POLICY

Effective Date: June 1, 2012
Approved By: President Bruce Shepard

Authority: RCW 42.17.130 42.52; 42.56; 40.14
WAC 292-110-010

See Also: 
POL-U1500.08 Using University Resources
POL-U1600.02 Ensuring Equal Opportunity and Prohibiting Discrimination
POL-U1600.04 Preventing and Responding to Sex Discrimination
POL-U4910.01 Managing University Archival Records
POL-U5615.01 Responding to Campus Violence or Threats of Violence
POL-U7100.02 Using Email Accounts for Official Correspondence with Students
Code of Responsibility for Security and Confidentiality of Records and Files

POL-U3000.02 USING ELECTRONIC METHODS FOR UNIVERSITY COMMUNICATION

This policy applies to all employees including permanent and, temporary employees and student employees assigned a First.Last@wwu.edu account or who have been granted permission to access group a mailbox(es) or resource account(s).

Definitions:

Account Owner: The individual assigned as the primary user of an electronic communication account or communication device for the purpose of conducting university business.

Electronic Communications: Any electronic means of communication, including but not limited to, cell phones, pagers, and electronic mail regardless of device ownership.

1. First.Last@wwu.edu Account is Official University Mode of Electronic Communication

All employees will be assigned a First.Last@wwu.edu email account. This account is the official account where important university notifications will be sent. Employees are to use this account to perform university official duties. All employees are expected to regularly monitor mail received through their assigned First.Last@wwu.edu email account.

2. University Access Permitted to Comply with Public Records Requests, Subpoenas or Legal Processes

The state’s Public Records Act (RCW 42.56) requires that electronic mail or files containing information relating to the conduct of university business is made available for
public inspection and copying. Employees should endeavor to retain email in compliance with the University Retention Schedule, prudent management of it to avoid retaining materials that ought to be deleted, in order to minimize storage costs and ensuring that retrieval can be timely and efficiently completed as required under the Public Records Act. The University's Public Records Officer determines which electronic mail and/or files are public records. University business conducted on private email or other private electronic communication accounts is subject to public records requests and legal discovery.

3. **Use of Electronic Mail Limited to University Business**

Electronic mail is to be used only to support teaching, research, service, and administrative functions consistent with the employee’s official duties, promotion of organizational effectiveness, or enhancement of job-related skills.

As defined by POL U5400.13, Using University Property for Political Activity, electronic mail may not be used for political activity.

Activities that are considered university service rather than outside work are not subject to the prohibition on the use of university resources.

*Exception:* Personal use of email is permitted. Personal use must be *de minimis* and is defined by WAC 292–110–010: Personal use is *de minimis* only if all five of the following conditions are met:

- There is little or no cost to the state;
- Any use is brief;
- Any use occurs infrequently;
- The use does not interfere with the performance of any state employees' official duties; and
- The use does not compromise the security or integrity of state property, information, or software.

4. **Mass Email Distribution Requires Approval**

Distribution of mass email to all employees or large groups of employees (i.e. more than one division/college or employee classification) must be approved by the Office of Communications.

*Exceptions:*

- Essential or emergency messages may be sent by Public Safety or Information Technology.
• The President, Vice Presidents, and Chief Information Officer (CIO) may approve mass email distribution and may establish division policies/procedures for division-wide distribution.

• Official union, Faculty Senate, Professional Staff Organization, and Departmental communication to their respective constituents does not require approval.

5. **Account Owners Responsible for Maintaining Privacy, Security and Confidentiality**

Account owners of electronic mail/files are responsible for maintaining appropriate access restrictions, as well as protecting their passwords. Allowing another person to use his or her username or password is strictly prohibited. However, electronically assigning “delegates” to email and calendar accounts is permitted.

Security and confidentiality are of concern to all university employees and to all other persons who have access to electronic records. Each individual who is given access to electronic information must adhere to the *Code of Responsibility for Security and Confidentiality of Records and Files*.

6. **Security and Privacy Not Guaranteed**

The University respects the privacy of employees and does not routinely inspect or monitor electronic mail communication. However, all email communication is considered University property and, therefore, the security and privacy of any employee’s electronic mail and/or electronic files is not guaranteed.

Responsible system maintenance requires that files are backed up, data cached, activity logs kept, and overall system activity monitored. In the process of these activities, The University’s informational technology staff may see an employee’s electronic mail and files.

7. **University Access Permitted to Comply with Records Retention Requirements See POL-U4910.01**

Department heads are responsible, in consultation with the University’s Records Manager, for training and implementing appropriate measures and requirements of their employees that ensure retention of electronic communications in accordance with record retention requirements of state law (RCW 40.14) and University policy. Additionally, users are advised that electronic messages and other files stored on local or personal hard drives must be managed in accordance with records retention requirements.

When acquiring new computers, departments must ensure all electronic communication files needed for retention purposes are transferred to the new computer before being
deleted from the discarded computer. Material that continues to exist on a hard drive, or forwarded to another computer, may be subject to disclosure.

8. **Access to Another Employee’s University Electronic Communication Requires Chief Information Officer (CIO) Approval**

Supervisors may access an employee’s university computer account and university assigned computer equipment when that employee is unavailable and access is for a legitimate business purpose. This access may only be granted by the Chief Information Officer (CIO) or designee. Incidental viewing during maintenance activities described in Section 6 do not need CIO approval.

Employees who receive access must do so in a manner that is consistent with any research and/or confidentiality agreements which may apply to those files.

9. **CIO Acts to Comply with Legal and Ethical Requirements**

The CIO may have or grant access to electronic mail/files when necessary to:

- Comply with legally issued subpoenas,
- Enact for litigation discovery holds,
- Comply with legal discovery, and
- Court orders.

10. **University Access Permitted for Investigation of Misconduct**

The University may also access electronic files to investigate an employee’s misconduct related to suspected illegal activity or policy violations and the access is consistent with legal requirements. Such access may only be done with the approval of the CIO or designee.

11. **Unethical and Illegal Use of Electronic Email Prohibited**

Unethical or illegal activity is prohibited via university electronic communications. Prohibited activities include, but are not limited to, the following:

- Sending harassing and/or derogatory messages based on legally protected groups,
- Sending sexually explicit messages including pornography,
- Sending harassing and/or threatening messages,
- Forgery (or attempted forgery) of messages,
- Unauthorized reading, deleting, copying or modifying the electronic messages of other users,
- Sending unsolicited junk mail, "for-profit" messages or chain letters,
- Hiding the actual user’s id by "spoofing" or any other means,
• Conducting an outside business or private employment or other activities conducted for private financial gain,
• Supporting, promoting, or soliciting for an outside organization or group unless otherwise provided by law and University policy,
• Assisting an election campaign, promoting or opposing a ballot proposition or initiative, or lobbying the state legislature, or a state agency head,
• Advertising and selling for commercial purposes, or
• Any use related to conduct that is prohibited by a federal or state law or rule, or a state agency policy.