

WVU Parkersburg Answer Book #VII-1, Appropriate Use of Computer Resources, June 24, 2003

Purpose

West Virginia University at 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 WVUP 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.

In accordance with WVU policy **OIT-8**, this campus policy outlines the application of the principles that govern our academic community in the appropriate use of college computer and information network resources. This policy was designed to ensure the proper use of computing resources consistent with the general principles that govern WVUP. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, individuals' rights to privacy, and freedom from harassment. Computing and networking resources include: computers, computer networks, connections to external computer networks, and subscriptions to external computer services. Open access to these resources is a privilege. It requires individual computer users to act responsibly, conserve computer resources, and consider the rights and privacy of others. Use of any college computing resource constitutes acceptance of this policy.

Scope

This policy applies to all WVU at Parkersburg staff, faculty, administrators, officers and students (collectively, "users"), including those at the Jackson County Center and other off-campus instructional sites.

Policy

West Virginia University at Parkersburg computer resources are provided primarily for the use of students, faculty and staff. They are intended to be used for administrative and educational purposes and to carry out legitimate college business. In addition, access to the network may be provided to alumni and members of the local community for the purpose of communicating with students and employees and for accessing WVUP information resources and the internet. Appropriate use of these resources includes conducting college business, instruction, study assignments, research, communications, and official work of campus organizations. 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 have always been, and will remain, the property of West Virginia University at Parkersburg. Use of any college computing resource constitutes acceptance of this policy. All users are expected to utilize college resources in a responsible manner consistent with University policies and the guidelines and operating policies that the WVU Associate Provost of Information Technology (CIO) or WVUP Director of Computer Services 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 WVUP computer resources must comply with all federal, West Virginia, and other applicable law and other university and campus 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:
 - 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 email; 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).
 - Authorizing another person or organization to use college computer accounts or WVUP 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 WVUP network resources to unauthorized persons.

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

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

- Use of college resources to gain unauthorized access to resources of this or other institutions, organizations, or individuals.
- Use of false or misleading information for the purpose of obtaining access to unauthorized resources.
- 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)
- 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 (see also

WVU Copyright Policy and Guidelines).

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

- Use of any resource irresponsibly or in a manner that adversely affects the work of others, such as:
- *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.
- Use of college resources for non-college related activities that unduly increase network load (e.g., chain mail, network games and spamming).
- 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:

- Using college resources for one’s own commercial gain, or for other commercial purposes not officially approved by the college, including web ads.
- Using college resources to operate or support a non-college related business.
- Use of college resources in a manner inconsistent with the college’s contractual obligations to suppliers of those resources or with any published campus or University policy.

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

- Pirating software, music and images.
- Effecting or receiving unauthorized electronic transfer of funds.
- Disseminating child pornography or other illegal material.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

Security Obligation

- **System Security:** 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 Director of Computer Services and/or the Network Administrator. This security information is the property of WVU at Parkersburg.
- All college employees have an obligation to report security breach information to the Director of Computer Services and/or the Network Administrator. 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 WVUP community, incidental personal use is tolerated. However, one should not use college sources of e-mail, Internet access, and other computer services for activities of an extensive nature that are unrelated to college purposes. Excessive use of systems for recreational Internet browsing, e-mail, or game playing is to be avoided and may subject employees to disciplinary action up to and including termination.

Enforcement

Although the college does not routinely monitor computer and network use, the college does reserve the right to monitor computer and network use for operational needs and to ensure compliance with applicable laws and University policies. WVU at 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 Director of Computer Services is authorized to disconnect a user's account if the user represents a serious threat to system or email integrity. Violators are subject to disciplinary action as dictated by University 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 Campus President as well as the Director of Computer Services, Director of Human Resources, and/or the Dean of Students will be notified of infractions. Director of Computer Services by e-mail or by calling 424-8296. In reporting a violation, complainants should cite the specific section of this policy that has been violated. If any provision of this policy is ruled invalid under law, it shall be deemed modified or omitted solely to the extent necessary to come into compliance with said law, and the remainder of the policy shall continue in full force and effect.

Questions or Problems

Questions, concerns or additional information about this policy should be directed to the Director of Computer Services.

Responsibility

The Director of Computer Services is the policy administrator for computer resources at WVUP and will ensure this process is followed. Additionally, deans, directors and department heads are responsible for compliance with campus policy within their respective administrative areas.