VICTOR VALLEY COMMUNITY COLLEGE DISTRICT

ADMINISTRATIVE POLICY

ADMINISTRATIVE SERVICES Chapter 6

COMPUTER AND TELECOMMUNICATIONS TECHNOLOGY USE
AP___

Introduction

This policy refers to all responsible use of all district information resources whether individually controlled or shared, stand alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the district. This includes desktop computers, laptop computers, workstations, mainframes, minicomputers, telecommunications devices, associated peripherals, software, and data regardless of whether used for administration, research, teaching, or other purposes.

Individual units within the College may further define "conditions of use" for information resources under their control. However, these statements must be consistent with this overall policy but may provide additional detail, guidelines and/or restrictions. Where such "conditions of use" exist, enforcement mechanisms shall apply. These individual units are responsible for publicizing both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible. Where use of external networks is involved, policies governing such use also are applicable and must be adhered to.

Access to the information resource infrastructure both within and beyond the College campus, sharing of information, and security of the intellectual products of the community, all require that each and every user accept responsibility to protect the rights of the community. Access to the networks and to the information technology resources at Victor Valley College is a privilege and must be treated as such by all users of these systems. Anyone who accesses, uses, destroys, alters, or damages College information resources, properties or facilities without authorization, may be guilty of violating the privacy of others, of injuring or misappropriating the work produced and records maintained by others, and threatening the integrity of information kept within these systems. Purposely or recklessly doing so is unethical and unacceptable.

Audience and Agreement

All users of the district computing systems must read, understand, and comply with these procedures as well as any additional guidelines established by the administrators of each system. Such guidelines will be reviewed by the College Assembly. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE PROCEDURES.

The policies as stated in this document are intended to ensure that users of College information resources shall:

1. respect software copyrights and licenses
2. respect the integrity of computer-based information resources
3. refrain from seeking to gain unauthorized access
4. respect the privacy of other computer users

Examples of Unacceptable Use

If a user allegedly violates the acceptable user policy, due process shall be followed. The College characterizes as unethical and unacceptable, and just cause for taking disciplinary action up to and including discharge, dismissal, expulsion, and/or legal action, any activity through which an individual using College information resources purposely or recklessly:

1. Violates any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, reports or other copy write material without proper, recorded authorization.

   All software protected by copyright shall not be copied except as specifically stipulated by the owner of the copyright. Protected software is not to be copied into, from, or by any College facility or system, except by license. The number and distribution of copies must be handled in such a way that the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.

2. Interferes with the intended use of the information resources or without authorization, destroys, alters, dismantles, disfigures, prevents rightful access to or otherwise interferes with the integrity of computer-based information and/or information resources.

   Computer users shall not attempt to alter, modify or remove computer equipment, software, or peripherals without proper authorization. This includes moving equipment from one location to the other or trading resources with another department.

   It is a violation of policy for computer users to encroach on others use of the College's computers. This includes but is not limited to: the sending of chain-letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs; running grossly inefficient programs when efficient alternatives are known to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a College computer; damaging or vandalizing College computing facilities, equipment, software, or computer files. Computer users shall not intentionally

develop or use programs which harass other computer users or which access private or restricted portions of the system and/or damage the software or hardware components of the system.

Computer users shall use great care to ensure that they do not use programs or utilities that interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users shall not use network links for any use other than permitted. The use of any unauthorized or destructive program may result in legal civil action for damages or other punitive action by any injured party, including the college, as well as criminal action.

Access to the College's computing facilities is a privilege granted to College students, faculty, and staff. Access to College information resources may be granted by the owners of that information based on the owner's judgment of the following factors: relevant laws and contractual obligations, the requestor's need to know, the information's sensitivity, and the risk of damage to or loss by the College.

The College reserves the right to limit, restrict, or extend computing privileges and access to its information resources. Data owners-whether departments, units, faculty, students, or staff-may allow individuals other than College faculty, staff, and students access to information for which they are responsible, so long as such access does not violate any license or contractual agreement; College policy; or any federal, state, county, or local law or ordinance.

Use of College computers must comply with Federal and State law and College policies. College computing facilities and accounts are to be used for the College-related activities for which they are assigned. This policy applies equally to all College-owned or College-leased computers. The use of College Computing Facilities to generate or access obscene or pornographic material, as defined by California and federal law and acceptable community standards is expressly forbidden.

3. Seeks to gain or gains unauthorized access to information resources or enables unauthorized access.

   Users of College information resources shall not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally allow others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of Victor Valley College computing privileges.

The well being of all computer users depends on the availability and integrity of the system. Any defects discovered in system accounting or system security are to be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem. The cooperation of all users is needed to ensure prompt action. The integrity of most systems is maintained by password protection of accounts. A computer user who has been authorized to use such a protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.

4. Without authorization an individual invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources.

   Use of the electronic communication facilities to send fraudulent, harassing, obscene, threatening, or other unlawful messages is prohibited. Users shall respect the purpose and charters of computer mailing lists (including local or network newsgroups and bulletin-boards). It is the responsibility of any user of an electronic mailing list to determine the purpose of the list before sending messages to the list or receiving messages from the list. Persons subscribing to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the purpose of the list. Persons sending to a mailing list any materials that are not consistent with the purpose of the mailing list will be viewed as having sent unsolicited material to the mailing list.

