Computer Use Guidelines

State Law (Article 7.1 of Title 18.2 of the Code of Virginia) classifies damage to computer hardware or software (18.2- 152.4), invasion of privacy (18.2-152.5), or theft of computer services (18.2-152.6) of computer systems as (misdemeanor) crimes. Computer fraud (18.2-152.3) and use of a computer as an instrument of forgery (18.2-152.14) can be felonies. The PHCC's internal procedures for enforcement of its policy are independent of possible prosecution under the law.

DEFINITION
PHCC information technology resources include mainframe computers, servers, desktop computers, notebook computers, handheld devices, networks, software, data files, facilities, and the related supplies.

The following guidelines shall govern the use of all PHCC Information Technology resources:

1. You must use only those computer resources that you have the authority to use. You must not provide false or misleading information to gain access to computing resources. The PHCC may regard these actions as criminal acts and may treat them accordingly. You must not use PHCC IT resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc.
2. You must not authorize anyone to use your computer accounts for any reason. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorized persons. You must not, for example, share your password with anyone.
3. You must use your computer resources only for authorized purposes. Students or staff, for example, may not use their accounts for private consulting or to support a personal business venture. You must not use your computer resources for unlawful purposes, such as the installation of fraudulently or illegally obtained software. Use of external networks connected to any PHCC facility must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.
4. Other than material known to be in the public domain, you must not access, alter, copy, move or remove information, proprietary software or other files (including programs, members of subroutine libraries, data and electronic mail) without prior authorization.
5. The data owner, data custodian, security officer, appropriate college official or other responsible party may grant authorization to use electronically stored materials in accordance with policies, copyright laws and procedures.
6. You must not distribute or disclose third party proprietary software without prior authorization from the licenser. You must not install proprietary software on systems not properly licensed for its use.
7. You must not use any computing facility irresponsibly or needlessly affect the work of others. This includes transmitting or making accessible offensive, annoying or harassing material. This includes intentionally, recklessly, or

negligently damaging systems, intentionally damaging or violating the privacy of information not belonging to you. This includes the intentional misuse of resources or allowing misuse of resources by others. This includes loading software or data from untrustworthy sources, such as free-ware, onto official systems without prior approval.

8. You must not use the Commonwealth's Internet access or electronic communication in cases where it:
   - interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
   - adversely affects the efficient operation of the computer system;
   - results in any personal gain or profit to the user
   - violates any provision of this policy, any supplemental policy adopted by the agency supplying the Internet or electronic communication systems, or any other policy, regulation, law or guideline as set forth by local, State or Federal law. (See Code of Virginia §2.1-804-805; §2.2-2827 as of October 1, 2001.)
9. Peer-to-Peer file sharing (P2P) is prohibited on the campus network. P2P applications are considered a big security risk because they use direct communications between computers (or "peers") to share or transfer data. They require client software to be installed and, by so doing, expose the network to a number of risks. Security flaws in P2P applications may provide attackers with ways to crash computers, access confidential information, or infect the entire network. In addition, P2P applications can consume large amounts of bandwidth that are reserved for academic and administrative purposes and are, therefore, considered network abuse. Users of the Patrick Henry Community College network may not use peer-to-peer file sharing programs, including, but not limited to, Limewire, eDonkey, KaZaA, Gnutella, Morpheus, Audiogalaxy, WinMX and BitTorrent. For the purposes of this policy, a Peer-to-peer file sharing application is any application that transforms a personal computer into a server that distributes data simultaneously to other computers. Please note that copyrighted materials cannot be shared by any means without proper permission. This includes sharing via network file shares, the web, or any other means and is not limited to peer-to-peer programs. Peer-to-Peer files sharing programs run on any Patrick Henry Community College computer can be traced back to the source by external Agencies. By using a PHCC computer for this purpose, the user is therefore making the College liable.

You should report any violation of these regulations by another individual and any information relating to a flaw or bypass of computing facility security to the Information Security Office.

ENFORCEMENT PROCEDURE

a. Faculty, staff, students, and patrons at the college or System Office should immediately report violations of information security policies to the local Chief Information Officer (CIO).

b. If the accused is an employee, the CIO will collect the facts of the case and identify the offender. If, in the opinion of the CIO, the alleged violation is of a serious nature, the CIO will notify the offender's supervisor. The supervisor, in conjunction with the College or System Human Resources Office and the CIO, will determine the appropriate disciplinary action. Disciplinary actions may include but are not limited to:

1. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.
2. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.
3. Disciplinary action for faculty and classified staff in accordance with the guidelines established in the State Standards of Conduct Policy.

c. In the event that a student is the offender, the accuser should notify the Vice President of Instruction. The VP, in cooperation with the CIO, will determine the appropriate disciplinary actions which may include but are not limited to:

1. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months.
2. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the cost associated with determining the case facts.
3. Disciplinary action for student offenders shall be in accordance with the college student standards of conduct.

d. The College President or designee will report any violations of state and federal law to the appropriate authorities.

All formal disciplinary actions taken under this policy are subject to the Commonwealth’s personnel guidelines and the accused may pursue findings through the appropriate grievance procedure.