Update #:	23
Title:	**DHRM Policy 1.75 Use of Electronic Communications and Social Media**
Type:	The 2016-17 Catalog and Student Handbook has been updated to include a link to the DHRM website where this policy may be obtained.
Effective:	Immediately (10-28-16)

TECHNOLOGY USE POLICIES

VCCS Computer Acceptable Use Guidelines

Thousands of users share VCCS information technology resources. Everyone must use these resources responsibly since misuse by even a few individuals has the potential to disrupt VCCS business or the work of others. Therefore, you must exercise ethical behavior when using these resources.

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), unauthorized examination (18.2–152.5), or unauthorized use (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 VCCS's internal procedures for enforcement of its policy are independent of possible prosecution under the law.

Definition

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

Standard

The following standards shall govern the use of all VCCS information technology resources:

- All users of VCCS IT resources must read and adhere to Virginia Department of Human Resource Management Policy 1.75-Use of Electronic Communications and Social Media. A copy of this policy may be obtained from the Virginia DHRM website: http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol175useofinternet.pdf
- 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 VCCS may regard these actions as criminal acts and may treat them accordingly. You must not use VCCS IT resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc. Th
- The System Office and colleges reserve the right (with or without cause) to monitor, access and disclose all data created, sent, received, processed, or stored on VCCS systems to ensure compliance with VCCS policies and federal, state, or local regulations. College or System Office officials will have the right to review and/or confiscate (as needed) any equipment (COV owned or personal) connected to a COV owned device or network.

- The System Office and Colleges shall use an authorized COV warning banner to communicate that IT systems and their use may be monitored and/or confiscated by authorized personnel; and there is no expectation of privacy when using a Commonwealth IT system.
- Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the agency head); and user commands; email and Internet usage; and message and data content.
- Local Administrator rights, or the equivalent on non-Microsoft Windows-based IT systems shall be limited to only authorized staff as appropriate to prevent users from: a. Installing or using proprietary encryption hardware/software on VCCS systems; b. Tampering with security controls configured on their workstations; c. Installing personal software on a VCCS system; d. Adding hardware to, removing hardware from, or modifying hardware on a VCCS system and;
- You must not authorize 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.
- The transmission of unencrypted sensitive data over the internet shall be prohibited unless properly encrypted and approved by the agency head. When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.
- 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 VCCS facility must comply with the policies of acceptable use promulgated by the organizations responsible for those networks. The VCCS shall document the user’s acceptance of the System Office or college Acceptable Use Policy before or as soon as practicable after, gaining access to VCCS IT systems.
- 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.
- 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.
- 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.
- 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. 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 or the Internal Audit department.

- 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 profits 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, 2011.)

Any user of VCCS IT resources employing the Commonwealth's Internet or electronic communication systems for personal use must present their communications in such a way as to be clear that the communication is personal and is not a communication of the agency or the Commonwealth.

Enforcement Procedures

1) 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).
2) 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 Office Human Resources Office and the CIO, will determine the appropriate disciplinary action. Disciplinary actions may include but are not limited to: a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months. b. Restitution for damages, materials consumed, machine time, etc., on an actual cost basis. Such restitution may include the costs associated with determining the case facts. c. Disciplinary action for faculty and classified staff in accordance with the guidelines established in the State Standards of Conduct Policy.
3) In the event that a student is the offender, the accuser should notify the Vice President of Academic and Student Development. The Vice President, in cooperation with the CIO, will determine the appropriate disciplinary action(s) which may include but are not limited to: a. Temporary restriction of the violator's computing resource access for a fixed period of time, generally not more than six months. b. Restitution for damages, materials consumed, machine time, etc. on an actual cost basis. Such restitution may include the costs associated with determining the case facts. c. Disciplinary action for student offenders shall be in accordance with the College student standards of conduct.

4) The College President or designee will report any violations of state and federal law to the appropriate authorities.
5) All formal disciplinary action(s) taken under this policy are subject to the Commonwealth's personnel guidelines and the accused may pursue findings through the appropriate grievance procedure.

VCCS Information Technology Student/Patron Acceptable Use Agreement

As a user of the Virginia Community College System's local and shared computer systems, I understand and agree to abide by the following acceptable use agreement terms. These terms govern my access to and use of the information technology applications, services and resources of the VCCS and the information they generate.

