

COMPUTING AND TELECOMMUNICATION GUIDELINES

The College's computing and telecommunications facilities are provided for the use of students in fulfilling their needs which relate to the mission of the college. Computing resources are valuable, and their abuse affects everyone who uses computing facilities. The same morality and ethical behavior that applies in the non-computing environment applies in the computing environment.

Every student using the College's telecommunications and computing equipment and capabilities agrees to abide by the tenets set forth in the following computing policy:

"I hereby acknowledge that permission is granted to me for academic use of the computing and telecommunications facilities and services of the college, including its computer systems, associated peripherals and files, and telephone and network access, according to the terms described herein.

"In consideration of the permission granted to use the above mentioned systems, I hereby acknowledge that:

- A. The college licenses the use of such computer software from a variety of outside companies. The college does not own this software or related documentation and, unless authorized by the software developer, does not have the right to reproduce or modify it.
- B. I agree not to copy, disclose, transfer, or modify, without written permission, any computer software or documentation that the college permits me to use. I also agree not to install any software on College owned equipment without the express written permission of the college.
- C. Media containing licensed software and the accompanying documentation is to be used in the college's office areas, classrooms, and computing labs, and is not to be removed from such designated areas.
- D. All use of software provided by the college and all the college's computer and telecommunications equipment is governed by the college's license agreements, this policy statement, and applicable federal and state laws. I hereby agree to comply with all such restrictions.
- E. I also agree not to use the college's computer and telecommunications systems in any way that diminishes or interferes with the use of those systems by others. I acknowledge the College's right to remove immediately any file which appears to be intended for any such misuse. I further acknowledge the College's right to inspect when necessary, as a function of responsible system management, all electronic files and other recorded information on the college's computing and telecommunications facilities.
- F. According to United States Copyright law, illegal reproduction of software can be subject to civil damages of as much as \$100,000 and criminal penalties, including fines and imprisonment. Students who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may result in denial of computing and telecommunications privileges or other sanctions. The College does not condone the illegal duplication or modification of software.
- G. I agree not to encroach on other's use of the facilities or deprive others of resources. For example, users should not play computer games while other users are waiting for computer resources for legitimate academic activities.
- H. I agree to respect the privacy of others by not: attempting to access another user's computer files; supplying or attempting to

supply false or misleading information or identification in order to access another user's account.

- I. I agree that the following usages of computing resources are unethical and subject to disciplinary action:
 1. Solicitation for charity or other benefits
 2. Activities related to the promotion or running of a personal for-profit venture or other activities unrelated to the pursuit of an education.
 3. Using foul or abusive language on the network or any electronic communication medium.
 4. Promoting and sending chain letters.
 5. Harassing students or employees at the college or other institutions.
 6. Sexual harassment comments directed to another person.
 7. Racial comments directed to another person.
- J. By utilizing the systems outlined in this policy statement, I agree to the terms herein, and shall indemnify and hold harmless against all damages, losses, expenses, or costs resulting from the breach of obligations contained herein."

VCCS COMPUTER ETHICS GUIDELINES

Thousands of users share VCCNet computing resources. Everyone must use these resources responsibly since misuse by even a few individuals has the potential to disrupt Virginia Community College System business or the works of others. Therefore you must exercise ethical behavior when using VCCNet 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 or 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

VCCNet resources include mainframe computers, minicomputers, microcomputers, networks, software, data, facilities and related supplies.

Guidelines

The following guidelines shall govern the use of all VCCNet resources:

- A. 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 VCCNet resources to gain unauthorized access to computing resources of other institutions, organizations or individuals.
- B. 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.
- C. You must use your computer resources only for authorized purposes. Students or staff, for example, may not use their accounts for private consulting. 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 VCCNet must comply with the policies of acceptable use promulgated by the organizations responsible for those networks.
- D. 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 VCCNet 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 licenses for its use.

- E. 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.
- F. You should report any violation of these regulations by other individual and any information relating to a flaw or bypass of computing facility security to the Information Security Officer or the Internal Audit department.

Enforcement Procedure

- A. Faculty, staff and students at the college or VCCNet facility 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 Office 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 costs 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 Academic and Student Services. The Dean, 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 assess 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 costs 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 will report any violations of state and federal law to the appropriate authorities.
 - E. All formal disciplinary actions taken under this policy are grievable and the accused may pursue findings through the appropriate grievance procedure.

Approval

This guideline shall remain in effect from March 31, 1995, until superseded or suspended.

Arnold Oliver
Chancellor

Note: The following agreement is posted in MECC computer labs.

INFORMATION TECHNOLOGY STUDENT/PATRON ETHICS AGREEMENT

As a user of the Virginia Community College System's local and wide area computer systems, 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 Information Security Policy and the Computer Ethics Guideline. 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 VCCNet administration, 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 re-

source that may undermine the authorized use of any network computing facilities (see VCCS Information Security Policy for details.)

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.

INTERNET CODE OF ETHICS

In support of intellectual freedom, Mountain Empire Community College does not monitor and has no control over information accessed through the Internet. It is the users or their guardians responsibility to ensure that accessed material is appropriate for the intended audience.

All users of electronic information sources such as the Internet are expected to use these resources in a responsible manner, consistent with the educational and informational purposes for which they are provided and to follow the rules and regulations of the college providing these resources.

Responsible, ethical use of the Internet includes:

- A. Using the Internet for educational and informational purposes only; not for unauthorized, illegal or unethical purposes.
- B. Not attempting to modify or gain unauthorized access to files, passwords, or data belonging to others; not seeking unauthorized access to any computer system; and not damaging or altering software components of any network or database.
- C. Not sending, receiving or displaying text or graphics which may reasonably be construed as obscene.

Note: The following policy is posted in MECC computer labs.

INTERNET ACCESS POLICY

Class related use of the internet using MECC computers has priority.

ACCESSING AND DISPLAYING PORNOGRAPHIC MATERIAL ARE PROHIBITED.

No user may transmit or make accessible any offensive, annoying or harassing material.

Violation of this policy may result in referral to the Director of Student Services for possible disciplinary action.