   In general, the College's electronic communication facilities are not to be used for the transmission of commercial or personal advertisements, solicitations, promotions, or programs intended to harass other computer users or access private or restricted computer or network resources. Some public bulletin boards in addition to the present one may be designated for selling items, etc., and must be used appropriately, according to the stated purpose of the list(s).

   Users shall not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users without the permission of those other users.

   College systems provide mechanisms for the protection of private information from unauthorized examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to private information are unlawful and will be treated as a violation of College policy. Authorized system administrators may access computer users' files at any time for maintenance purposes. System administrators will report suspected unlawful or improper activities to the proper authorities. Computer users, when requested in writing, shall cooperate with system administrators in investigations of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files.

5. Unless specifically authorized by a class instructor, all of the following uses of a computer are violations of student policy:
    a. Copying a computer file that contains another student's assignment and submitting it for credit
    b. Copying a computer file that contains another student's assignment and using it as a model for one's own work
    c. Collaborating on an assignment, sharing the computer files and submitting that file, or a modification thereof, as one's individual work

Acceptable Use of Email

Email is provided to employees as a business tool. Personal use should be rare and incidental. Communication of personal advertisements, commercial ventures, solicitations, or political announcements is prohibited. The only exception to this policy is the group account titled VVC Personals that should be used in a limited manner only for its original intent.

Access to the email system to conduct Union business must be in accordance with the access rights and released time provisions accorded in the collective bargaining agreements regarding use of campus mail and campus mailboxes. Do not use the email for illegal, offensive, obscene, frivolous, discriminatory or harassing purposes. The following are specifically prohibited:

- Viewing or downloading and distributing pornographic or other inappropriate or non-business related material; and
- Sending sexually explicit, discriminatory, harassing, threatening or other messages that are harmful to college operations.
- If you are uncertain of what you can or cannot do contact your Manager or IT department.

Electronic communications systems are owned and maintained by the Board of Trustees of the college. Therefore, please be aware that all electronic messages, chat sessions, phone calls, websites accessed, information, electronic files, and equipment may be monitored, reviewed, and examined, as college needs require.

Also remember that your message could be forwarded to another individual without your knowledge and your communication could be mistakenly misdirected or disclosed to the wrong individual and your communication could be intercepted by unauthorized individuals. Never send anything you wouldn't mind seeing on the evening news. "Deleted" doesn't mean destroyed.

- Never give your password to anyone else (except the authorized I.T. Personnel) and change it as is appropriate.
- Never use another individuals' account. This constitutes identity theft.

- Exit password protected computer functions before leaving your work area.
- Be aware of viruses and related procedures to control them.
- Do not attempt to access areas or tamper with files or accounts for which you are not authorized.

Acceptable Use of the Wireless Network

All wireless Access Points / Base Stations connected to the district network must be registered and approved by VVC Technical Services (VVCTS). These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interfaces used in all district or user-owned devices must be registered with VVCTS.

All computers with wireless LAN devices must utilize the district-approved Network Access Control (NAC) system configured to pass all unregistered devices to a guest VLAN for internet access only. In order to comply with this policy, wireless devices wishing to gain access to the secure wireless network must install and maintain the current NAC agent. All implementations must comply with all software and hardware security policies managed by NAC. NAC requires all secure wireless network users to be pre-registered and tracked by Media Access Control (MAC) address and other methods.

System Administrator Responsibilities

While the Victor Valley College Board of Trustees are the legal "owners" of all computers and networks purchased with College funds, control of any particular system resides with the head of a specific subdivision of the College structure, such as a Department Head or Area Administrator. For College-owned equipment, that person is the "owner" in the sense of these policies.

The owner may designate another person(s) to manage the system. This person(s), or the owner in the absence of such a designation, is the "system administrator". The system administrator's use of the College's computing resources is governed by the same guidelines that apply to any other user. However, the system administrator has additional responsibilities and authorities with respect to the system under his/her control and its users.

The system administrator has certain responsibilities to the College as a whole for the system(s) under his/her control, regardless of the policies of his/her department or group, and the owner has the ultimate responsibility to see that the system administrator carries these out. These responsibilities are:

- To take reasonable precautions against theft of, or damage to, the system components.

- To faithfully execute all hardware and software licensing agreements applicable to the system.
- To treat information about, and information stored by, the system's users as confidential and to take reasonable precautions to ensure the security of a system or network and the information contained therein.
- To promulgate information about: specific policies and procedures that governs access to and use of the system; and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.
- To cooperate with the system administrators of other computer systems or networks, whether within or without the California Community College System, to find and correct problems caused on another system by the use of the system under his/her control.

In the case of an emergency, when system response, integrity, or security is threatened, as outlined above, a system administrator is authorized to access all files and information necessary to find and correct the problem or otherwise resolve the situation. Affected users will be properly notified.