

1.8 - Electronic Mail Policy

The following represent WVUP's electronic mail policy:

- West Virginia University at Parkersburg reserves the right, consistent with policy and applicable law, to access, review, and release all relevant electronic information that is transmitted over or stored on the college computer and network systems, whether or not the information is private in nature, and therefore cannot complete confidentiality or privacy of electronic mail is not guaranteed. Confidentiality cannot be guaranteed due to the nature of the medium, the need for authorized staff to maintain electronic mail systems, and the college's accountability as a public institution, as well as instances involving the health or safety of people or property; violations of college codes of conduct, regulations, policies, or law; other legal responsibilities or obligations to the college, or the locating of information required for college business.
- Terminating employees' accounts will be closed on the last day of employment. Terminating employees shall be advised that their email accounts may be accessed by departmental directors in order to continue to conduct college business after their departure. Departmental directors and deans must send a written request to the Office of Information Technology requesting this access. The Office of Information Technology will reset the password and restore access. By default, accounts re-activated for this purpose will stay active for thirty days, which gives the user with acquired access enough time to transfer relevant emails and to inform correspondents of an address change.
- Users should exercise extreme caution in using email to communicate confidential or sensitive matters, and should not assume that their electronic mail is private or confidential.
- Users may not access, use or disclose personal or confidential information without appropriate authorization, and must take necessary precautions to protect confidentiality of personal or confidential information in compliance with college policy and applicable law, regardless of whether the information is maintained on paper or whether it is found in electronic mail or other electronic records.
- Electronic mail users and operators must follow sound professional practices in providing for the security of electronic mail records, data, applications programs, and systems programs under their jurisdiction.
- Users are responsible for safeguarding their login credentials (username and password) for using them only as authorized. Each user is responsible for all electronic mail transactions made under the authorization of his or her user ID.

Misuse

- Using the West Virginia University at Parkersburg email system for illegal activities is strictly prohibited. Illegal use may include, but is not limited to:
 - obscenity
 - child pornography
 - threats
 - harassments
 - theft
 - attempting unauthorized access to data or attempting to breach any security measures of a communications system
 - attempting to intercept any electronic communication transmissions without proper authority
 - violation of copyright, trademark or defamation law
- The following electronic mail practices are prohibited:
 - entry, examination, use, transfer and/or tampering with the accounts and files of others, unless authorized pursuant to policy
 - altering electronic mail system software or hardware configurations
 - interfering with the work of others or with college or other computer facilities
- College-provided email services shall not be used for commercial activities, personal financial gain or advancement of a political agenda.
- Email users shall not give the impression that they are representing, giving opinions, or otherwise make statements on behalf of West Virginia University at Parkersburg or any unit of the college unless expressly authorized to do so.
- Email services shall not be used for purposes that could reasonably be expected to cause strain on any computer system, or interference with others' use of the email systems.

Such uses include, but are not limited to, the use of email services to:

- send or forward chain letters
- send SPAM (unsolicited email)
- send letter bombs
- knowingly send or transmit computer viruses

Violations

Suspected or known violations of policy or law should be reported to the appropriate supervisory level for the operational unit in which the violation occurs. Violations will be processed by the appropriate college authorities and/or law enforcement agencies. Violations may result in various actions, including but not limited to revocation of electronic mail privileges; academic dishonesty or Code of Conduct proceedings; faculty, staff, or student disciplinary action up to and including dismissal; referral to law enforcement agencies, or other legal action.