

University of Wisconsin - Stevens Point Information Technology (IT)

Discouraging P2P File Sharing

Procedure No. 6

Date Drafted: 5/5/2015

Date Approved:

Last Date Revised: 4/26/2019

Status

Draft

Under Review

Approved

Obsolete

Responsible University Office

Information Security Office

Responsible Coordinating Office

Information Technology

1. Procedure Purpose

The purpose of this procedure is to define how UWSP discourages its network users from using Peer-to-Peer (P2P) file sharing application software to illegally share files such as music and videos.

(NOTE: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Common Definitions Policy document)

2. Procedure Scope

UWSP must comply with the Higher Education Opportunity Act of 2008 (HEOA) which calls for methods to be employed to discourage or block P2P network traffic. Since not all P2P traffic is illegal, and since it is nearly impossible to block P2P network traffic, UWSP employs several strategies to discourage illegal file sharing via P2P applications.

3. Procedure Statement

UWSP discourages our network users from illegally sharing files via the Internet in a number of ways to comply with the HEOA.

All use of the UWSP network is governed by the following policies:

- The Board of Regents “Acceptable use of Information Technology Resources” policy:
<https://www.wisconsin.edu/regents/policies/acceptable-use-of-information-technology-resources/>
- UWSP Information Technology’s guidelines/policies:
<http://www.uwsp.edu/infotech/Pages/Policies/Policies.aspx>.

DMCA Notice Response

When a Digital Millennium Copyright Act (DMCA) violation notice is received, the Information Security Office determines whether the offending Internet address (IP) corresponds to a student or an *employee*.

If the notice applies to a **student**, the network access of the offender’s device is limited to certain University resources, such as the UWSP website, campus email, and course management system. When attempting to access any other Internet resource, the offender will be redirected to a University webpage indicating that their network access has been restricted due to a Copyright violation.

Differing levels of action will be taken depending on the number of violations generated by the student:

- **First Violation:** Internet access of the offending device is restricted when the DMCA notice is processed. Restrictions will remain in-place until three days after the offender acknowledges receipt of their DMCA notice.
- **Second Violation:** Internet access of the offending device is restricted when the DMCA notice is processed. Restrictions will remain in-place until the offender meets with the DMCA Officer, with a minimum restriction period of seven days.
- **Third Violation:** Internet access of the offending device is restricted when the DMCA notice is processed. Restrictions will remain in-place indefinitely, and will only be restored at the directive of the Dean of Students.

If the notice applies to an **employee**, the Information Security Office will send an email message to the campus Human Resources Director announcing that a named employee has violated Copyright Law. A portion of the original infringement notice is incorporated into the message, including the notice ID number and a description of which file was illegally shared and when the sharing occurred.

Employee discipline is meted out by the Human Resources Director and the employee's supervisor according to campus disciplinary policies and procedures.

(NOTE: Phrases shown in *italics* at their first occurrence in this document are defined in the associated IT Common Definitions Document)

4. Terms and Definitions

A common set of terms and definitions used in IT policies are defined in the IT Common Definitions document.

5. Related Policies, Procedures, References, and Attachments

The collection of University of Wisconsin - Stevens Point - IT policies and procedures contain acceptable use, security, networking, administrative, and academic policies that have been developed to supplement and clarify University of Wisconsin - Stevens Point policy.

- IT policies and procedures are available at <http://www.uwsp.edu/it/policies/>.
- IT Procedure – Policy Development, Approval, and Implementation
- IT Reference – Common Definitions

Contact Information

For questions about this IT policy, contact the Director of Information Technology/CIO.