



**MISERICORDIA
UNIVERSITY**

Origination 09/2021
Last Approved 08/2025
Effective 08/2025

Policy Steward Mark Reboli:
Networking and Telecommunications
Manager
Area IT, Networking
Group

Peer-to-Peer Policy

I. Reason for the Policy

Misericordia University is committed to preventing the illegal downloading and uploading of copyright material through peer-to-peer (P2P) file sharing. This policy addresses the use of P2P file-sharing and the University's compliance with relevant laws.

II. Policy Statement

The University prohibits illegal or unethical use of peer-to-peer applications. We ensure compliance with the Higher Education Opportunity Act (HEOA) and all other applicable laws and regulations.

III. Who Should Read This Policy

This policy applies to all users of the University's information systems or physical infrastructure, regardless of format. Each user is responsible for reading, understanding, and complying with this policy.

IV. The Policy

The university has implemented technical controls to monitor network traffic. All users must respect all copyright laws. Unauthorized distribution of copyrighted material and peer-to-peer sharing may lead to civil and criminal liabilities.

The University is not obligated to shield users from legal actions arising from alleged copyright infringements or other P2P or file-sharing software violations.

Users should recognize that material accessed via the Internet is not necessarily authorized for distribution. Content often requires payment and may not be authorized for free distribution.

The University employs bandwidth management technologies to prevent P2P programs from degrading

network performance. IT reserves the right to implement or adjust packet shaping, URL filtering, and traffic monitoring.

Should P2P applications degrade IT Resources, the University will be take appropriate action against the responsible user(s). Users should be aware that P2P applications may:

- Violate copyright, patent, trademark, or other intellectual property rights,
- Disclose confidential information,
- Jeopardize IT security.

The University enforces safeguards against the illegal exchange and distribution of copyrighted materials. Excessive bandwidth use and unauthorized distribution of copyrighted materials violate the Acceptable Use of Information Technology Resources Policy.

1. Compliance

The IT Department receives electronic notices alleging copyright infringement from various sources, including the RIAA, MPAA, and other organizations.

Upon receiving an allegation, IT staff will:

1. Investigate using the provided IP address, port, date, and time. Verified information will be matched with login and activity records to identify the user. Relevant details will be recorded in an IT-maintained database.
2. Send the user a warning letter via email with the original allegation. The letter will detail potential consequences and offer technical assistance to cease P2P activity.
3. If necessary, send a second warning notice to the Dean of Students for disciplinary action, including suspending network service for 30 days.

IT will not disclose the identity of an alleged infringer without a subpoena but may be required to do so if legally compelled.

The University educates students about P2P file-sharing through:

- This policy
- Announcements on the myMU portal
- IT portlet information on the myMU portal
- The Misericordia University Student Handbook

2. Currently Blocked Applications

The University does not list all sites except for major ones impacting network resources or linked to multiple cease-and-desist notices. This information is available in the myMU portal.

V. Definitions

Peer-to-peer applications - Programs that enable data sharing, such as music, movies, or software, directly between users over a network without a centralized server.

VI. Procedures

1. Procedures in Place to Reduce Illegal Peer-to-Peer file sharing

The IT Department periodically reviews information and updates procedures to address illegal P2P file sharing. The Department reserves the right to block abusive or dangerous file-sharing protocols and may restrict network access.

Approval Signatures

Step Description	Approver	Date
Final Approval	Daniel Myers: President	08/2025
Final Review	Mark Van Etten: Vice President, Finance and Administration	08/2025
	David Johndrow jr: Director of Information Technology	05/2025
	Mark Reboli: Networking and Telecommunications Manager	05/2025