

WPI Information Technology

Network Usage Standard

Purpose

WPI's network is essential to the school's day-to-day operations. It handles academic, administrative, and research processes, as well as traffic from its campus residents. It is important that proper management and use be maintained at all times for acceptable performance and functionality. This standard will help define what can and cannot be performed on the network. It explains the following information:

- Background.
- Limits of the WPI network.
- Expectations upon the network users.
- Ramifications of failing to follow this standard.

Scope

This standard covers every machine and user that connects to the WPI wired or wireless network.

Background

The WPI network was created to facilitate WPI's business and academic progress, as well as pass useful and timely information to the WPI community. Commercial activity on the WPI network is only permitted for business done on behalf of WPI or its organizations, not for the benefit of private individuals or other organizations without authorization. This business activity must be authorized by WPI.

Since the WPI network is for the use of the entire university, denying its use through the forms of excessive traffic, running prohibited network equipment, or circumventing or exploiting security vulnerabilities to disrupt normal operations is prohibited. The network must be available at all times for all members of the university.

Network bandwidth is a finite resource that is managed in a reasonable fashion. Despite being an acceptable use of network bandwidth, network-intensive research work and other such enterprises should always be cleared with WPI Network Operations before proceeding. Also, non-academic applications may be blocked or limited in use if found to be causing problems with normal day-to-day operations.

Violations of privacy through network sniffing are not allowed. Although a useful diagnostic tool, it is too easy to disrupt normal operations or violate the privacy of others using a sniffer. Classes that are believed to need sniffers should contact Information Security (itsecurity@wpi.edu (<mailto:itsecurity@wpi.edu>)) before the class begins to work on these issues.

The University views personal network connections as a privilege and not a right for community members. The university reserves the right to suspend or eliminate personal computers from its network should they pose a business risk. Personal servers that are not owned by the university and perform a significant amount of non-academic related work are prohibited.

WPI users are required to register their systems for the WPI network and must only register machines that they own and use. Users are responsible for the activities on the machines that are registered to them, and will be held accountable for any legal or policy violations that occur. Systems for non-WPI community members (i.e. significant others, friends, family, etc) are prohibited either for full-time or casual use.

Standard

Users must register the system they own and use, and provide accurate registration information.

The following activities are prohibited:

- Abusing network bandwidth by using over 25 Gigabytes of external Internet traffic in a day or more than 75 Gigabytes of external Internet traffic for a 7 day period. Exceptions may be made for academic, WPI operational, or research work.
- Running a private business or advertisements on the WPI network.
- Reselling WPI network resources is not permitted.
- Disrupting normal operations for other users via excessive internal bandwidth (i.e. broadcast a storm of packets, causing excessive network traffic, making the network run slowly for others.).
- Running unapproved network equipment. See the list of Prohibited Activities (<https://www.wpi.edu/Academics/CCC/Netops/Policies/no.html>) for an up to date list.
- Circumventing security or exploiting security vulnerabilities, at WPI or on other networks.
- Sniffing, and other forms of network wiretapping. Faculty or staff needing sniffers for academic pursuits will contact Information Security prior to their use.
- Registering networked systems that are not directly owned or managed by the registrant, or are registered for those outside the WPI community

Consequences

Minor Offense: Faculty, staff, and students will be warned and this policy will be explained. Computers and resources that are mediums for the violations may be disabled until the owner has a discussion about the violation. A second minor offense counts as a major offense.

Major Offense: Faculty, staff, and students will need to speak with a member of Information Security about the violation. A student's network access for their personal computers will be suspended from the point the second violation is discovered to one week after the violation is explained and a notice will be sent to the Student Affairs Office. A second minor offense counts as a serious offense.

Serious Violations: Faculty, staff, and students will need to speak with a member of Information Security about the violation. Those students with repeat offenses or who exhibit malicious intent to compromise, disrupt, or circumvent security will be referred to the Dean of Students Office for resolution, which may include forwarding to the Campus Hearing Board (CHB). The student will have their network access for their personal computers suspended pending the resolution of the case. Other computing resources may be suspended if they were involved in the student's transgressions.

Concerns

Please email any concerns or comments to itsecurity@wpi.edu (<mailto:itsecurity@wpi.edu>).

Revisions

In order to stay current with the changing policy environment and network architecture, this standard is reviewed yearly. Changes are made when necessary.

Revision History

August 19, 2008 - IT approved the standard.

October 20, 2008 - Minor clarifications at the request of CITP

August 10, 2009 - Updating bandwidth limits, judicial review, and other minor changes.

August 20, 2010 - Updating bandwidth limits

August 22, 2013 - Updating bandwidth limits

Maintained by [itweb \(/Academics/CCC/Help/Services/form.html\)](#)
Last modified: Aug 22, 2013, 13:36 EDT

Information Technology - Worcester Polytechnic Institute
100 Institute Road, Worcester, MA 01609-2280
Phone: +1-508-831-5531 - Fax: +1-508-831-5483 - [itweb \(/Academics/CCC/Help/Services/form.html\)](#)