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.

I. Policy Statement

Worcester Polytechnic Institute (WPI) establishes and maintains Computing and Networking Resources for shared use by authorized members of the WPI community. These resources are essential in providing academic, research and university business for exclusive use by the WPI community.

This Acceptable Use Policy (AUP) outlines responsibilities and obligations by Users of these resources. The intent of this policy is to promote the efficient, ethical, and lawful use of such resources.

II. Scope

This policy applies to all Users, including all students, faculty, staff and guests who access WPI's Computing and Network Resources.

III. Definitions

"Users" refers to those members of the WPI community (including students, faculty, staff, emeritus employees, and contractors) who are authorized to access WPI Computing and Networking Resources.

"WPI Computing and Networking Resources" refers to systems, networks, applications, information, lab computers, research computers, and similar equipment owned by WPI that support academic, research and business purposes. For purposes of this policy, this definition includes WPI Computing and Networking Resources that are accessed by personally-owned devices (such as a personal mobile device).

IV. Policy

A. Key Elements of the Policy

Comply with the intended use of WPI Computing and Networking Resources.

All WPI Computing and Networking Resources 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 WPI's Employee Benefits and Policies.

Ensure the ethical and legal use of WPI Computing and Networking Resources.

Users must not use WPI Computing and Networking Resources for unethical or illegal activities, and must comply with federal, state and local laws. Users shall respect the privacy of others, use data only as authorized by the data owner, and not use these resources to harass or attack others.

Respect the personal property and privacy of other users.

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 Computing and Networking Resources to anyone outside the WPI community without express permission. WPI retains the right to review and audit any WPI-owned electronic communication devices, connections, and services to ensure the security and integrity of WPI Computing and Networking Resources and prevent unauthorized access, malicious software or other potential security / operational issues and maintain compliance with WPI policies. WPI retains the right to deny network access to any non-WPI owned electronic communication devices.

Use the WPI Computing and Networking Resources for non-commercial purposes only.

WPI Computing and Network Resources may not be used for commercial use, to host advertising, or to create or mine digital currencies. Users may not resell WPI Computing and Network Resources. Such usage is inconsistent with WPI's academic and research missions and WPI's non-profit status.

B. Response to AUP Offenses

First and/or Minor Offense:

Student- and employee-Users will have a meeting with a member of Information Security to discuss how the User's activities may have deviated from the AUP provisions. During the meeting, the AUP will be reviewed with the User 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. WPI Computing and Networking Resources that are registered to the User may be disabled until the User has had a discussion about the incident.

Repeat Offenses:

Students: In the event of suspected repeat offenses, the User will have a meeting with a member of Information Security. During the meeting, the alleged deviations from the AUP will be reviewed. Depending on the nature of the further offense(s), the incident may be: (1) handled in the same manner as a first and/or minor offense; or (2) referred to the Dean of Students Office for resolution. As part of the resolution, WPI Computing and Networking Resources registered to the User may be disabled.

Staff: In the event of suspected repeat offenses, the User will have a meeting with a member of Information Security. During the meeting, the alleged offense(s) and the AUP will be reviewed and the details of the offense(s) will be referred to WPI's Division of Talent and Inclusion for resolution. In addition, Information Security may disable the User's access to WPI Computing and Networking Resources.

Faculty: In the event of suspected repeat offenses of a Faculty member, the following WPI departments will collaborate to understand the extent of the offense(s): Information Security, WPI's Division of Talent & Inclusion, the Office of the Provost, and the User's Dean and/or Department Head. Information Security may disable the User's access to WPI Computing and Networking Resources. Disciplinary action, if any, will be addressed through applicable policies and procedures contained in the Faculty Handbook.

Serious Offenses:

Students: Alleged offenses of a more serious nature (e.g., activities which exhibit malicious intent to compromise, disrupt, or circumvent security of the WPI Computing and Networking Resources) may be referred to the Dean of Students Office for resolution. Please refer to theWPI Student Code of Conduct for a full description of resolution methods and processes. WPI Computing and Network Resources registered to the User may be suspended pending the resolution of the case.

Staff: Alleged offenses of a more serious nature will be referred to WPI's Division of Talent and Inclusion for resolution.

Faculty: In the event of serious offenses of a Faculty member, the following WPI departments will collaborate to understand the extent of the offense(s): Information Security, WPI's Division of Talent & Inclusion, the Office of the Provost, and the User's Dean and/or Department Head. Information Security may disable the User's access to WPI Computing and Networking Resources. Disciplinary action, if any, will be addressed through applicable policies and procedures contained in the Faculty Handbook.

V. Exceptions

Exceptions to the AUP and 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. Exceptions for academic purposes can be requested by a Faculty member.

VI. Questions

If you have any questions regarding this policy, please contact the WPI Service Desk at its@wpi.edu.

* * *

Policy Sponsor: Chief Information Officer

Responsible Department: Information Technology

Effective Date (i.e., date of Presidential Approval): May 12, 2022

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
- May 4, 2022 – updated policy statement; added definitions; revised offenses section; approved by Administrative Policy Group and the Committee on IT Policy