The college has granted access to me as a necessary privilege in order to perform authorized functions at the college where I am currently enrolled. I will not knowingly permit use of my entrusted access control mechanism for any purposes other than those required to perform authorized functions related to my status as a student. These include logon identification, password, workstation identification, user identification, digital certificates or 2-factor authentication mechanisms.

I will not disclose information concerning any access control mechanism unless properly authorized to do so by my enrolling college. I will not use any access mechanism that the VCCS has not expressly assigned to me. I will treat all information maintained on the college computer systems as strictly confidential and will not release information to any unauthorized person.

Computer software, databases, and electronic documents are protected by copyright law. A copyright is a work of authorship in a tangible medium. Copyright owners have the sole right to reproduce their work, prepare derivatives or adaptations of it, distribute it by sale, rent, license lease, or lending and/or to perform or display it. A student must either have an express or implied license to use copyrighted material or data, or be able to prove fair use. Students and other users of college computers are responsible for understanding how copyright law applies to their electronic transactions. They may not violate the copyright protection of any information, software, or data with which they come into contact through the college computing resources. Downloading or distributing copyrighted materials such as documents, movies, music, etc. without the permission of the rightful owner may be considered copyright infringement, which is illegal under federal and state copyright law. Use of the college's network resources to commit acts of copyright infringement may be subject to prosecution and disciplinary action.

The penalties for infringing copyright law can be found under the U.S. Copyright Act, 17 U.S.C. §§ 501-518 (http://www.copyright.gov/title 17/92chap5.html) and in the U.S. Copyright Office's summary of the Digital Millennium Copyright Act (http://www.copyright.gov/legislation/dmca.pdf).

I agree to abide by all applicable state, federal, VCCS, and college policies, procedures and standards that relate to the Virginia Department of Human Resource Management Policy 1.76-Use of Internet and Electronic Communication Systems, the VCCS Information Security Standard and the VCCS Information Technology Acceptable Use Standard. These include, but are not limited to:

- Attempting to gain access to information owned by the college or by its authorized users without the permission of the owners of that information.
- Accessing, downloading, printing, or storing information with sexually explicit content as prohibited by law or policy;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
- Installing or downloading computer software, programs, or executable files contrary to policy;
- Uploading or downloading copyrighted materials or proprietary agency information contrary to policy;
- Sending e-mail using another's identity, an assumed name, or anonymously;
- Attempting to intercept or read messages not intended for them;
- Intentionally developing or experimenting with malicious programs (viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) on any college-owned computer;
- Knowingly propagating malicious programs;
- Changing administrator rights on any college-owned computer, or the equivalent on non-Microsoft Windows based systems;
- Using college computing resources to support any commercial venture or for personal financial gain.

Students must follow any special rules that are posted or communicated to them by responsible staff members, whenever they use college computing laboratories, classrooms, and computers in the Learning Resource Centers. They shall do nothing intentionally that degrades or disrupts the computer systems or interferes with systems and equipment that support the work of others. Problems with college computing resources should be reported to the staff in charge or to the Information Technology Help Desk.

If I observe any incidents of non-compliance with the terms of this agreement, I am responsible for reporting them to the Information Security Officer and/or management of my college.

I understand that I must use only those computer resources that I have the authority to use. I must not provide false or misleading information to gain access to computing resources. The VCCS may regard these actions as criminal acts and may treat them accordingly. I must not use VCCS IT resources to gain unauthorized access to computing resources of other institutions, organizations, individuals, etc.

The System Office and colleges reserve the right (with or without cause) to monitor, access and disclose all data created, sent, received, processed, or stored on VCCS systems to ensure compliance with VCCS policies and federal, state, or local regulations. College or System Office officials will have the right to review and/or confiscate (as needed) any equipment (COV owned or personal) connected to a COV owned device or network.

I understand that it is my responsibility to read and abide by this agreement, even if I do not agree with it. If I have any questions about the VCCS Information Technology Acceptable Use Agreement, I understand that I need to contact the college Information Security Officer or appropriate college official. By acknowledging this agreement, I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same. I further acknowledge that should I violate this agreement, I will be subject to disciplinary action.

Paul D. Camp Community College 2016-17 Catalog

and Student Handbook

May 23, 2016

Franklin Campus 100 North College Drive Franklin, Virginia 23851	Hobbs Suffolk Campus 271 Keynon Road Suffolk, Virginia 23434	PDCCC Smithfield 253 James Street Smithfield, Virginia 23430