

PVCC Computing Handbook

A Guide for Students, Faculty, and Staff

I. You, the College, and the Electronic Community

As a student, faculty, or staff member at PVCC, you will have many opportunities to improve your proficiency in the use of information technologies. As a leader in the 21st century, you will want to know how these technologies are used in your major field and in society at large. Information technologies can help you be more productive as a student -- to produce papers and submit assignments on-line, to use the library services, to send messages to your professors and friends, to access class notes, and to participate in many other aspects of student life. The College makes information technologies available to you in many ways:

- Everyone at the college has access to information servers for electronic mail (e-mail) and other Internet services.
- The college's World Wide Web site contains information to help you register for classes, apply for financial aid, keep up with college events, and much more.
- Microcomputers are available for general use at several locations on campus. These microcomputer sites provide access to the Internet and essential software for coursework. Some locations have student consultants on duty to help you with your computing questions. Many at the college have access to a voice mail system, which makes it easy and convenient to keep in touch with colleagues and professors.

II. Who "Owns" What?

We will use the possessive word "your" frequently in this booklet, but the term does not always mean ownership. In some cases, it means "exclusive use." You may own a personal computer or workstation. You will make the decisions about how that equipment will be used. You may own a software license -- word processing or spreadsheet software, perhaps -- that you purchased from a software vendor. Your license usually allows you to possess ONE copy of this software for your own use.

The college owns the departmental computer labs, the microcomputing sites, the computers it places on its employees' desks and all the software it has installed on them. The college determines who may use these resources and how they may use them. The college owns the college network -- all the wires, cables, and routers that connect the central computers, computer labs, microcomputer sites to each other and to the Internet. The college determines who is authorized to use its network, and can limit the nature of the use.

III. E-mail: Rules, Responsibilities, and Privacy

You can expect that, except in specific circumstances, the content of the e-mail files associated with your account will be treated as confidential by the college because it does not routinely examine or monitor such content. You should be aware, however, that e-mail messages can sometimes be records that are subject to review with sufficient justification. They may be subject to Virginia Freedom of Information Act if they were produced, collected, received or retained in pursuance of law or in connection with the transaction of public business (rarely the case with student e-mail). They may lose whatever confidentiality they have if their release is compelled by orders issued through courts of law. Also, officials overseeing the college's disciplinary processes may rule that e-mail or other files are evidence that may be reviewed as part of investigations. Under these circumstances, the privacy of your e-mail is not guaranteed.

Although you may have downloaded and/or deleted your e-mail messages, many email delivery systems work in such a way that messages may be preserved for a time as computer files on centrally-administered disks and at system back-up locations, so your capacity to control if and where copies exist is not absolute. The array of storage locations is another factor making the confidentiality of your e-mail conditional. And most produce messages in plain text; they are like postcards in that others might view the messages in transit or those left in plain view.

Sometimes messages are so badly misaddressed that they cannot be delivered and will end up in the hands of computing staff for redirection. People often make mistakes in addressing their mail that puts private messages in the mailbox of someone other than the intended recipient. If you are the recipient of such a message, common courtesy dictates that you either return the message to the sender with a brief note explaining its misdirection or that you delete the message.

College procedures allow Computing Services' system administrators to view and modify any files, including e-mail messages, in the course of diagnosing or resolving system problems and maintaining information integrity. Computing Services' system administrators, as part of their jobs, are expected to treat any such information on the systems as confidential. However, if an administrator comes across information that indicates illegal activity, he or she is required to report the discovery to appropriate authorities. For example, electronic mail messages that carry threats to persons or their immediate families may be prosecuted and punished as felonies under Virginia law. If a Computing Services' system administrator inadvertently encounters an e-mail message containing a threat, it will be turned over to law enforcement officials.

College policies prohibit certain other kinds of e-mail messages. For example, e-mail, college computers, or the college network cannot be used by individuals for commercial purposes or for personal gain. Such policies pertain to e-mail just as they do to any other college resource and are enforced when brought to the attention of appropriate college officials. Large-scale mailings impose loads on the college's electronic mail services. They should be used judiciously and often require approval from Computing Services. You will be wise to coordinate any large-scale mailing with the college's e-mail postmaster (postmaster@pvcc.edu).

E-mail accounts are vulnerable to malicious use when others know the owner's computing ID and password; carefully protect your electronic identity from use by anyone other than you. Your e-mail account is also subject to misuse when you leave open a computing session that you have begun in a college computing lab or when you fail to logout from the college Web Mail service before you close your browser. It is prudent to reboot the computer you use in any lab setting when you finish your work there or even if you leave the workstation, planning to return to it soon.

