POLICY: 6Hx28:7A-02

Responsible Official: Vice President, Business Operations and Finance

Specific Authority: 1001.64, F.S.
Law Implemented: 1001.64, F.S.

Effective Date: 03-12-2002

Acceptable Use of Information Technology Resources

Policy Statement:

I. Computers, networks and electronic information systems are essential resources for accomplishing Valencia College's mission of teaching and learning. Valencia grants members of the college community shared access to these resources in support of accomplishing Valencia's mission. Access to these resources imposes certain responsibilities and obligations and is granted subject to college policies and procedures, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

II. Valencia's information technology resources are a valuable community asset to be used and managed responsibly to ensure their integrity, security, and availability for appropriate educational and administrative activities. All users of these resources shall use them in an effective, efficient, and responsible manner.

III. Users of College information technology resources must be aware of and comply with Valencia's "User Authentication Requirements for Access to Valencia Computer Resources" and "Acceptable Use of Information Technology Resources" procedures, which shall address matters including personal communication, privacy and security issues, passwords and Ids, information and data use, consequences of violations, and hardware, software, and network use.

IV. Use of College information technology resources in some areas, for example LRC's and student labs, may be subject to more refined requirements and restrictions. In such instances, more refined usage requirements will be provided and documented in those areas.

Procedures:

I. User's Rights and Responsibilities

Members of the Valencia College community are granted access to information technology resources in order to facilitate their college-related academic, research, and job activities. By using these resources, users agree to abide by all relevant Valencia College policies and procedures, as well as all current federal, state, and local laws. These include but are not limited to college policies and procedures related to harassment, plagiarism, commercial use, security, and unethical conduct, and laws prohibiting theft, copyright and licensing infringement, unlawful intrusions, and data privacy laws.

A. The computing and network resources of the College may not be used to impersonate another person or misrepresent authorization to act on behalf of others or the College.

B. The computing and network resources of the College may not be used to harass another person. Users should not transmit to others or display images, sounds, or messages that might be perceived by a reasonable person as, or have been identified as, harassing (see policies on sexual harassment and student conduct).

C. Campus and network computing resources must be used in a manner consistent with Chapter 815, Florida Statutes Computer Crimes Act and Title 18, United States Code, Electronic Communications Privacy Act of 1985. Unauthorized or fraudulent use of the College's computing resources may result in felony prosecution and punishment as provided for in Florida Statutes, Chapter 775, Florida Criminal Code.

D. The computing and network resources of the College may not be used for personal financial gain or commercial purposes except as expressly allowed by college policy.

E. Owners of computer accounts are responsible for all use of the accounts. They should follow guidelines to prevent unauthorized use by others, and report intrusions to the system administrators.

F. Individuals must not attempt to undermine the security or the integrity of computing systems or networks and must not attempt to gain unauthorized access. Users may not use any computer program or device to intercept or decode passwords or similar access control information. If security gaps are observed, they should be reported to the appropriate system administrators.

G. Individuals must not intentionally damage or disable computer systems, networks, or software.

H. Copying or using software, except as explicitly permitted under licensing agreements, is a violation of law. Computer users must be able to document ownership, license rights or exceptions to license rights of software in their possession, with the assistance of the College in cases of college-installed software.

I. To help maintain the proper functioning of computer and networking hardware and software, the College will take reasonable steps to ensure its computing resources are free of deliberately destructive software, such as viruses. Individuals must share responsibility for protecting college computers, and must ensure the integrity of any electronic media they introduce.

J. Respect for intellectual labor, creativity, and the right to privacy is vital to academic discourse and enterprise. System integrity is also essential for individual function. Invasion of privacy, and unauthorized access to files can be justified only by real threats to the integrity of the network or node. Unauthorized access to files, either by direct examination or by automated searching, will not be permitted unless there is documented reasonable cause, and access is approved by the appropriate College official.

K. Users are responsible for:

1. reviewing, understanding, and complying with all policies, procedures and laws related to access, acceptable use, and security of college information technology resources;

2. asking systems administrators or data custodians for clarification on access and acceptable use issues not specifically addressed in college policies, rules, guidelines, and procedures; and

3. reporting possible policy violations to the system/network administrators.

L. Liability for Personal Communications

Users of college information technology resources are responsible for the content of their personal communications. Valencia College accepts no responsibility or liability for any personal or unauthorized use of its resources by users.

M. Privacy and Security Awareness

1. Users should be aware that although the College takes reasonable security measures to protect the security of its computing resources and accounts assigned to individuals, the College does not guarantee absolute security and privacy. Users must follow the appropriate security procedures listed in these procedures to assist in keeping systems and accounts secure.

