Marywood University
Policies and Procedures

Copyright Compliance and Peer to Peer File Sharing Policy

I. Policy Statement:

Any individual using the Marywood University network is required to comply with all copyright laws and regulations of the United States, and the University's copyright and peer-to-peer (P2P) file sharing regulations as described in this policy.

II. Reason for Policy:

Marywood University fully complies with copyright laws and regulations, and regulates the use of peer-to-peer (p2p) file sharing activities on its network, which can be illegal.

III. Entities Affected:

This policy governs all users of Marywood University information technology resources machine or device (17 U.S.C. § 102). Copyright exists from the moment of creation of the work. Copyright protects the expression of an idea, but not an idea itself. Works of authorship include the following categories:

IV. Definitions:

Copyright: Under federal copyright law, copyright protection covers original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device (17 U.S.C. § 102). Copyright exists from the moment of creation of the work. Copyright protects the expression of an idea, but not an idea itself. Works of authorship include the following categories:

a. literary works, such as books, journal articles, text books, laboratory manuals, lectures, computer programs, monographs, glossaries, bibliographies, study guides, syllabi, work papers, unpublished scripts, lectures, and programmed instruction materials;

b. musical works, including any accompanying words;

c. dramatic works, including any accompanying music, live video and audio broadcasts;

d. pantomimes and choreographic works;

e. pictorial, graphic, and sculptural works, including works of fine, graphic, and applied art, photographs, prints, slides, charts, transparencies and other visual aids;

f. motion pictures and other audiovisual works, such as films, videotapes, videodiscs and multimedia works;

g. sound recordings, such as audiotapes, audio cassettes, phonorecords and compact discs; and

h. architectural works.

File Sharing: The practice of distributing or providing access to digitally stored information, such as computer programs, multi-media (audio, video), documents, or electronic books is known as File Sharing. It may be implemented through a variety of storage, transmission, and distribution models and common methods of file sharing incorporate manual sharing using removable media, centralized computer file server installations on computer networks, World Wide Web- based hyperlinked documents, and the use of distributed peer-to-peer (P2P) networking.

Peer-to-Peer (P2P): P2P technology enables millions of computer users around the world to find and trade digital files with each other. By using a P2P computer program, a user can scan the hard drives of millions of people and instantly acquire (download) content with the click of a mouse. At the same time, that user can enable the millions of people on the P2P network to copy the contents of their hard drive. Unlike email or instant messaging, P2P enables the transfer of billions of files among millions of people without knowledge of identity or even location. It is, essentially, a massive listing and public warehouse of digital content.

While P2P technology itself can be used for legitimate purposes, the predominant – indeed, almost exclusive – use of P2P networks has been to trade copyrighted music, movies, pictures and software. From a legal standpoint, this activity violates copyright holders' exclusive rights to copy and distribute their works.

V. Responsibilities:

As an academic institution, Marywood University respects creative expression and academic research. However, both academic and recreational accessing of information must follow all copyright regulations, including Article 1 of the U.S. Constitution and Title 17 of the United States Code (otherwise known as the Copyright Act), the Digital Millennium Copyright Act (DMCA), and this Marywood University policy.

If copyright infringement is found to have occurred through technological means, enforcement of the DMCA does not require the finding of any evidence of intent in order to find liability. Colleges and universities can be subpoenaed to identify infringers within their networks. Marywood University will comply with any court ordered requests it may receive seeking such information.

Notes:

1. Individuals using the network must comply with all copyright laws and policies when accessing or downloading copyrighted content.

2. If and when a copyright infringement notice is received, the University will follow the disciplinary procedures outlined in this policy (See: Procedures, section VI).

VI. Procedures:

In order to prevent and stop illegal downloading activity at Marywood University and protect the networks, the University has established polices regarding firewalls, network security, and bandwidth management. The purpose of these policies is to limit or block traffic which can negatively affect the network, giving priority to the traffic which supports the attainment of the University mission. Steps to educate users within the network about the nature of peer-to- peer file

sharing violations and other copyright infringement activities will form a central part of the enforcement of this policy. These procedures will be reviewed and modified in accordance with changing legislation.

Individuals who are in violation of copyright law will be subject to disciplinary action, which may include written warnings and suspension of network access. If violations are discovered within the University's networks, the University will take steps to investigate the activity, provide education regarding the offense, and impose sanctions on network activity, if warranted. Violations will be dealt with under the tenets of the University's *Acceptable Use of Information Technology Resources Policy*, the *Code of Conduct*, *Student Code of Conduct* and/or *Academic Honesty Policy*, as applicable.

