Title: #VII-1. Guidelines for Appropriate Use of Computer Resources

Date: September 16, 2025 (replaces version dated May 15, 2017)

Introduction

These guidelines are provided in accordance with Board of Governors Policy E-57, Appropriate Use of Computer Resources, and apply to all WVU Parkersburg staff, faculty, administrators, officers and students (collectively, “users”), including those at the Jackson County Center, ITC, and other off-campus instructional sites. All faculty, staff and students of WVU Parkersburg are expected to acquaint themselves with Board of Governors Policy E-57 and these procedures, copies of which are available in student, faculty, and staff handbooks and online at: www.wvup.edu/about/policies-and-procedures/campus-procedures-guidelines/. New employees, including adjunct faculty, will be provided a copy of Policy E-57 and these campus procedures, and asked to verify that they have read and understand them.

WVU Parkersburg’s computer and information network is a continually growing and changing resource that supports thousands of users and systems. These resources are vital for the fulfillment of the academic, research and business needs of the WVU Parkersburg community. In order to ensure a reasonable and dependable level of service, it is essential that each individual faculty member, staff member, and student exercise responsible, ethical behavior when using these resources. Misuse by even a few individuals has the potential to disrupt college business, and, even worse, the legitimate academic and research work of faculty and students.

Appropriate Use of Resources

Conducting college business, instruction, study assignments, research, communications, and official work of campus organizations are appropriate uses of WVU Parkersburg’s computer resources. Access to computer resources is a privilege. It requires individual computer users to act responsibly, conserve computer resources, and consider the rights and privacy of others. The resources are the property of WVU Parkersburg. All users are expected to utilize college resources in a responsible manner consistent with Board of Governors Policy E-57 and operational guidelines that the Chief Information Officer may issue from time to time.

Prohibited Use of Resources

Users should be aware that they may be subject to the laws of other states and countries when they engage in electronic communications with persons in such other states or countries or on other systems or networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to their particular uses. Additionally, users of WVU Parkersburg computer resources must comply with all federal, West

Virginia, and other applicable law and other college policies. The following uses of college computer resources are prohibited:

1. Interference or impairment to the activities of others, including but not limited to the following:

   a. Creating, modifying, executing or retransmitting any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail; bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or examine or collect data from the network (e.g., a "network sniffer" program).

   b. Authorizing another person or organization to use college computer accounts or WVU Parkersburg network resources. Users are responsible for all of their accounts. Users must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their accounts by unauthorized persons. Users must not share their passwords with anyone else or provide access to the WVU Parkersburg network resources to unauthorized persons. Users must log out or lock devices that are not in use to prevent access to resources from unauthorized persons.

   c. Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

   d. Failing to keep media containing confidential or limited access data secure. Such media might include portable devices, USB thumb drives, CDs, DVDs, or paper.

   e. Failing to destroy media containing confidential or limited data once it is no longer needed. For example, printouts with this sort of data should be shredded. Data stored on removable media should be thoroughly erased. All storage mediums installed in a device must be thoroughly erased or destroyed prior to the device being re-provisioned or decommissioned.

2. Unauthorized access and use of the resources of others, including but not limited to the following:

   a. Use of college resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.

   b. Use of false or misleading information for the purpose of obtaining access to unauthorized resources.

   c. Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorization (e.g., use of a "network sniffer" program)

d. Making unauthorized copies of copyrighted materials. Users should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorization of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.

3. Damage or impairment of college resources, including but not limited to the following:

   a. Use of any resource irresponsibly or in a manner that adversely affects the work of

      - *Hacking* **-** attempting to obtain or use, passwords, IP addresses or other network codes that have not been assigned to you or authorized for use as college employees, attempting to obtain unauthorized access to computer accounts, software, files, or any other college computer resources.

