# 700.125 ACCEPTABLE AND ETHICAL USE POLICY

## A. PURPOSE

This acceptable and ethical use policy is intended to provide Wenatchee Valley College (WVC) technology users, including but not limited to employees, students, guests and vendors, with guidelines for responsible and appropriate use of the WVC computing and technology resources. WVC owns all college computing systems and applications, including professional development devices, and reserves the right to determine, at any time, what constitutes appropriate use of the college network, devices and resources. Technology resources are provided to support the college's mission, including educational, research and administrative functions. The role of the WVC Information Technology department is to foster and support the learning processes, provide services for students, faculty, and staff, and facilitate connectivity between college sites, the community, on-line learning resources, and other educational colleges, in accordance with the laws and regulations of the state of Washington.

This policy does not intend to expand, diminish, or alter academic freedom but to provide an appropriate framework for the proper exercise of those freedoms consistent with Washington state laws and the academic freedom provision.

This policy applies to all users who may be authorized to use any WVC technology resources and applies to the use of state resources at WVC facilities or any use of WVC technology resources, regardless of its location.

## B. GENERAL GUIDELINES

### 1. Acceptable Uses

Authorized use of WVC’s electronic information resources must comply with the mission of the college and be directly tied to the accomplishment of the college’s stated strategic outcomes and in compliance with [WAC 292-110-010](https://apps.leg.wa.gov/WAC/default.aspx?cite=292-110-010) – Use of State Resources, including, learning, teaching, research and college business.

### 2. Responsible Use

Users are expected to use the college's technology resources responsibly, ethically, and in compliance with applicable laws, regulations and college policies. Users must respect the rights of others and must not engage in activities that may disrupt or compromise the integrity, availability or security of technology resources.

### 3. Ownership and Personal Use

Users should understand that the college’s technology resources are the property of the state of Washington. While reasonable personal use is permitted under the de minimis use standard as outlined in [WAC 292-110-010](https://apps.leg.wa.gov/wac/default.aspx?cite=292-110-010), such use should not interfere with academic or work-related activities, violate any laws or regulations or result in additional costs to the college. The college reserves the right to monitor and restrict personal use, if necessary.

## C. DEVICE USAGE

### 1. Authorized Use

Users may only use devices authorized by the college for academic or work-related activities. Unauthorized devices may not be connected to the college’s networks or used to access its technology resources.

### 2. Device Security

The college technology department is responsible for ensuring the security of their devices. This includes keeping devices up to date with security patches, running up to date antivirus software, and implementing appropriate security measures and group policies to protect against unauthorized access. [16 C.F.R. 314.4(c)(2)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4)

### 3. Personal Device Use

Use of personal devices to access college data and resources will be allowed if the device is deemed compliant. A compliant device must be up to date with OS security patches, anti-virus definitions and browser updates. For more information, please refer to college policy 710.500, mobile communications devices and accompanying procedure, 1710.500.

## D. NETWORK AND INTERNET USAGE

### 1. Internal Network Access

Users may only connect to the college’s networks using authorized means. Unauthorized access points, routers, or any other network equipment that may disrupt or compromise the integrity, availability, or security of the college’s networks is prohibited.

### 2. External Network Access

Users who have a business case approved by their cabinet level supervisor to access the college network remotely, will be provided with an authorized access method. Unauthorized access is not permissible.

### 3. Internet Access

Users should use the college’s internet access for educational, research and work-related purposes. Accessing or distributing unlawful, offensive, or inappropriate material through the college’s networks is prohibited.

### 4. Bandwidth Usage

Users should use the college’s network resources responsibly and avoid excessive or unnecessary use that may degrade network performance for others. Activities such as streaming high-bandwidth media, downloading large personal files, or engaging in online gaming, unless by sanctioned clubs or events, is not allowed.

### 5. Monitoring of Use

WVC reserves the right to monitor all network activity, including network and internet traffic, website usage, downloads and streaming services.