Other important tips related to e-mail:

- Remember, the e-mail messages you send become the possession of the receiver. They can easily be redistributed by recipients, and rules of disclosure by their systems apply to mail they received from you. When in doubt, double-check the addresses of your intended recipients.
- Do think before you send e-mail -- once sent, it is almost impossible to keep e-mail messages from reaching their destinations.
- Realize that college policy and secure passwords provide good but not complete assurance of the privacy of your e-mail messages. When the confidentiality of a message is of the utmost importance, only a person-to-person conversation may be sufficiently secure.
- Delete messages that should not be preserved.
- Never send or forward chain mail, whether it promises fame and fortune, or even supposed donations for a sick child. In virtually every known case, the claims made by such messages are untrue. A message that has been forwarded ten or more times is by definition in our policy a chain letter. This policy violation is a waste of computing resources and a nuisance and often offends recipients.
- Don't pass on unconfirmed rumors -- especially about viruses -- because they often only cause needless panic. You can check at <http://www.helpvirus.com> for a list of well-known virus hoaxes, or check at <http://www.urbanlegends.com> for a list of other well-known hoaxes that may not involve computers but about which you may receive information via e-mail.
- Don't open or execute attachments about which you have any question, even if they appear to be coming from a friend. Attachments have become an increasingly popular way of automatically distributing viruses, and your friend may not even know that his or her e-mail account is being used for that purpose.
- College policy prohibits use of college resources, computing or otherwise, for commercial purposes.
- Realize that if you die while you are a member of the PVCC community, your stored e-mail is a part of your personal effects and records that will be given to your executor (the person -- usually a family member -- designated to deal with your property at your death) if he or she requests it.

IV. About Home Pages

The college's Web server and tools are in place to help you publish a personal home page. PVCC's Instructional Technologist provides courses designed to help faculty publish a home page. Remember that you are expected to act responsibly when publishing your home page, just as you are in all use of computing resources at the college. The college's computing resources are intended to enable the institution to carry out its responsibilities of education and public service. Therefore, these functions have priority in using computing resources; however, the college recognizes the value of the Internet as a resource for information and communication. When computing resources are available, students may use them for co-curricular or personal purposes provided they abide by the policies and procedures governing such use.

Responsibility

All users of college computing systems must comply with the requirements of responsible computing in the college environment, as outlined here. Individual users assume full legal responsibility for the content of their home pages, and they must abide by all applicable local, state, and federal laws, including laws of copyright. Copyright law pertains to many types of materials, including cartoons, pictures, graphics, text, song lyrics, and sounds (including most MP3 and other files shared via so-called peer-to-peer procedures). The college is not responsible for the content of Web pages other than those defined as its "official" Web pages (the official Web pages of college departments, divisions, and other units). As a neutral provider of computing services and access to the Internet, PVCC does not review in advance or monitor the content of any materials transmitted, received, published or stored on or otherwise available through its systems. If PVCC receives complaints regarding the content of such materials, it will refer the complaint to the appropriate disciplinary system within the college, and it will cooperate with any resulting investigation in accord with the policies, procedures, and principles described or cited in this handbook. Assumptions about audiences who will see information you publish.

You will be wise to remember the very public nature of information you disseminate on the Internet through the World Wide Web. Information in a home page is published and available to everyone who can get to the Web. You must not assume that your information is restricted to only a close circle of friends, or even the PVCC community.

You are not allowed to use your Web page to gather information on visitors.

Fundraising and Advertising

You may not use home pages for fundraising or advertising for commercial or non-commercial organizations, except for college-related organizations and college-related events and in accord with policies governing these activities. Use of the College Name, Logo, Seal, or Photographs You may not use the college name in your home pages in any way that implies college endorsement of other organizations, products, or services. You may not use college logos and trademarks, the college seal or photographs copyrighted by the college.

V. Copyrights: Ethical and Legal Use

Unauthorized use of copyright-protected or licensed materials (including, but not limited to, graphic images, music or audio files, and written word) is a serious matter and is a violation of federal law. Any individual who reproduces copyrighted material in excess of "fair use" in electronic mail messages or on the World Wide Web may be at risk for the penalties of copyright infringement. An introduction to copyright law and college copyright policy is at <http://www.loc.gov/copyright/>.

Most software available for use on computers at the college is protected by federal copyright laws. Educational institutions are not exempt from the laws covering copyrights. In addition, software is normally protected by a license agreement between the purchaser and the software seller. The software provided through the college for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses. Licenses sometimes specify that you may use the software only while you are a member of the PVCC community.

It is the policy of the college to respect the copyright protections given to software owners by federal law. It is against college policy for faculty, staff, or students to copy or reproduce any licensed software on college computing equipment, except as expressly permitted by the software license. Of course, faculty, staff, and students may not use unauthorized copies of software on college-owned computers.

At the college, unauthorized use of software is a serious matter. Any such use is without the consent of the college and is subject to disciplinary action.

