

# Computer Usage Policy

## For Students

The following policy contains the governing philosophy for regulating the use of Delaware Valley College's computing network facilities and resources. Access to the computing network facilities and resources is a privilege granted to Delaware Valley College faculty, staff, and registered students by the College. All users of the computing network facilities must act responsibly and maintain the integrity of these resources. The College reserves the right to limit, restrict, remove or extend computing network privileges and access to its resources.

Those who do not abide by the policies listed below are subject to suspension of computer privileges and possible disciplinary action.

Information Services should be notified about violations of laws and policies governing information use, intellectual property rights, or copyrights, as well as about potential loopholes in the security of its computer systems and networks. The user community is expected to cooperate with Information Services in its operation of computer systems and information networks as well as in the investigation of misuse or abuse. Should the security of a computer system or information network be threatened, suspected user files may be examined under the direction of the College President. In addition, the College will comply with all governmental and law enforcement subpoenas, warrants, or orders requiring the examination of user files.

The primary use of computing network facilities is for academic activities. Other non-restricted use such as entertainment is secondary and must yield to academic and administrative use. Entertainment and other secondary uses may be restricted when they are interfering with academic use.

## Policies

The College's computing policies include, but are not limited to, the list below.

- Computer facilities are to be used by registered Delaware Valley College students, faculty, and staff only.
- Physical abuse and willful damage of the computer equipment is prohibited and will result in loss of computer lab privileges, disciplinary action, and criminal prosecution.
- Restrict recreational use on lab computers to low traffic times. Students needing the computers for academic purposes have priority. Recreational users may be asked to discontinue their use to provide access for academic applications.
- Use of the College's network resources to gain or attempt to gain unauthorized access to remote computers is prohibited.
- Any deliberate act which may seriously impact the operation of computers, peripherals, or networks is prohibited. Such acts include, but are not limited to, the following: tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.
- Attempting to modify in any way a program or diskette which the College supplies for any type of use is prohibited.
- No person shall knowingly run or install on any of the College's computer systems, or give to another, a program which could result in the eventual damage to a file, computer system, or information network, and/or the reproduction of itself. This is directed towards, but not limited to, the classes of programs known as computer viruses, Trojan horses, and worms.
- No person shall attempt to circumvent data protection schemes or uncover security loopholes.
- All persons shall abide by the terms of all licensing agreements and copyright laws. In particular, unauthorized copying or downloading of copyrighted software is prohibited.
- Deliberate acts which are wasteful of computing resources or which unfairly monopolize resources to the exclusion of others are prohibited. These acts include, but are not limited to, sending mass mailings or

chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary output, or printing or creating unnecessary network traffic.

- The following type of information or software cannot be placed on any College-owned computer system:
  - that which infringes upon the rights of another person
  - that which is abusive, profane, or sexually offensive to the average person
  - that which may injure someone else and/or lead to a lawsuit or criminal charges; examples of these are: pirated material, destructive software, pornographic materials, or libelous statements
  - that which consists of any advertisements for commercial enterprises
- No person shall harass others by sending annoying, threatening, libelous, sexually, racially, or religiously offensive messages through electronic means..
- Use of the College's computer resources to monitor another user's data communications, or to read, copy, change, or delete another user's files or software, without permission of the owner, is prohibited.
- Use of the College's computers, workstations, or information networks must be related to a Delaware Valley College course, research project, work-related activity, departmental activity, or for inter-personal communications. Use of these resources for personal or financial gain is prohibited.
- Any network traffic exiting the College is subject to the acceptable use policies of the network through which it flows, as well as to the policies listed here.

### **E-mail**

- Maintenance of a user's electronic mailbox is the user's responsibility.
- Check e-mail daily and remain within your limited disk quota.
- Delete unwanted messages immediately since they take up disk storage.
- Keep messages remaining in your electronic mailbox to a minimum.
- Never assume that your e-mail can be read by no one except yourself; others may be able to read or access your mail. Never send or keep anything that you do not want seen.
- Be professional and careful about what you say regarding other persons. E-mail is easily forwarded.
- Use discretion when forwarding mail to group addresses or distribution lists.
- Avoid forwarding personal e-mail to mailing lists without the original author's permission.
- Chain letters are strictly prohibited and should be reported to Computer Services.
- All mail may be purged at the end of each semester without notice.
- Misuse of an e-mail account may result in the revocation of that account and possible disciplinary action.

### **Consequences**

Violation of one or more of these published policies will result in a loss of access to the College computing systems with possible referral to the appropriate judicial process.

Offenders may also be subject to criminal prosecution under federal or state law, and should expect the College to pursue such action. As an example, under Pennsylvania law, it is a felony punishable by a fine of up to \$15,000 and imprisonment up to seven years for any person to access, alter or damage any computer system, network, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization [18 Pa.C.S.3933(a)(1)]. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to \$10,000 and imprisonment of up to five years, as is intentional and unauthorized access to a computer, interference with the operation of a computer or network, or alteration of a computer software [18 Pa.C.S.3933(a)(2) and (3)].

### **Reference**

State System of Higher Education, "Model Policies Concerning Computer Use"

"Policies Concerning Computer Use", West Chester University

"Computer Lab and Network Use Policy", East Stroudsburg University, October 1995

"Policies on the Use of Computer Systems and Facilities", Lehigh University, August 1999