When the University receives a notice of claimed copyright infringement, which includes relevant information necessary to verify and process the claim, the notice is processed through the University's DMCA response protocol, which follows:

Digital Millennium Copyright Act (DMCA) Copyright Violation Notice Response Protocol

In the event that Marywood University receives a valid DMCA violation notice regarding a University-owned IP address that is allocated to a valid client network, the following response protocol is followed:

General Procedures:

1. The IP address and time stamp listed in the DMCA notice is compared against University system logs in order to identify:

a. The potential validity of the claim, based solely upon network traffic audit logs.

b. The device utilizing the indicated IP address at the specified time stamp.

c. The username used to authenticate the identified device to the campus network.

2. The University's Information Technology Department will suspend the accused individual's network access and send an email notification of the suspension to the User Support Service and the Network Operations Group. The original infringement notice is included in this notification.

3. The Information Technology Department replies to the infringement notification, confirming that network access has been revoked. This reply is copied to the Network Operations Group, the University's Chief Information Officer, and the Vice President of Operations.

University Community Members (Student, Staff, Faculty and Guests):

A.) In addition to the general procedures defined above, the University will follow these procedures for university faculty members, staff, and students:

1. A member of the Information Technology staff schedules an appointment with the accused individual.

2. The staff member meeting with the individual prepares two paper copies of the infringement notice prior to the meeting.

3. At the meeting, the staff member presents the individual with one copy of the infringement notice and instructs him/her to retain it for their personal records. The staff member asks the individual to sign and date the second notice, and returns for purposes of record retention the original signed copy to the Information Technology Department and a copy of the original to the University's Human Resources office for record retention.

4. The staff member explains to the individual what it is that he/she are accused of, and where the accusation originated from.

5. The staff member directs the individual to available copyright education resources, including the University's *Copyright Compliance and Peer-to-Peer File Sharing Policy*.

6. The staff member informs the individual that his/her identity has not been disclosed to the complainant and that the University can only release this information in response to a properly issued subpoena.

7. The staff member informs the individual that they may either:

a. Deny the complainant's accusation – at which point the infringement claim becomes a legal matter between the individual and the complainant. The suspension of network access will remain until claim resolution.

b. Remove the infringing content and thereby regain network access. This does not guarantee that the complainant will not seek damages for the infringement.

B.) In all cases, the staff member educates the individual about our three-tiered violation process and the remedies involved for repeat offenses.

Procedures and sanctions for DMCA and peer-to-peer file sharing related violations are specified within a three-tiered structure for students.

On a first offense, the individual student must contact the Information Technology Department and indicate that he/she has removed the offending application, content, and/or malware from his/her networked device. Network access may then be re-enabled for that device. The Information Technology Department staff may reserve the right to verify the removal prior to re-enabling network access.

In the case of a second offense, the individual student must contact the Information Technology Department and indicate that he/she has removed the offending application, content, and/or malware from his/her networked device. Network access may then be re-enabled for that device. Information Technology staff may reserve the right to verify the removal prior to re-enabling network access.

In the case of a third offense the Information Technology Department will refer the individual student to the Vice President of the Office of Student Experience for adjudication of the alleged policy violations. The Vice President or designee will determine the appropriate sanctions and whether network access privileges should be restored to the individual.

C.) For the purposes of this policy, individual students committing less than three offenses within an academic year will be considered as having no prior offenses at the beginning of the following academic year, provided the offenses are resolved by the close of that academic year.

D.) Violations by faculty and staff will be referred to the appropriate academic Dean, administrative supervisor or department head.

University Guests, Contractors and other Third Parties:

A.) In addition to the general procedures defined above, the following procedure will be followed for University Guests:

1. If the accused is a university guest attending an approved conference or event, the Information Technology Department will:

a. Notify the Vice President of Operations of the complaint and obtain the contact information for the conference or event chaperone(s).

b. Electronically forward the notice to the chaperone(s), including the network account of the accused (if known) and the nature of the complaint.

c. Inform the conference or event chaperone(s) that the identity of the accused has not been disclosed to the complainant and that this information can be released only in response to a properly issued subpoena.

d. Suspend the accused's network access for the duration of their conference or event.

2. For all other University Guests, Contractors of Third Parties, the Information Technology Department will:

a. Attempt to contact the accused and/or University sponsor, if known.

b. If the accused or University sponsor is identified, the Information Technology Department will electronically forward the notice to the accused.

c. Suspend the accused's network access until it can reasonably be determined by the Chief Information Officer, in consultation with University Administration, that network access should be restored.

VII. Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (17 U.S.C. §106). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion,

also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the web site of the U.S. Copyright Office at http://www.copyright.gov/, especially their FAQ's at www.copyright.gov/help.

Policy History: 2025-05-22: The President approved this policy as recommended by the Policy Committee at their May 9, 2025 meeting.

Related Committees and Policies:
Acceptable Use of Information Technology Resources Policy
IT Configuration Management Policy
IT Security and Privacy Request for Exemption
IT Security for 3rd Party Partners and Providers
IT Security Incident Response
IT Security Framework
IT Security for IT and Data Professionals
University Website Policy

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES

Mary Theresa Gardier Paterson, Esquire
Secretary of the University and General Counsel