

The University of Scranton
Peer-to-peer File Sharing Policy for Students, Faculty, and Staff

Peer-to-peer file sharing is a type of technological networking whereby files, such as music or video, are shared. When copyrighted files are shared the activity can be illegal. Recent legislation can require colleges and universities to identify users on their network who have engaged in illegal downloading. The following policy describes The University of Scranton's regulation of peer-to-peer file sharing within its network.

1. As an academic institution, the 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), and the Digital Millennium Copyright Act (DMCA). If copyright infringement is found, enforcement doesn't 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 will comply with any court ordered requests it may receive.
2. As stated in the University's responsible computing codes for students, faculty, and staff, individuals who are in violation of copyright law will be subject to disciplinary action, which may range from written warnings to 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.

Faculty and staff violations will be dealt with under the tenets of the University's Code of Responsible Computing for Faculty and Staff¹.

Student violations will be addressed under the Student Computing Policy², and specifically by the following protocol. There are three primary ways in which a student can end up in violation of this policy:

- a. The University receives a DMCA infringement notice that cites the student's IP address as the alleged offending source. The University verifies this information against its own Internet activity logs. The offense is processed via the University's DMCA response protocol for student violations (see page 3).
- b. The University's networking monitoring technologies detect that student's computer is operating a disruptive peer-to-peer application. The individual will receive an automated warning via email instructing them to cease this

¹ Accessible at: http://academic.scranton.edu/department/helpdesk/html_old/facultypolicy.html

² Accessible at: http://academic.scranton.edu/department/helpdesk/html_old/studentpolicy.html

activity. If the individual does not comply within a reasonable amount of time, network access for the machine operating the disruptive application is suspended.

c. The University's network monitoring processes determine that a student's machine is infected with malware (such as a virus or spyware), or is under the remote control of a malicious third party. The network access for the machine hosting the threat is suspended.

In the event of either of the violations described in points b and c, offenses will be handled by a three-tiered penalty structure³. The first step for each of these responses is suspension of network access for the machine involved. If this is the student's first offense, the student can contact the HelpDesk and indicate that they have removed the offending application and/or malware from their PC. Network access is then re-enabled.

In the case of a second offense, a residential network consultant (ResCon) is dispatched to verify that the offending application and/or malware has been removed from the student's PC. Upon this confirmation, network access is re-enabled.

In the case of a third offense, the student will be required to meet with the Office of Judicial Affairs to discuss their policy violations. The Office will determine whether or not network access should be re-enabled; to restore access, the student is required to pay a fine of \$50. For those who do not commit a third offense, their offense count is reset to zero at the beginning of the following academic year.

3. 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.
4. Steps to educate users within our network about the nature of peer-to-peer filesharing 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.

³ DMCA infringement notices also count toward at student's "three strikes."

University of Scranton
Digital Millennium Copyright Act (DMCA)
Student Copyright Violation Notice Response Protocol

In the event that the University of Scranton receives a DMCA violation notice regarding a University-owned IP address identified in connection with a student user on the University network, the following response protocol is followed:

1. The IP address and timestamp listed in the DMCA notice is compared against University server logs to identify the individual user who has incurred the violation.
2. The University's security officer suspends the student's network access, and opens a Help Desk "ticket" in Wonderdesk⁴. The infringement notice is attached to the ticket.
3. Security Officer replies to infringement notification stating that network access has been revoked for the alleged infringer. This email is copied to the ResNet Operations Group and the University's chief information officer.
4. A ResNet Ops member picks up the help desk ticket and schedules an appointment with the student to discuss the violation and educate them about acceptable network activity. Meeting details are added to the ticket. Should the student contact the Help Desk prior to ticket ownership, the Help Desk employee should update the ticket with the student's personal phone number information.
5. Ops member should print two copies of the infringement notice and bring them to the meeting with the student.
6. The Ops member will present the student with one copy of the infringement notice, have the student sign the second copy and return this signed copy to the Security Officer.
7. The Ops member will explain to the student what it is that they are accused of, and where the accusation is coming from.
8. The Ops member will direct the student to copyright education resources.
9. The Ops member will inform the student that their identity has not been disclosed to complainant and that this information would have to be subpoenaed in order to be released.
10. The Ops member will inform the student that they may either :
 - a. Deny the complainant's accusation – at which point the Infringement becomes a legal ordeal between the student and the complainant. The student's network access will remain revoked until resolution.
 - b. Remove the infringing content, have this removal verified by a ResCon, and regain network access. This does not guarantee that the complainant will not seek damages for the infringed content.

⁴ Wonderdesk is the system the Help Desk uses to log customer calls. A "ticket" is synonymous with a "call" or "case". Each "ticket" is assigned a reference number for easy identification.

12/19/2007

11. The Ops member will educate the student about our three-tier violation process and the recourses involved in repeat offenses.