



Email Use Policy

1.0 Purpose

This addendum to the Acceptable Use of Computer Resources Policy serves to provide a guiding reference to members of the Plymouth State University community on issues of appropriate use, privacy, and access of electronic mail. This policy will apply to all University electronic communication services, including stored files, herein referred to as "e-mail". Such services include but are not limited to e-mail, voice-mail, bulletin boards, group documents and chat rooms operated by the University.

2.0 Scope

This policy covers appropriate use of any e-mail sent from a PSU e-mail address and applies to all employees, vendors, and agents operating on behalf of PSU.

3.0 Policy

3.1.0 General Statements

1. E-mail is subject to the University System of New Hampshire Property Policy on Use of Technological Resources, USY-VI-F4. (link) This policy establishes the University System and its component institutions for retaining ownership over the records resident on the technological resources covered by this policy. Therefore, the University retains these rights, in accordance with USNH policy, to maintain ultimate control and authority over its technology resources, including E-mail, and to take appropriate actions to further legitimate institutional interests.
2. E-Mail communications may be subject to public access under the New Hampshire Public Records Law RSA 91-A and, when relevant, to discovery in civil litigation. Any such disclosure of E-mail under these conditions will be approved by the President of the University or his/her designee.
3. The University has a responsibility to protect students' and staff rights as well as ensure the accuracy of its business processes based on e-mail correspondence. Therefore, e-mail containing official business of the University shall be addressed to the person's official University e-mail address and should not be addressed to alternative addresses.

3.1.1 Individual Expectations

1. E-Mail messages are expected to be in compliance with university policies. University officials follow policy in regard to privacy and access to electronic records.
2. Individually addressed e-mail communications may not be intercepted (read) by any third party except as noted below. Any access of individual e-mail communications other than that noted below is in violation of University policy and appropriate action will be taken as defined in section 4 of this policy.

3.1.2 University Requirements

1. University officials and supervisors shall have the right to read any e-mail when written permission for such access has been given by the individual.
2. University officials shall have the right to access any E-mail to preserve life and ensure the safety of the University community. The President and/or appropriate vice president shall be notified of the access when conditions have warranted such action.
3. Under certain circumstances the system administrator may, in the course of their duties, access an individual's e-mail for legitimate management or maintenance purposes (e.g. virus removal, backup, restoration, delivery resolution, etc.). The University reserves the right to inspect and remove e-mail that might contain viruses or other harmful content or otherwise interfere with the delivery of e-mail or normal operation of computer systems. It also reserves the right to filter

- known or suspected virus attachments in mass prior to delivery. In such cases, ITS will notify the University as to the specific filtering being applied.
4. If an occasion arises when a University officer or supervisor believes that access to an individual's e-mail account is required for the conduct of urgent University business or if there is reasonable cause that the email account is being used in violation of PSU, USNH or other policies or laws, a request may be made to have the email account in question be accessed by an ITS professional under the supervision of the CIO. The individual may or may not be informed in advance, depending on the nature of the circumstances under which the investigation is being pursued. the University individual is not available, and a system administrator is required to access the individual's e-mail account, the following procedure shall be followed:
 - a. The University official or supervisor shall secure permission to access the e-mail account from the supervising Principal Administrator, the Director of Human Resources or President of the University.
 - b. An appropriate written order of the principal administrator or President shall be presented to the system administrator allowing the system administrator to proceed to access the e-mail account.
 5. All e-mail communications and files on campus computers, accounts, and databases are university property (see II.A.1). Upon employee termination, resignation, or withdrawal, these materials remain the property of the University.
 6. On termination, resignation or withdrawal, an individual's e-mail account will be terminated, and all information not retained by the university will be deleted. Exceptions to this practice are granted for individuals with 20 years or more of service and leave the University in good standing.

3.2 Business Use

As with other University resources, e-mail is primarily used for purposes that further the goals of the University. While personal use isn't excluded, it should be limited. Furthermore, with ubiquitous options available for free email accounts through Google, Yahoo and Hotmail, employees are encouraged to use personal email accounts for their private and personal business. PSU employees should NOT use personal email systems for their official PSU work.

Some activities are explicitly inappropriate on PSU systems:

1. Any use of PSU resources for personal commercial gain or solicitation except in cases of officially sanctioned University activities,
2. for self- or other promotion in political campaigns,
3. participation in chain-letters.

3.3 Unlawful Use

Persons may not use e-mail in violation of USNH or campus policies and local, state or federal laws. Such policies or laws may include but are not limited to:

1. stalking, harassment, hate speech or other unlawful activity.
2. fraudulent acts, including the use of a deceptive alias to disguise one's true identity.
3. intentional distribution of viruses (real or simulated) or otherwise destructive software using e-mail.

3.4 Authentic Use

All materials sent by campus e-mail must be attributed to the individual, office, or organization sending the material.

3.5 Personal Use.

Using a reasonable amount of PSU resources for personal e-mail is acceptable, but non-work related e-mail should be saved in a separate folder from work related e-mail. It is also recommended that users subscribe to a readily-available and free email system to carry on their private email communications.

3.6 Bulk E-Mailing

Virus or other malware warnings and mass mailings from PSU shall be approved by the Public Relations Office or Information Technology Services before sending. These restrictions also apply to the forwarding of mail received by a PSU employee.

3.7 E-Mail forwarding

Employees must exercise utmost caution when forwarding any E-mail from inside PSU to an external e-mail address. Unless approved by an employee's manager, e-mail shall not be automatically forwarded to an external address.

3.8 Monitoring

PSU does not monitor individual e-mail activities.. Email traffic patterns are assessed to ensure optimal performance and to address specific problems. If a particular situation arises that negatively impacts performance, ITS will work with the specific user to address the problem.

3.9 Aliases

All aliases and distribution lists must use a dash or a period in the name to avoid conflicts with our existing username convention (first initial + middle initial + up to the first 16 characters in the last name). Such aliases are typically given to departments or employees with usernames similar to other users. Aliases are not available to students or Alumni.

3.10 Retention

It is PSU's policy to comply with all federal, state and local regulations and laws, and the terms of contracts and agreements with regard to retentions of business record. Originators and recipients of emails are responsible for identifying and saving documents. Any emails that fall within the scope of any business record retention regulations and contractual terms should be treated consistently with those requirements. PSU servers are configured with reasonable quotas for e mail storage, and no email will be systematically archived.

4.0 Enforcement

- Community members should report violations of this policy to the Director of Information Technology Services, Director of Human Resources, or the Dean of Students.
- Violation of this policy will be assessed by the appropriate Principal Administrator in accordance with established University procedures as defined in student and employee handbooks.

5.0 Definitions

Term	Definition
E-Mail:	The electronic transmission of information through a mail protocol such as SMTP or IMAP.
Chain E-Mail or letter:	E-mail sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information:	Information is considered sensitive if it can be damaging to PSU or its guests, students, staff or Alumni.
Forwarded E-Mail	Email resent, either manually or by use of a forward, from the original address to an external e-mail address.
Virus warning:	E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure:	The intentional or unintentional revealing of restricted information to people, both inside and outside PSU, who do not have a need to know that information.

Policy reviewed and endorsed by the Technology Advisory Group (TAG) in April 2008 and the Executive Steering Committee for Information Systems in May 2008.