VI. Good Citizenship in the Internet Community

As more than one writer has observed, the Internet isn't a thing; it is neither an entity nor an organization; it isn't owned or run by anyone. It is a world of a million publishers with some of the characteristics of a frontier. The only code of behavior on that frontier is one that demands individual responsibility and accountability and that rewards those attributes with rational self-government, albeit quite limited in scope. The college provides Internet access to its students and employees with the expectation that they be good, responsible, and accountable Internet citizens. But, what does that mean in practical terms? How can you be a good Internet citizen?

READ and understand applicable policies, notably VCCS Ethics Guidelines.

KNOW what it means to take responsibility for your safety and security in the Internet environment and for deciding what is right and wrong in circumstances where often rules have not yet been written. You must take responsibility for educating yourself about the medium that you're using and for helping shape its use by good personal behavior. **BE AWARE** of the hundreds of others who rely on the college's computers to do their work. Consider how your on-line behavior will affect them.

UNDERSTAND that college policies that address academic dishonesty, including theft, plagiarism, disruptive conduct and misuse of materials and property, must guide your computing activities, just as they guide your activities in the classroom, computing labs, library or elsewhere on campus.

DON'T let other students, relatives or any other person gain access to the college's computing resources through your account. Understand that you will be held accountable for any abuse of computing resources by persons you allow to use your PVCC computing ID and password.

DON'T use computer accounts, computing IDs, and passwords that belong to someone else. To do so violates policy.

BE ACCOUNTABLE for your actions. Hiding your identity to avoid responsibility for your behavior on the network or using someone else's network identity are -- at a minimum -- violations of policy, and they may be serious violations of law.

DON'T play games that waste shared computing resources and have no academic purpose. You are not authorized to use your computer account or access to play such games.

KNOW that local, state, and federal laws and regulations pertain to computing activities wherever appropriate -- laws dealing with fraud, forgery, harassment, extortion, gambling, threats, copyright, obscene content, among others. Violators may be prosecuted.

BE WARY of those who will (sometimes unknowingly) provide on-line information that is untrue or fraudulent. If you are not certain, ask.

KNOW that messages you post to newsgroups or Web pages that you create in an attempt to be humorous may not be received in that spirit. Remember that archives of newsgroups and Web pages remain accessible for years -- don't be surprised if an interviewer asks about something you posted to a newsgroup while a student when you're trying to get that job you really want in a few years.

UNDERSTAND what you are authorized to do. Know what the college's purpose is in making these computing resources available to you.

- Your computer account is provided so you can send and receive e-mail, read and post notices to newsgroups and access library and other information resources.
- In some cases, professors will authorize further account access so students can do class assignments.
- Microcomputer labs are available so you can do word processing, make spreadsheets, and access other PVCC computer resources and the Internet. The software in the labs is for use there; you cannot copy it and use it elsewhere.

DON'T MISUNDERSTAND. Your access to computing resources can be revoked. In extending these resources, the college trusts students to make responsible use of them. If you violate that trust, you may lose access through various processes described elsewhere in this booklet.

VII. Threats to Your On-Line Safety and Security

The Internet community is under regular attack -- at varying levels of seriousness -- from "outlaws." Such outlaws (both within our community and outside it):

- steal other people's computing IDs and passwords;
- disrupt computer systems and networks;
- flood electronic mail systems with unwanted messages (spam);

- send forged electronic messages from Santa Claus, God, the College president, or, maybe, YOU;
- post messages that vilify and threaten other people;
- post inappropriate messages to mailing lists;
- spread viruses;
- subscribe others to mailing lists, or unsubscribe them, without their permission;
- or invade the privacy of others.

Students who do these things at the college may lose computing privileges and be subject to suspension or expulsion from the college. They might even be subject to prosecution under state and federal laws.

Cracking Passwords

Your password may be guessed or "cracked" if you choose a common word, or a friend's or a pet's name, or your nickname, or the name of your favorite team or the name of a celebrity. Choose a password that combines letters, numbers, and special characters (for example, \$, *, !).

Whether you use your PVCC computing ID and password or not, it is your responsibility to keep them secure. Do not let anyone talk you into "sharing." Don't keep your password and computing ID together. If you can remember your password without writing it down, that is best. Don't tell your friends -- or anyone, even someone assisting you with problem solving - - what your password is. Change your password regularly. **Crashing and Disrupting the System**

Malicious computer users make the system stop working or perform poorly. It's like speeding, shop-lifting, spray-painting cars or slashing tires. These users find out, from a variety of sources -- sometimes each other -- about things they can do to disrupt the systems. In almost every instance, such behavior violates the law, and, in every instance, it violates college policy. Consequences are severe.

Forging E-mail

Forging electronic messages is usually against the law in its own right, and, in connection with the sending of unsolicited bulk e-mail, may violate other state or federal laws.

