



Approved By: Eric Behrens, Vice President of Library and Information Services and Chief Information Officer

Issue Date: February 2018

Revision Date(s): no revisions

Related Policies or Procedures: Information Security and Compliance Program

Additional References:

Higher Education Opportunities Act of 2008 (HEOA) [34 CFR Section 668]

Responsible Officer: Widener University Chief Information Officer (CIO)

Policy:

It is the policy of Widener University that the abuse of network resources to illegally obtain and distribute media or software, through peer to peer (P2P) networks, Usenet, or direct download, is not permissible. While Widener University recognizes that there are legitimate uses for the previously mentioned applications, the University also understands that significant risks are implicit in the use of such applications.

Widener maintains a campus network to support and enhance the academic and administrative needs of our students, faculty, staff, guests and community. The University is required by federal law to inform the University community that illegal distribution of copyrighted materials may lead to civil and/or criminal penalties. The law also requires that the college take steps to detect and punish users who illegally distribute copyrighted materials.

This policy shall apply to all computer workstations, laptops, servers, networked appliances, and any other device if such device is owned by Widener University; or any device utilizing University network resources, even if that device is privately owned by an individual or third party. This policy applies to all individuals, regardless of affiliation or status with the University, at such time they are using the University network.

This policy strictly prohibits, by any method, the distribution, downloading, uploading, or sharing of any material, software, data, document, sound, picture, or any other file that is:

- Specified as illegal by any federal or state law, statute, proclamation, order, or decree.
- Copyrighted and not authorized for distribution by the copyright owner.
- Considered to be proprietary, privileged, private, or otherwise vital to the operation of the university; including, but not limited to, personnel, student, financial, or strategic records and documents, or any material governed by federal and state regulations.



- Any virus or malicious software for the purpose of deployment or implementation with ill-intent.

Any illegal or copyright-infringing P2P activity is strictly forbidden in the cases of:

- Computer labs.
- Computer workstations and other network devices readily accessible to multiple users.
- Computer workstations and other network devices used in daily operation by areas and departments heavily affected by federally mandated regulatory compliance.
- Laptops, computer workstations, tablets, cell phones and any other network capable device whether owned by Widener or privately owned by an individual.

Users of Widener University resources may not attempt to circumvent, bypass, defeat, or disrupt any device, method, or technology implemented by the university for the purpose of P2P mitigation.

Individual departments, colleges, administrative areas, students, faculty and staff and other entities must respond in a timely and efficient manner to all inquiries and complaints that arise in regard to this policy.

Technology Measures

Widener University has implemented technology designed to mitigate illegal Peer to Peer (P2P) activity. This technology is designed to:

- Allow legal P2P traffic (certain paid-for commercial services).
- Limit all P2P bandwidth to preserve network usage for business and educational use.
- Detect, monitor and block illegal P2P traffic
- Notify internal departments regarding suspicious and malicious use of University resources

Violation notification process

Any faculty, staff, or student found to have violated this policy may be subject to disciplinary action, conducted in keeping with the guidelines established by University policy. This includes relevant sections of the Faculty, Employee, and Student Handbooks, as required. Judicial proceedings that are adjudicated by Widener University will be resolved in the manner stated in the appropriate handbooks and policies applicable to the status of the user. Illegal acts involving Widener University computing resources may also be subject to prosecution under local, state and federal laws.



Any external entity, contractor, consultant, or temporary worker found to have violated this policy may be held in breach of contract, and as such, may be subject to grievances or penalties allowed by such contract.

Any individual, regardless of their affiliation or status with the University, can have their wireless Internet access permanently suspended for egregious or multiple violations of this policy.

A notice of alleged copyright violation that complies with the Digital Millennium Copyright Act will be referred to as a "DMCA Notice." DMCA notices received by the University as a result of abuse while utilizing an individual wireless internet access account will be researched, and if possible matched with the individual responsible for the abuse.

Students:

- Student's network access is suspended and students are required to bring their devices to ITS for inspection.
- Students are required to sign a notice acknowledging the P2P content on their device.
- Security investigation is performed, and further determination will follow the Student Handbook.

Faculty, Staff and other University employees:

- Network access is suspended and the device is inspected by ITS.
- Employee is required to sign a notice acknowledging the P2P content on their device.
- Security investigation is performed, and further determination will follow the appropriate employee Handbook.

For all Guest/Temporary access:

- The access to the wireless network is revoked and permanently banned if the University receives just one DMCA notice linked to the account, or on any other offense of this policy.



Links to Alternate Resources (Note: These links will take the user to websites not managed by Widener University).

Music	Video
Center for Copyright Information	Center for Copyright Information
Apple iTunes	Apple iTunes
Amazon MP3	Amazon Movies & TV

Purpose:

The purpose of the policy is to ensure compliance with the Higher Education Opportunities Act of 2008 (HEOA) [34 CFR Section 668]. The HEOA specifically requires Universities to take steps to eliminate illegal downloads and P2P abuse.

Effective:

This policy is effective once reviewed and approved by the Information Security Compliance Committee and the Executive Team of Widener University.