2. The College assigns responsibility for protecting its resources and data to system administrators and data custodians, who treat the contents of individually assigned accounts and personal communications as private and does not examine or disclose the contents except:

    a. as required for system maintenance including security measures;

    b. when there exists reason to believe an individual is violating the

    c. law or college policy; and/or

    d. as permitted by applicable policy or law.

3. The College supports each individual's right to private communication, and will take reasonable steps to ensure security of the network. Although messages on College computing resources are potentially accessible to others through public records laws, Public Records Law requests for documents maintained on College computing resources must be dealt with by the user who controls the requested documents. The College cannot guarantee absolute privacy of electronic communication.

N. Consequences of Violations

The College considers any violation of acceptable use policies and procedures to be a serious offense and reserves the right to copy and examine any files or information resident on college systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Access privileges to the College's information technology resources will not be denied without cause. If in the course of an investigation, it appears necessary to protect the integrity, security, or continued operation of its computers and networks or to protect itself from liability, the College may temporarily deny access to those resources. Alleged policy violations will be referred to appropriate college investigative and disciplinary units. For example, alleged violations by students may be directed to the Campus President's Office. The College may also refer suspected violations of law to appropriate law enforcement agencies. Depending on the nature and severity of the offense, policy violations may result in loss of access privileges, college disciplinary action, and/or criminal prosecution under applicable state and federal laws.

II. Valencia College's Rights and Responsibilities

A. As owner of the computers and networks that comprise Valencia College's technical infrastructure, the College owns all official administrative data that resides on its systems and networks, and is responsible for taking necessary measures to ensure the security of its systems, data, and user's accounts. The

College does not seek out personal misuse. However, when it becomes aware of violations, either through routine system administration activities or from a complaint, it is the College's responsibility to investigate as needed or directed, and to take necessary actions to protect its resources and/or to provide information relevant to an investigation.

B. Individual units within the College may define additional conditions of use for resources or facilities under their control. Such additional conditions must be consistent with this overall policy but may provide additional detail, guidelines, and/or restrictions.

III. Use of IDs and Passwords

A. Users are responsible for their activities on their username/account ID, including appropriate protection of their username/account ID and password.

B. The account name or password assigned to users must not be shared with others.

C. Users should select an obscure password and change it frequently.

D. A system/network administrator must be contacted immediately if the user has reason to believe that his/her username/account ID or password has been compromised.

E. Specific College systems may have other, more defined password requirements, for example Oracle, Atlas, WebCT, and SCT Banner.

F. Guidelines for helping users select a secure password may be found in the _Guidelines for Selecting a Secure Password_ document.

IV. Use of Information/Data

A. Users may access only accounts, files, and data that are their own, that are publicly available, or to which they have been given authorized access. Information that is in the user's possession should be kept secure.

B. The confidentiality of information considered to be student educational records, employee evaluative records, or otherwise confidential shall be maintained and such information shall not be disclosed or distributed except in accordance with college policy and law.

C. College information and resources shall be used for tasks related to job responsibilities and not for personal purposes.

D. Information to which the user has access, but for which he/she does not have ownership, authority, or permission to disclose must not be disclosed.

E. Users should accurately update their own records through college self-service systems and other processes provided for them.

V. Use of Software and Hardware

A. College e-mail, computers, and networks must be used only for legal, authorized purposes. Unauthorized or illegal uses include but are not limited to the following:

1. Harassment;

2. Destruction of or damage to equipment, software, or data belonging to others;

3. Unauthorized copying of copyrighted materials; or

4. Conducting private business unrelated to college activities.

B. Users must not engage in any activity that might be harmful to systems or to an information/data stored thereon, such as:

1. Creating or propagating viruses;

2. Disrupting services or damaging files; or

3. Making unauthorized or non-approved changes.

C. When vacating computer workstations, users must sign-off or secure the system from unauthorized use.

D. Users must use only legal versions of copyrighted software on Valencia College owned computer or network resources, in compliance with vendor license requirements.

E. Users should be aware of any conditions attached to or affecting the provision of college technology services:

1. Consult with the system administrator for any questions about system workload or performance.

2. Refrain from monopolizing systems, overloading systems or networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

VI. For situations not covered here, users should contact their system/network administrator, departmental computer contact, the Office of Information Technology, or the Vice President for Policy and General Counsel.

Related Documents/Policies:

Guidelines for Selecting a Secure Password

Policy History:

Adopted 6-15-83; Amended 11-18-92; Amended 03-12-02; Formerly 6Hx28:04-38.02

Procedure History:

Adopted 6-15-83; Amended 11-18-92; Amended 03-12-02; Formerly 6Hx28:04-38.02