"Spamming"

Spam is essentially the same message e-mailed over and over and broadcast to recipients who did not request it. Just because a message is annoying, off-topic or stupid doesn't make it spam; the defining characteristic of spam is the volume with which it is sent. Most common forms of spam violate Virginia law. In many cases, simply deleting the unwanted message is the best action you can take.

Controlling Access to Your Computing Files

The college's computing environment is designed to be an open environment. Many faculty and students want, or need, others to view and use their computer information -- their files. An instructor may want students to find a class assignment on the network. A student may want to share some information with friends. Computer systems are designed to let this happen. But many students and faculty do not want others seeing their messages, course work or research. On computers, you can control who can see your files by protection settings. Use these settings as you would locks to keep your files private. However, malicious users realize that many people don't know how to use the settings. If you need help in using the settings, introductory computing documents are available from the PVCC Computing Help Desk. The Help Desk is located in room 832 and can be reached at **434.961.5261** or on UVa's ITCWeb (<http://www.itc.virginia.edu/security/vulnerabilities.html>).

Because some people don't know how to limit access to their files, sometimes information is left unintentionally unprotected. When people are good citizens of the Internet community, unprotected files are not a problem. Good Internet citizens respect one another's privacy. Students who gain access to resources either by directly breaking into them or because they are just poorly protected violate PVCC policy. If you have any doubt about whether any resources or materials were intended to be public, ask the owner before you look. If you happen across resources or materials that you suspect weren't intended to be public, let the owner know. That owner may have no idea that he or she has left something open to worldwide viewing.

VIII. What You Should Do If You Are a Victim of Computer Abuse or Irresponsible Behavior

Unfortunately computer abuse, malicious behavior, and unauthorized account access do happen. Should any of these things happen to you, report them to the Help Desk, your system administrator or other appropriate college authority. Computing resource abuse should be reported to the electronic mail address abuse@pvcc.edu . This step will alert a number of Computing Services to your situation. Abuse cases are handled individually and confidentially.

IX. Security and Connecting Your Equipment to the College Network

If you connect your personal computer equipment to the college's network, you are responsible for the security of your resources -- not only for risks to the resources themselves but also for the possibility that your unsecured resources can be used by anyone on the Internet as remote locations to mount attacks on other computing systems. Any misuse of your equipment through your neglect in providing safeguards may be reason to deny access for your equipment to our network. "Neglect" in this instance may take many forms -- here are a few:

Failure to:

- use a strong password
- limit access to your equipment
- keep files from unknown sources off your equipment
- back up your files
- use up-to-date antivirus software
- keep your operating system up-to-date
- keep application software updated
- turn off or delete unneeded software features

X. Disciplinary Action for Abuse of Computing Resources

Students at the college have both rights and responsibilities. The college is committed to supporting the exercise of any right guaranteed to individuals by the Constitution and the Code of Virginia and to educating students relative to their responsibilities. Students' rights are listed in The PVCC Student Handbook. Standards of Conduct

The college is a community of scholars in which the ideals of freedom of inquiry, freedom of thought, freedom of expression, and freedom of the individual are sustained. It is committed to preserving the exercise of any right guaranteed to individuals by the Constitution. However, the exercise and preservation of these freedoms and rights require a respect for the rights of all in the community to enjoy them to the same extent. It is clear that in a community of learning, willful disruption of the educational process, destruction of property, and interference with the orderly process of the college or with the rights of other members of the college cannot be tolerated. Students enrolling in the college assume an obligation to conduct themselves in a manner compatible with the college's function as an educational institution. To fulfill its functions of imparting and gaining knowledge, the college retains the power to maintain order within the college and to exclude those who are disruptive of the educational process.

Faculty and staff disciplinary actions are based on the handbooks for faculty, classified staff, and part-time faculty.

How Computing Services Handles Student Computer Policy Violations

Step 1:

When Computing Services is notified (usually through abuse@pvcc.vccs.edu) that a student appears to be abusing computing resources, all of his or her computing privileges may be suspended immediately when such an action is warranted to protect the computing resources and to assure reliable service to the rest of the community.

Step 2:

Often, Computing Services staff will notify the student through phone contact, electronic or U.S. mail of the apparent violation. Frequently, the matter is resolved at that step by explanation from the student and, in the case of minor issues, assurance from the student that the behavior will not continue. If computing access has been suspended, it is usually restored at successful conclusion of this step.

Step 3:

If the matter cannot be resolved at Step 2, Computing Services may refer the matter through the Division of Student Services for disciplinary processes or through law enforcement officials if the matter involves an apparent violation of law. Computing access may remain suspended during these processes. Sometimes, individuals in the college community who are complaining about the behavior take the matter directly to Student Services or law enforcement.