6.03 ACCEPTABLE USE OF YVC COMPUTERS

Approved by Administrative Council on August 8, 2006

Yakima Valley College (YVC) owns all YVC computing systems and applications. This document is intended to provide college users with guidelines for responsible and appropriate utilization of these computing and technology resources. This document supplements the YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources; all of its tenets and other applicable YVC policies, procedures and/or standards that apply to the use of the assets defined in this document as well. YVC reserves the right to determine, at any time, what constitutes appropriate use of YVC technology resources and the YVC network resources, access, and/or services provided by YVC. This document also complies with the Washington State Department of Information Services (DIS) IT Security Audit Process.

Applicability

This procedure applies to all YVC employees, students and/or non-employees who may be authorized to use any YVC technology resources as defined by this document. They shall be notified in writing of these procedures before being granted permission to access this resource. No part of this document supersedes the YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources. Its principles extend to and include any use of YVC technology resources, regardless of its location. YVC users shall also apply this procedure when using YVC technology resources to navigate through networks or computing systems beyond the local systems.

Use of YVC Technology Resources

Use of the YVC technology resources shall be for the purpose of facilitating the exchange of information and furtherance of education, and administrative missions of the college. The use of YVC technology resources will be consistent with the purposes and objectives of YVC, the Community and Technical College system (see Washington State Executive Order 91-10, Sec. III [A]) and RCW 42.52).

Goals

The goals of the Acceptable Use of YVC Computers Procedure are to:

- Help assure the integrity and reliability of the YVC internal networks, hosts on those networks and any computing resource connected to them.
- Ensure the security and privacy of the YVC computer systems and networks.
- Ensure the protection and retention of sensitive college data.
- Establish appropriate guidelines for the use of YVC-owned technology on and off- campus.

Permission

It is not the intent of this procedure to limit academic freedom, but to provide an appropriate framework for the proper exercise of those freedoms. Furthermore, it is not the intent of this procedure to impinge on the intellectual property rights of authorized users. YVC employees and students may:

- Use YVC owned computers, programs and data to which each individual has authorized access;
- Use YVC provided networking, including access to the Internet;
- Use computing and networking facilities and resources in a manner that is consistent with the mission and educational purpose of YVC.

Prohibitions

Utilizing YVC technology resources for uses and/or communications that are specifically proscribed in the YVC Board Policy 1.05 Standards of Ethical Conduct or violate any other YVC policy, procedure, or standard, and/or state and federal rule or law is strictly prohibited.

Specifically prohibited uses of YVC technology resources include:

- Subverting, attempting to subvert, or assisting others to subvert or breach the security of any YVC network or technology resource, or to facilitate unauthorized access;
- Use of any YVC technology resource to create, disseminate or execute self-replicating or destructive programs (e.g., viruses, worms, Trojan horses);
- Participating in activities involving disclosure or masquerading;
- Viewing, copying, altering or destroying data, software, documentation or data communications belonging to YVC or to another individual without permission;
- Individuals allowing another individual (whether they might otherwise be authorized to use the YVC technology resource or not) to use their login account password.

Personal Use

As defined in the YVC Administrative Procedure 6.02 YVC Acceptable Use of Technology Resources, YVC allows de minimis personal use of YVC technology resources by employees consistent with WAC 292-110-010 (3) and WAC 292-110-010 (6), unless such use is prohibited by policy/procedure, or is specifically identified as a prohibited use in the YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources.

Responsibilities

All authorized users of the YVC Network have a responsibility to comply with this procedure and to understand their responsibilities and all expectations as spelled out in the YVC Administrative Procedure 6.2 Acceptable Use of Technology Resources. This includes the requirement for confidentiality, retention and access to public records detailed there.
Yakima Valley College and its representatives also have responsibilities under this procedure. These include the responsibilities for logging and monitoring, and for the monitoring of electronic messaging systems as enumerated in the Administrative Procedure 6.01 Acceptable Use of Technology Resources. Additional specific responsibilities include:

Policy Maintenance

- **Technology Services (TS)**
  The primary responsibility for maintenance and administration of this document rests with the Director of Technology Services. TS is responsible for

drafting any updates and changes to the procedure. After appropriate campus review and final approval by the College President, TS will announce the new or revised procedure to the campus providing a brief description of the procedure and its implications for employees and other affected individuals or groups.

- **Human Resources (HR)**
  The Director of Human Resources is responsible for reviewing any updates and changes to this procedure, in light of current policies and procedures providing input on the procedure and its implications for employees and other affected individuals or groups.

Procedures
These procedures apply to all YVC employees, students and non-employees who may be authorized to use the YVC computing resources, and describe the steps to be completed, and identify who is responsible for completing them. Compliance with these procedures will assure the integrity and reliability of these resources.

