8.11 - Information Classification and Handling
- Policy 8.17 - Information Systems Operations Security

Previously Referenced as: Jan 2015 (4.05.07)

Adopted: January 2015

Revised: September 2025