      - *Malicious Activity* **-** intentionally, recklessly or negligently damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program); damaging or violating the privacy of information not belonging to the user; or misusing or allowing misuse of system resources.

   b. Use of college resources for non-college related activities that unduly increase network load (e.g., chain mail, network games and spamming).

   c. Altering software, system logs, configuration files, or other files needed for the proper operation of a computer system without prior authorization.

   d. Using or possessing unauthorized access devices (i.e. card skimmers). Unauthorized possession of these devices on campus may result in disciplinary action.

   e. Any other activity not specifically cited above that may be illegal, harmful, destructive, damaging, or inappropriate use of college computer resources.

4. Unauthorized commercial activities, including but not limited to the following:

   a. Using college resources for one's own commercial gain, or for other commercial purposes not officially approved by the college, including web ads.

   b. Using college resources to operate or support a non-college related business.

   c. Use of college resources in a manner inconsistent with the college's contractual obligations to suppliers of those resources or with any published college policy.

5. Violation of city, state or federal laws, including but not limited to the following:

a. Pirating software, music and images.

b. Effecting or receiving unauthorized electronic transfer of funds.

c. Disseminating child pornography or other illegal material.

d. Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

Security Obligation

Access to information stored on the college's computers and network equipment is controlled by assignment of accounts and passwords. These accounts and passwords are controlled by the Office of Information Technology Staff. This security information is the property of WVU Parkersburg.

All college employees have an obligation to report security breach information to the Office of the Chief Information Officer. Failure to do so may result in disciplinary action. Any attempt to access, copy or modify this security information or to obtain system privileges to which employees are not entitled or any action which interferes with the supervisory or accounting functions of the systems or that is likely to have such effects will result in appropriate disciplinary action.

De Minimis Usage

In the interest of making the use of computer resources a natural part of the day-to-day learning and work of all members of the WVU Parkersburg community, incidental personal use is tolerated. However, one should not use college sources of e-mail, Internet access, social media, and other computer services for activities of an extensive nature that are unrelated to college purposes. Additionally, there should be no expectation of privacy or confidentiality in connection with the personal use of these resources. Excessive use of systems for recreational Internet browsing, e-mail, social networking, or game playing is to be avoided and may subject employees to disciplinary action up to and including termination.

Electronic Mail Access, Confidentiality and Security

1. Access to email is provided to active students and employees. Students who have graduated or who have been inactive for two years will have their email accounts deleted.

2. Departing employees' accounts will be closed on the last day of employment. Email accounts of departing employees 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.

3. WVU Parkersburg does not routinely monitor or scan electronic mail. However, the college does reserve 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.

4. 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.

5. 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.

6. Records containing Personally Identifiable Information (PII) may not be sent use unencrypted email. Encrypted methods such as secure file transfers must be used instead.

7. 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.

8. 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. **Enforcement**

The college reserves the right to monitor computer and network use for operational needs and to ensure that operational needs and compliance with applicable laws and college policies are met. WVU Parkersburg considers any violation of this policy to be a serious offense and reserves the right to copy and examine any files or information contained on college systems or equipment that may be related to inappropriate use.

The Chief Information Officer is authorized to disconnect a user's access if the user appears to represent~~s~~ a serious threat to system or email integrity. Violators are subject to disciplinary action as dictated by college policy. Users should also be aware that offenders may be subject to prosecution under laws including, but not limited to, the Privacy Act of 1974, The Computer Fraud and Abuse Act of 1986, National Stolen Property Act, The West Virginia Computer Crime and Abuse Act, and the Electronic Communications Privacy Act. The President as well as the Chief

Information Officer, Director of Human Resources, and/or the Executive Vice President for Academic Affairs will be notified of infractions.

Suspected violations of policy or related statute should be reported to the Chief Information Officer by e-mail or by calling 424-8280. In reporting a violation, complainants should cite the specific violation of Policy E-57 or these guidelines.

Responsibility

The Chief Information Officer is the policy administrator for computer resources at WVU Parkersburg and will ensure compliance with these guidelines. Additionally, deans, directors and department heads are responsible for compliance with college policy within their respective administrative areas.

Responsible Administrator: Chief Information Officer, 304-424-8280