Employee and Non-Employee Permission for Use

- **Network**
  Before using any YVC network resource, including computers, employees and non-employees must be authorized by the administrator for their assigned unit. The procedure for requesting login accounts is enumerated in the procedures section of the YVC Administrative Procedure 6.04 Acceptable Use of the YVC Network and Data Management Systems. The required forms for this request are also appendices to that document.
- **Non-network**
  Some YVC-owned computers may not be attached to the YVC network. However, to protect these resources from misuse and/or accidental damage, these resources will still be set up by Technology Services technical support personnel to require the use of login accounts. The same procedures for requesting network login accounts will be followed for this type of resource, despite their lack of actual network connectivity.

Student Permission for Use

- **Network**
  Before using any YVC network resource, including computers, students must be authorized. The procedure for requesting login accounts is enumerated in the procedures section of the YVC Administrative Procedure 6.04 Acceptable Use of the YVC Network and Data Management Systems.

- **Non-network**
  Some computers authorized for student use may not be attached to the YVC network. These may either be set up with a generic login account or may require the use of an appropriate student login account, depending on a security analysis of the purpose of the computer. If individual login accounts are required to access these resources—to protect these resources from misuse and/or accidental damage—the same procedures for requesting network login accounts will be followed, despite their lack of actual network connectivity.
  Issuance and/or use of non-computing technology resources will follow applicable YVC policies and procedures, and be authorized by Technology Services.

Software Installation

- All software installations and/or upgrades to software on YVC-owned computers will be done by an authorized Technology Services technical support staff member, or designee authorized by the Director of Technology Services. The specific procedures and standards regarding software installations are detailed in the YVC Administrative Procedure 6.06 Software Licensing Compliance, and the YVC IT Security Standard 6.58 Software Management.

Use of Personal Software for Work Purposes

- Under certain circumstances, personally-owned software may be installed on YVC-owned computers, provided the software is to be used for work purposes only. The specific procedures and standards regarding the use of personal software are detailed in the YVC Administrative Procedure 6.06 Software Licensing Compliance, and the YVC IT Security Standard 6.58 Software Management.

Use of YVC-owned software at home

- Under certain circumstances, YVC-owned software may be authorized for installation on personal home computers of YVC employees. Employees are never licensed to use the software at home for personal purposes. The policies, procedures, standards, and requirements for this type of software use are identified in the YVC Administrative Procedure 6.06 Software Licensing Compliance, and the YVC IT Security Standard 6.69 Use of YVC Technology Resources Off-Campus.

Use of YVC-owned computers at home

- Under certain circumstances YVC employees may be authorized to take YVC-owned computer systems home for use in fulfilling their official duties. Technology Services technical support staff, or designee authorized by the Director of Technology Services, will perform the initial installation and configuration of the software on such computers. Employees will be required to have administrative approval for this type of use and will be required to fill out and have signed a YVC Portable Device Transfer Agreement for the loan of state owned equipment to employees before taking any equipment from campus. Additionally for very short term usage, YVC Library's Media Services will loan YVC owned computer systems to employees for classroom functions, seminars or conferences through the library's resource checkout procedure.
- All provisions for the use of state-owned equipment identified in the YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources, (see also YVC Administrative Procedure 1.12 Equipment Use) will apply. All provisions of this procedure and the YVC Administrative Procedure 6.04 Acceptable Use of the YVC Network and Data Management Systems will apply. The processes, procedures and requirements for this type of software and equipment use are specifically identified in the YVC IT Security Standard 6.69 Use of YVC Technology Resources Off-Campus.

Unattended Workstation Security

- All YVC computer drives will be configured to automatically lock after 15 minutes of inactivity. This may be done by means of a password-protected screensaver. This configuration will be the responsibility of YVC technical support personnel setting up the computer.
- If any user logged into any YVC resource physically leaves the workstation

they are using, they will lock the computer by a password-protected means. Compliance with this requirement is an individual responsibility.

Security Rights

- YVC users are granted standard security privileges or access to the computing equipment assigned to them sufficient to perform their official duties. System administration, installation and removal of software (including plug-ins and system patches), and repair of YVC systems is the principal responsibility of authorized YVC TS support personnel and designees authorized by the Director of Technology Services (TS).
- In some circumstances—including physical distance of the system from technical support personnel and special technical needs, it may become necessary for the user of a YVC computer to perform some of these tasks. In these cases, the YVC employee may be granted local administrative privileges for the specific computing system assigned to him/her. The specific processes, procedures and requirements for requesting and granting these privileges are identified in the YVC IT Security Standard 6.54 Security Privileges.

Connection of Personal Computer/Telecommunications Equipment

YVC users may connect personal workstations to the YVC network for short-term use in multimedia classrooms, labs and campus meeting spaces. Personal equipment may also be connected to the YVC network or to YVC-owned computers for long-term use. The processes, procedures and requirements enumerated in the YVC IT Security Standard 6.22 Connecting Non-YVC Computer/Telecommunications Equipment to YVC Networks must be fulfilled before this type of connection may be made.

