

Computer Guidelines

Virginia Community College System

Information Technology Student/Patron Acceptable Use Agreement

As a user of the Virginia Community College System's information technology resources, I understand and agree to abide by the following ethics 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 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, file protection keys, or production read or write keys.

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 VCCS computer systems as strictly confidential and will not release information to any unauthorized person. I agree to abide by all applicable state, federal, VCCS, and college policies, procedures and standards that relate to the VCCS Information Security Standard and the VCCS Information Technology Acceptable Use Standard. I will follow all the security procedures of the VCCS computer systems and protect the data contained therein.

If I observe any incidents of noncompliance with the terms of this agreement, I am responsible for reporting them to the Information Security Officer and management of my college. I understand that the VCCS Information Security Office or appropriate designated college officials reserve the right without notice to limit or restrict any individual's access and to inspect, remove or otherwise alter any data, file, or

system resource that may undermine the authorized use of any VCCS or college IT resources. 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.

Official E-mail Communications with Students

VCCS has established email as a primary vehicle for official communication with students. An official VCCS Gmail email address has been established and assigned by the VCCS and the colleges for each registered student, and current faculty and staff member. All communications sent via email will be sent to this address. Faculty members will use the official VCCS Gmail email address to communicate with a student registered in their classes and administrative units will correspond with students via this address.

Information Technology Acceptable Use Standard

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 works 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) 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 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 standard shall govern the use of all VCCS 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 VCCS may regard these actions as criminal acts and may treat them accordingly. You must not use the VCCS IT resources to gain unauthorized access to computing resources of other institutions, organizations or individuals.
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 the VCCS 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 or subroutine libraries, data and electronic mail) without prior authorization. The college or data trustee, 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 copy, distribute, or disclose third party proprietary software without prior authorization from the licensor. You must not install proprietary software on systems not properly licensed for its use.
5. 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 freeware, onto official systems without prior approval.
6. 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.
7. You must not use the Commonwealth's Internet access or electronic communication systems for personal use. It is strictly prohibited if it:
 - a. interferes with the user's productivity or work performance, or with any other employee's productivity or work performance;
 - b. adversely affects the efficient operation of the computer system;
 - c. results in any personal gain or profit to the user;
 - d. 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.)

Note: 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 not a communication of the agency or the Commonwealth.

Enforcement Procedure

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) at (540) 857-6126.
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 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.
3. 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 that 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 cost 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 will report any violations of state and federal law to the appropriate authorities.
5. All formal disciplinary actions taken under the policy are grievable and the accused may pursue findings through the appropriate grievance procedure.