

Seattle Pacific University

Computer and Information Systems

Policies, Procedures, Plans and Standards

Email Retention and Recovery Policy

Effective: September 1, 2005
Updated and Approved by CIS: February 3, 2009

Contents:

1.0 Purpose/Introduction

2.0 Scope

3.0 Email Classification and Retention

- A. Individual Responsibility
- B. Message Classification
- C. Institutional Data and Institutional Servers
- D. Confidential and Sensitive Personal Information

4.0 Email Deletion and Recovery

1.0 Purpose/Introduction

This policy is intended to help employees determine what information sent or received by email should be retained and for how long. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail, instant messaging, or other online technologies. All employees (and their supervisors and managers) should familiarize themselves with these email retention requirements to assure that important institutional data is being preserved and maintained. Additionally, this policy sets forth reasonable expectations for the recovery of material accidentally deleted or corrupted.

Ownership: Implied in this policy is the understanding that a substantial portion of university business is conducted via email. University provided email accounts are intended for institutional use and benefit. Seattle Pacific maintains the right of ownership of the data and information shared and communicated through these resources.

Audit/Inspect/Monitor: The University reserves the right to audit, inspect and monitor all information stores and network transmissions within the campus network regardless of their source or origin.

Privacy: While campus technology resources are owned by the University and are intended exclusively for institutional use, we also respect the personal privacy and confidentiality of sensitive information stored on campus resources and seek to ensure that it is protected and secure.

Questions about the proper classification of a specific piece of information should be addressed to your area manager.

2.0 Scope

This email retention policy is secondary to Seattle Pacific University's policies on freedom of information and specific business or departmental record keeping requirements (procedural or statutory). Any email that contains information within the scope of the business record keeping policy created or maintained at the departmental level, should be treated in the manner prescribed by those policies.

3.0 Email Classification and Retention

In accordance with SPU's Acceptable Use Policy, the primary intent of SPU email is for university business. SPU retains ownership of all correspondence that resides on the central email server, and may at any time, store, archive or otherwise access email messages in accordance with the provisions set forth by university policy.

- A. Individual employees are responsible for saving/retaining important university-related email messages, unless otherwise dictated and prescribed by statute or university policy. SPU currently maintains a backup/archive of email messages for no more than six months, primarily for disaster planning and hardware/software maintenance purposes. Consequently, important correspondence pertaining to university business should be saved, printed or otherwise preserved by the individual email user in accordance with other university policy regarding the preservation of the academic, business, financial or administrative record.
- B. Email messages should be handled according to the value of their content. For university purposes, email may be characterized in two categories: Limited/Transitory; or Archival/Lasting.
 - 1. **Limited/Transitory:** Email that pertains to common communications between individuals, and that has a limited time of relevancy, should be deleted as soon as their short term reference value expires. An example of limited/transitory email would be that used in coordinating a departmental meeting. Retaining this message would have no value beyond the date of the meeting. Such messages should be deleted freely and frequently.
 - 2. **Archival/Lasting:** Email messages that have long term relevance and that pertain to university business or academic operations, should be retained for longer periods of time. Such messages include information regarding university policies, financial records, academic records, operational procedures, administrative actions, or personnel (employment) matters. Currently, SPU employees are individually responsible for retaining correspondence of an archival/lasting nature. Methods of retention could include archival in specific categorized folders (email), and/or printing out hard copy for permanent records filing.

- C. All institutional data should be maintained on campus owned and provided equipment and servers. If you need additional storage resources to maintain critical data on campus-provided equipment, please contact CIS for assistance. Do not copy or store institutional data on personally owned equipment or systems.
- D. Do not store or transmit confidential or sensitive personal information through insecure channels such as email. These data categories should only be stored and maintained in centralized servers.

If you have questions concerning your department's specific retention requirements, please consult your department head or supervisor.

4.0 Email Deletion and Recovery

There are several safeguards built into the campus email resources to protect data. You should be familiar with each of these resources.

- A. Deleted Items Folder – when you delete a message it is stored within your personal email box in the deleted items folder. This directory is automatically emptied once a week, but can be used to retrieve messages before that.
- B. Recover Deleted Items - messages that were deleted from your personal email account persist for roughly sixty days in a server based deleted items folder. These messages can be retrieved from the Tools, Recover Deleted Items menu. CIS makes no guarantee, however, that messages errantly deleted will be recoverable from the desktop. In the event that a message is errantly deleted, the first method of delivery is to check on the local machine from which the email was initially discarded.
- C. In the event that an email is non-recoverable from the local cache, but the error in deletion is detected within two weeks, the email may be retrievable from CIS central data recovery site. Contact CIS for assistance with this option. Requests for email recovery from the central data recovery site must be made in writing (email acceptable) and approved by the CIS assistant vice president or designate. CIS makes no guarantee that such information is recoverable from storage even within the two week window.
- D. As a final recourse in the recovery effort, critical university email may be obtained from off-site back up from the university archive. By policy, email messages are retained for a period of no more than 6 months, after which time no record of said email shall exist in local or remote archive. Requests for email recovery from the central data recovery site must be made in writing (email acceptable) by the requesting departmental area vice president to the CIS assistant vice president or designate. The requesting department shall be responsible for any fees associated with the non-routine retrieval of off-site archive data. CIS makes no guarantee that such information is recoverable from archive even within the six month retrieval window.

End of Document