Third-Party Access to Electronic Messages

- Requests for third-party access to stored electronic messages will be handled through the college’s public record procedure (see also YVC Administrative Procedure 2.08 Public Records Request). YVC may be required to provide third parties with access in order to honor valid legal discovery and public records requests.

Right to Access

- Materials stored on the YVC network or on YVC computers are the property of the College and may be inspected at any time. Users are also reminded that these materials may constitute a public record, which can be examined by members of the public if an appropriate request is received.

Business Purposes

- If the purpose is related to routine YVC business, the Director of Human Resources, or his/her designee, will identify the specific materials required and the employee will be given sufficient opportunity to provide YVC with the requested materials.
  - In the case of an emergency, best efforts will be made to contact the employee prior to accessing the specific materials required. If such contact is not possible, the Director of Human Resources will notify the employee of the access as soon as practical.
  - Any materials so accessed will generally be copied and not removed from the employee’s system, unless otherwise directed by the Director of Human Resources.

  - After such access, the employee will be given the opportunity to change their password, if desired.

Investigations

- If the purpose is related to an investigation of a suspected illegal act or violation of YVC Policy, the Director of Human Resources, or his/her designee, may gather the specific materials with or without notification to the employee.
  - Materials so accessed may either be copied or removed from the employee's system, as directed by the Director of Human Resources.
  - Copies of all materials related to the investigation will be retained by the office of the Director of Human Resources.
  - Any individual's network use privileges may be suspended immediately upon the discovery of a possible violation of this policy. Every attempt will be made to notify the individual immediately of this suspension. These privileges may be temporarily restored at the discretion of the Director of Human Resources pending resolution of the situation.
  - Such suspected violations will be confidentially reported to the appropriate supervisors and/or administrators.
  - Appropriate disciplinary action will take place under the direction of the Director of Human Resources in situations where a violation is confirmed.
  - If the employee is cleared of any wrong-doing at the conclusion of the investigation, the Director of Human Resources will notify the employee of the access and they will be given the opportunity to change their password, if desired.

Sanctions

- Violation of any of the provisions of this procedure will be dealt with in the same manner as violations of other college policies, procedures or standards, and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including:
  - Disciplinary action – Any disciplinary action will be taken in accordance with appropriate Human Resources procedures; and/or applicable collective bargaining agreements;
  - Dismissal from the college;
  - Referral to the Washington State Ethics Board; and/or
  - Legal action.

- Some violations of this procedure may also constitute a state, local or federal criminal offense.

Definitions:

All terms defined in YVC Administrative Procedure 6.02 Acceptable Use of Technology Resources are applicable in this procedure. In addition, the following are defined:

Software

- Unless otherwise stated, "software" refers to and includes all freeware,
- shareware, and third- party products, as well as commercially acquired products.

YVC Network

- This includes the YVC_NT administrative and YVCLABS academic local area networks (LAN), the wide area networks (WAN) supporting sites separated from the main YVC campus, internet connectivity, networked infrastructure devices such as hubs, switches and servers, CTC-Net, and all other computers, networks and electronic messaging systems operated for the benefit of YVC employees and students.

YVC Technology Resources

- Includes, but is not limited to, YVC-owned desktop, laptop or mainframe computer hardware or software; software licenses; workstations; data systems; personal digital assistants; electronic messaging systems; E-mail systems; pagers; telephones—both wired and cellular; SCAN services; voicemail systems; fax machines; YVC network resources, whether wire-based or wireless; Internet connections, accounts or access; and documentation photocopiers authorized by YVC to be used by employees, students and/or other campus users.

De Minimis

- The use of state resources is considered de minimis if the actual expenditure of state funds is so small as to be insignificant or negligible, any such use of the resource is brief in duration, occurs infrequently and is the most effective use of time or resources, if the use does not disrupt or distract from the conduct of state business due to volume or frequency, the use does not disrupt other state employees and does not obligate them to make a personal use of state resources; and the use does not compromise the security or integrity of state property, information, or software.

Disclosure

- This occurs when an unauthorized user gains access to information. Disclosure often occurs when messages are forwarded to unauthorized users.

Masquerading

- This is when a user presents himself/herself to the system as another user. This may be done in order to gain unauthorized access to information or resources, to disseminate (mis)information in another's name, or to block or deny a system from operating correctly.

Unauthorized Access

- Includes gaining access to accounts, resources, messages or files to which one is not granted privilege by the owner or sender.

RELEVANT LAWS AND OTHER RESOURCES

Revised Code of Washington http://apps.leg.wa.gov/rcw/
Washington Administrative Code http://apps.leg.wa.gov/wac/
Washington State DIS IT Security Policy http://isb.wa.gov/policies/security.aspx
Washington State DIS IT Security Audit Standards http://isb.wa.gov/policies/security.aspx
Washington State Ethics Board http://www1.leg.wa.gov/LEB/

Revision Log

Date	By	Notes

Procedure Contact: Director of Technology Services