Email Systems and Usage Policy

1.0 Purpose

The purpose of this policy is to provide guidance on how and when University partner email systems are approved and verified and who has access and authority to use these systems to communicate with student, staff, faculty and other University constituents while upholding information security standards and conforming to the relevant state and federal laws.

At WPI, electronic mail (email) is recognized as official University correspondence. As such, WPI provides this guidance and standards to assure that all communications originating from the institution are professional, appropriate, and for the agreed upon purposes of the system. This guidance will also enable WPI community members to distinguish legitimate University email from unauthorized messages.

2.0 Definitions

- University Application Vendors- On premise or hosted third-party vendors that have a contractual relationship with WPI. WPI employees leverage software from these vendors to send email to students, employees or other university constituents.
- University Third Party Vendors- Third-party vendors with a contractual relationship with WPI that communicate directly with WPI students, employees or other university constituents.
- Email and Standing Lists – WPI maintains a variety of standing lists with membership and acceptable use policies.
- Group and Distributions Lists are defined in the WPI Mailing List Policy.

3.0 Systems and Distribution

Enterprise email systems of record and other third-party systems that have been assessed and approved by Administrative Systems Working Group (ASWG) are used by individuals in various divisions to conduct business communications as varied as emergency alerts and daily news and events updates to employees.

WPI contracts with University Third Party Vendors, such as those who administer benefits, retirement, and job search for students and alumni, which send email to the email address that is provided by the University. Because WPI has less control over University Third Party Vendors, they do not fall under this policy. However, the University will maintain a list of these vendors so that all employees are aware of who may be sending emails to them.

Any University Application Vendors that will send mail to WPI community members must be approved through WPI's ASWG committee and adhere to the standards in this policy. Third-party vendors, that are not vetted or fail to uphold WPI policy, may have their messages filtered prior to delivery.

4.0 Applicability

This policy applies to all members of the WPI community, including students, faculty, staff, trusted partners, contractors, and users of the university network and messaging systems.

5.0 Policy

All University requirements and relevant laws must be followed when sending messages to WPI community members.

Messages sent out via University Application Vendors must:

- Follow relevant federal, state, and local laws, including the CAN-SPAM Act of 2003
- Use templates that adhere to University marketing standards
- Have a clear, accurate "from" field indicating the name of the person or University unit sending the message. The "from" address and "reply-to" addresses should be **wpi.edu** email addresses. The ASWG may authorize exceptions only when the use of wpi.edu addresses is technically infeasible.
- Accurate and descriptive subject line.
- Text identifying the WPI community, including "WPI", "Worcester Polytechnic Institute" or "on behalf of WPI 'department' " that is clearly identified in plain text messages and in the text-only portion that accompanies an HTML message.*
- The message footer must contain the audience the message was sent to and the name and physical mailing address of the sending unit (e.g., "This message was sent to weekly newsletter subscribers by the Office of the President at WPI, Worcester Polytechnic Institute, 100 Institute Road, Worcester, MA 01609-2280").
- For optional communications, the message must contain straightforward instructions to allow recipients to opt-out of the communication and any opt-out requests must be handled in a timely manner.
- Links contained in the message should be to web addresses hosted in the wpi.edu domain. For websites hosted at the third-party vendor's website, IT Services will maintain a list of vendors along with their URLs for people to check if they have concerns and leverage Microsoft's Advanced Threat Protection to check URLs for threats.

- The message should minimize the use of email attachments and avoid file types that could contain a malicious payload.

6.0 Policy Enforcement

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in WPI's Confidentiality Agreement for employees or Code of Conduct for students.

7.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on January 10, 2019.

Policy Reviewed Annually By: Chief Information Security Officer

Related University Policies:

- WPI Acceptable Use Policy (AUP)

Last Modified: 1/10/19