## E. COMMUNICATION GUIDELINES AND REQUIREMENTS

### 1. Unwanted Emails

Users will respect other users by not sending unwanted email messages, flooding the system with spam, sending frivolous or harassing messages or emails of a personal nature.

### 2. Spam

Occasional unsolicited receipt of email should be deleted, report repeated unsolicited receipt of email to helpdesk@wvc.edu.

### 3. Communications

All electronic communications (emails, texts, files, instant messages, voicemail messages) between staff and students are discoverable and subject to Freedom of Information Act requests. Any use of unauthorized communication methods is not permissible.

### 4. Authorized Communication Methods

When communicating with students, staff members should use one of the following authorized methods:

#### College provided email.

#### OneDrive or SharePoint (file sharing).

#### Learning Management System (LMS) Canvas Messaging or class related file sharing.

#### College provided texting system.

#### ctcLink.

#### College website.

## F. LEGAL USE GUIDELINES

### 1. Copyright Protected Resources Usage

Users must adhere to all local, state, and federal laws and regulations when using copyright protected resources, including software, images, music or other intellectual property. These must be used in compliance with the [U.S. Copyright Act](http://www.law.cornell.edu/uscode/17/).

### 2. Harassment and Cyberbullying

Transmitting images, sounds, or messages to others which might be considered harassing, malicious and/or cyber bullying is not permissible.

### 3. Illegal Use

Information technology resources may not be used for any illegal or criminal purposes.

### 4. Hacking or Network Intrusion

Users may not use college resources to attempt to break into, gain root access, probe, disrupt, or obstruct any system or network. Installation of invasive software or testing security flaws without authorization on any system is not permissible.

## G. DATA AND INFORMATION SECURITY

### 1. Data Protection

Users must respect the privacy and confidentiality of collegial data, as well as personal data of others. Users should not attempt to access, copy, modify, share, or delete data or information without proper authorization.

### 2. Passwords and Authentication

Users must adhere to password and authentication policies set by the college. Users should select strong and unique passwords that meet college password requirements, protect their authentication credentials, and not share them with others, including the technology department.

### 3. Data Encryption

All transfer of sensitive data via email, including Class 4 data, as outlined in the State Board for Community & Technical College’s (SBCTC) Data Classification [Data Brief](https://www.sbctc.edu/resources/documents/colleges-staff/data-services/data-warehouse/dataclassificationbrief.pdf), must be encrypted. Efforts to circumvent email encryption may result in disciplinary action, including dismissal, legal and civil actions.

### 4. Family Educational Rights and Privacy Act (FERPA) Compliance

Users must comply with the provisions of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of student educational records. Users should not access or disclose any student's personally identifiable information without appropriate authorization or a legitimate educational purpose. [20 U.S.C. § 1232g, 34 CFR Part 99](https://www.ecfr.gov/current/title-34/subtitle-A/part-99?toc=1).

### 5. Graham-Leach-Bliley Act (GLBA) Compliance

Users must comply with the provisions of the [Graham-Leach-Bliley Act (GLBA)](https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314/section-314.4), which requires organizations that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. Compliance includes required annual security training for all users.

## H. CONSEQUENCES OF POLICY VIOLATION

Violation of this policy may result in disciplinary action, including loss of access privileges, academic penalties, and legal or civil action as deemed appropriate by the college.

## I. POLICY REVIEW

This policy will be reviewed periodically and may be modified or updated by the college to reflect changes in technology, laws, or collegial needs. Users will be notified of any changes to this policy.

Approved by the president’s cabinet: 10/3/23

Adopted by the board of trustees: 10/18/23

Last reviewed: 10/18/23

Policy contact: Technology

Related policies and procedures

 710.210 [Privacy Policy](https://www.wvc.edu/humanresources/policies-procedures/700-technology/700.200-privacy.html)

 710.500 [Mobile Communication Device Policy](https://www.wvc.edu/humanresources/policies-procedures/700-technology/710.500-mobile-communication-devices.html)

 1710.500 [Mobile Communication Device Procedure](https://www.wvc.edu/humanresources/policies-procedures/700-technology/710.500-mobile-communication-devices.html)