University of Scranton

Division of Information Technology

Copyright Compliance and Peer-to-Peer File Sharing Policy

Executive Sponsor:
Associate Vice President for Information Technology/CIO

Responsible Office:
Information Security

Originally Issued: 2005
Revised: 12/2021
Reviewed: 12/2021

I. Policy Statement

Any individual using the University of Scranton 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

The University of Scranton 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 By This Policy

All users of University information technology resources are governed by this policy

IV. Website Address for this Policy

http://www.scranton.edu/information-technology/policies.shtml

V. Related Documents, Forms, and Tools

Related policy documents and/or other university and external documents:

1. The University of Scranton Copyright Policy
2. The University of Scranton Acceptable Use of Information Technology Resources Policy
3. Legal Downloading Alternatives: http://www.educause.edu/legalcontent

VI. Contacts

For policy clarification and interpretation, contact the Associate Vice President for Information Technology/CIO at 570-941-6185. For legal advice and interpretation of law, please contact the Office of General Counsel at 570-941-6213.

VII. 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manuals, lectures, computer programs, monographs, glossaries, bibliographies, study guides, syllabi, work papers, unpublished scripts, lectures, and programmed instruction materials;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. 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 his or her 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.

VIII. Responsibilities (required)

As an academic institution, The University of Scranton 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 the University of Scranton's Copyright 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. The University of Scranton will comply with any court ordered requests it may receive.

Notes:

1. Individuals using The University of Scranton 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 by The University of Scranton, the University will follow the disciplinary procedures outlined in this policy (See: *Procedures, section IX*).

IX. Procedures

In order to curb illegal downloading activity at the University, and protect our networks, a number of firewalling, network security, and bandwidth management policies have been implemented by the University. The purpose of these policies is to limit or block traffic which can negatively affect the network, giving priority to that traffic which supports the attainment of the University mission. Steps to educate users within our 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 our 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, Student Code of Conduct and/or Academic Code of Honesty, 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 the University of Scranton 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 that was utilizing the indicated IP address at the specified time stamp.
    c. The user name that was used to authenticate the identified device to the campus network.
2. The University's Information Security Office suspends the accused individual's network access, and sends an email notification of the suspension to the Technology Support Center (TSC) and the Network Operations Group. The original infringement notice is included in this notification.
3. The Information Security Office 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 Office of General Counsel.

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

A.) In addition to the general procedures defined above, the following procedure will be followed for University Student, Staff, Faculty:
    1. A member of the TSC 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 the second copy, and returns this signed copy to the Information Security 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 policy.

6. The staff member informs the individual that his/her identity has not been disclosed to the complainant and that this information would have to be subpoenaed in order to be released.
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; have the removal verified by a staff member, 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 may contact the Technology Support Center 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. TSC staff **may** reserve the right to verify the removal prior to re-enabling network access.

In the case of a second offense, a staff member must verify that the offending application, content, and/or malware has been removed from the individual's networked device. Upon removal confirmation, network access may be re-enabled for that device.

In the case of a third offense, the individual will be referred to the Office of Student Conduct for adjudication of their policy violations. The Office of Student Conduct 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 a conference or event through University Conference Services, the Information Security Office will:
    a. Notify University Conference Services of the complaint and obtain the contact information for the conference or event chaperon(s).
    b. Electronically forward the notice to the chaperon(s), including the network account of the accused (if known) and the nature of the complaint.
    c. Inform the conference or event chaperon(s) that the identity of the accused has not been disclosed to the complainant and that this information would have to be subpoenaed in order to be released.
    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 Security Office will:
    a. Attempt to contact the accused and/or University sponsor, if known.
    b. If the accused or University sponsor is identified, the Information Security Office 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.

X. Appendix

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/faq