



WPI

Acceptable Use Policy (AUP)

Introduction

Worcester Polytechnic Institute (WPI) maintains computing resources, including data and information, which are essential to performing University business. These are WPI assets over which the University has both rights and obligations to manage, protect and utilize to fulfill its mission. The Acceptable Use Policy was established to create usage standards in compliance with other University policies as well as regulatory requirements.

This Acceptable Use Policy (AUP), the Campus Code of Conduct, the Administrative Data Management Policy, and several other university policies govern WPI's computing resources collectively.

- [Policies](#)
- [Acceptable Use Policy \(AUP\)](#)

Purpose

The purpose of the AUP is multifold, as identified below:

- Educate the WPI community about the policies on the use of electronic facilities.
- Ensure all members of the WPI community have appropriate access to functional and safe technology resources.
- Prevent any misuse of, or damage to, computer assets or data.
- Clarify the application of the Code of Conduct to specific computer and network technologies.
- Assist the University and employees in complying with federal and state legislation regarding information security, privacy, disclosure, computer crime, and other information and computer legislation.

Scope

This policy applies to all users of WPI technology resources. It applies to any systems, software, components, or data that are connected to or utilize the WPI network and its computer systems. It applies to both academic and non-academic communication and activities.



WPI

Policy

Comply with the intended use of any system or service at WPI.

All systems and services available at WPI are used for academic and campus business priorities, with non-academic use being a secondary activity. Users shall comply with WPI's technical, administrative, and process controls. Users will not engage in disruptive activity that could cause a failure or degradation of systems or services used by others. Users will not subvert a system or service for illegal or inappropriate use as defined by the usage standards, WPI Student Code of Conduct, and Employee Handbook.

Ensure the ethical and legal use of WPI technology resources.

Users must not use any WPI system or service for unethical or illegal activities. Users shall respect the privacy of others, use data only as authorized by the data owner, and not use WPI technology resources to harass or attack others. The University and WPI community members are subject to and must comply with, federal, state, and local laws.

Respect WPI property and resources.

Users must obey technical and administrative controls regarding access. Users shall not take technical means to bypass these controls. Users must not grant access to WPI resources to users outside the WPI community without the express permission of the university. WPI retains the right to review and audit any university-owned electronic communication devices, connections, and services to ensure compliance with WPI policies. WPI retains the right to deny network access to any non-WPI owned electronic communication devices.

Respect the personal property and privacy of other users.

Users must ensure they handle University and personal property within the guidelines set by the property owner. Users must not invade the privacy of others by illicitly monitoring the network traffic of others or accessing private files without permission. Users must respect copyright regulations and the personal copyright of others.

Use the WPI network and computing resources for non-commercial purposes only.

The WPI network and computing systems may not be used for commercial use, to host advertising, or to create digital currencies. Users may not resell WPI computing or network resources. Such usage is inconsistent with WPI's academic and research missions and WPI's non-profit status.

Standards

The Acceptable Use Policy is administered through a collection of standards. The WPI Acceptable Use Policy and its standards are in effect at all times. The WPI Information Technology Services works in concert with the Dean of Students Office, the Campus Hearing Board, and Human



Resources to ensure fair and appropriate investigation, consideration, and consequences where appropriate. Users are expected to familiarize themselves with the standards and comply with them.

- [Network Usage Standard](#)
- [Responsible Copyright Standard](#)
- [Common Website Usage Standard](#)
- [Common Electronic Mail Standard](#)
- [Proxy Usage Standard](#)

Exceptions

Exceptions to the Acceptable Use Policy and its related standards are granted on a case-by-case basis. If an exception is requested, Information Security will work with the requestor to help determine the best course of action to minimize and possibly eliminate any such conflict. Exceptions for academic coursework can be requested by a Faculty member.

University Response to AUP Violations

First and/or Minor Offenses: Students and employees will have a meeting with a member of Information Security to discuss how the individual's activities may have deviated from the AUP Policy or Standards. During the meeting, the AUP Policy will be reviewed with the individual to ensure understanding. The discussion will be conversational in nature and non-adversarial, with the goal of both educating and preventing further offenses. As such, the discussion will serve as a warning. Computers and resources that are registered to the individual may be disabled until the owner has had a discussion about the incident.

Repeat and/or Serious Offenses: In the event of suspected repeat offenses, students will have a meeting with a member of Information Security to discuss the further offenses. During the meeting, the alleged violations and the AUP policy will be reviewed. If the student admits responsibility for the violations, they will sign an AUP Administrative Agreement. As part of the resolution to the incident, computers and resources that are registered to the individual may be disabled for up to one week following this meeting. The AUP Administrative Agreement and supporting documentation will be filed with the Dean of Students Office and a formal judicial record will be created. If the student does not admit responsibility for the alleged violation, the case will be forwarded to the Dean of Students Office for resolution.

For students, alleged violations of a more serious nature (e.g. activities which exhibit malicious intent to compromise, disrupt, or circumvent security of the AUP Policy) may be referred to the Dean of Students Office and/or the Campus Hearing Board for resolution. Please refer to the WPI Student Code of Conduct for a full description of judicial resolution processes. Computers and



resources that are registered to the individual may be suspended pending the resolution of the case.

If an employee is involved with suspected repeat violations of the AUP, the employee will have a meeting with a member of Information Security to discuss the further offenses. During the meeting, the alleged violations and the AUP policy will be reviewed and the details of the second incident will be forwarded to Human Resources. Alleged violations by employees of a more serious nature will be referred to Human Resources for resolution.

Reporting, Questions, and Assistance

Address any questions, exception requests, or report any suspected violations of the Acceptable Use Policy to the Office of Information Security, at itsecurity@wpi.edu.

Revision History

August 19, 2008 - IT approved the revised AUP for students. Until the updated version is approved by the Policy Committee, the prior version still applies to employees.

October 20th, 2008 - Minor style and format changes.

August 18th, 2008 - Added Proxy Usage Standard

October 2, 2015 - Updated and approved by IT and the Committee on IT Policy