

Information Services | West Chester University | 023 Anderson Hall West Chester, Pennsylvania 19383 | 610-436-2828 | fax: 610-436-3240 www.wcupa.edu/ infoservices/

- b. Never be wasteful of computing or information network resources or unfairly monopolize these resources. Waste in the form of examples such as unauthorized mass mailings, chain mail, unnecessary printing output, or creating unnecessary network traffic are expressly prohibited.
- c. Never attempt to modify a program or diskette which the University supplies for use.
- d. Never engage in behavior which could impair or impact the operation of computers, terminals, peripherals or networks. Acts such as tampering with the LAN, the high-speed backbone network, or otherwise blocking communication lines or interfering with the operational readiness of a computer is expressly prohibited.
- e.

financial gain or other personal benefit, or for other reasons which result in a direct cost to the University.

f. Never abuse work time by spending large amounts of time at work in pursuit of social or other non-related personal interests which engage the use of the and resources.

(Examples of this form of inappropriate use include chat rooms, sexually explicit sites, sports fantasy and betting sites, etc.)

- g. Never store or attempt to download or otherwise transmit data which would constitute a violation of state or federal law or the policies of the University, the State System of Higher Education or the Commonwealth of PA.
- h. Installation of any software package by clients on University computers requires an original license agreement to be housed at the location of the Computer or handheld device on which the software will be installed. University employees cannot install any software on University computers and handheld devices without proper software licenses. Always abide by the terms of all software license agreements. Unauthorized copying of software is illegal and expressly prohibited.
- 4. Privately owned computers: Faculty, staff, students, and guests of West Chester University who provide their own computer and equipment but connect to the University's network must still abide by all aspects of the Acceptable Use Policy. In addition, there are several special areas for these users to keep in mind:
  - a. The content of any files or services made available to others over the network is the sole responsibility of the person with ownership of and/ or administrative authority over the computer providing the service. It is this person's responsibility to be aware of all applicable federal and state laws, as well as university policies. This person will be liable for any violations of these laws and policies.
  - b. Any person operating a network-intensive application or a defective computer, which causes network overload, will be notified and steps will be taken to protect other users and the university network overall. This may include disconnecting the offending computer system from the network until the problem is resolved. If the condition is an imminent hazard to the university network or disrupts the activities of others, then the offending computer system or the subnet to which it is attached may be disabled w

5. Suspension of User Privileges: There may be circumstances where the nature of an allegation is so serious as to require a suspension of privileges while an investigation is being conducted. Under these circumstances, the student will be notified at the time of the suspension. Suspension of user privileges pending the outcome of an investigation is not a disciplinary action.

Occasionally requests from local, state or federal agencies will be made to investigate or provide information about technology related resources. These could include but not limited to server logs, email transactions, or user information. These requests will be routed through either the Department of Public Safety or the Office of Information Security. Once a request is made to either department, the other respective department will be notified as well, unless it would compromise the integrity of the investigation.

Verified, serious misuse or repeated, minor infractions of this policy will result in disciplinary action. The typical form of disciplinary action for non-criminal offenses is loss or restriction of privileges, although other forms of discipline which would be more appropriate under the circumstances are possible. Under normal circumstances, disciplinary actions will be issued by the department director or by the University official charged with that responsibility as part of the collective bargaining relationship.