



**GOVERNING BOARD POLICY (BP)**

<b>Article 1:</b>  <b>INSTITUTIONAL INTEGRITY AND MISSION AND GOALS</b>	<b>Accreditation Standard 1 &amp; 9:</b> Institution Mission and Goals and Effectiveness and Institutional Integrity
<b>Policy</b>  <b>VALUES PURSUANT TO ACCEPTABLE USE</b>	<b>Policy Number</b> BP1: 4.10
<b>Department Contact</b> Office of the Information and Technology	<b>Adopted by the Board of Trustees</b> 11/08/99
<b>Administrative Procedures</b>	<b>Revised:</b>
<b>Applicable WAC/RCW</b>	<b>Page 1 of 5</b>

**BP1: 4.10 Values Pursuant to Acceptable Use**

Cascadia Community College is a learning-centered College, maintained for the purpose of providing to all students, faculty, and staff knowledge and skills for the achievement of their academic, professional, technical, and personal goals. As a public institution of higher education, the College also exists to provide members with the capacity for critical judgment and an independent search for truth toward both optimal individual development and the well-being of the entire learning community.

Inherent in the College's mission, values, and goals are certain rights and freedoms, which provide members the support and respect needed for learning and personal development. Admission to, or employment with Cascadia Community College provides these rights to members, but also assumes that members accept the responsibility to conduct themselves in a manner that does not interfere with the purposes of the College in providing education for all of its learners.

**Purpose of Acceptable Use Policy**

The purpose of this policy is to guide students, faculty and staff in the acceptable use of Information and Learning Systems and Technology provided by Cascadia Community College.

Use of computing, telecommunications, network systems, learning systems, library systems, information and instructional technology and other related resources at Cascadia Community College is to be consistent with the educational mission of the College. Cascadia Community College's mission and goals foster learning, teaching, research, innovation, and the free exchange of ideas.

This policy establishes rules and prohibitions that define acceptable use of College systems and technology. While acceptable use is encouraged, unacceptable use may be grounds for loss of computing privileges, disciplinary action, and legal sanctions under federal, state and local laws.

### **Definitions**

**Systems and Technology:** Systems and technology comprise all computer hardware, software and associated communication technologies, including, but not limited to: administrative information systems; learning information systems; desktop computing; personal digital assistants; servers; library systems and automation; analog and digital networks (e.g., data, video, audio, voice, and multimedia); electronic (email) mail systems; television, telecommunications, and facsimile technology; routers, hubs, switches, and Internet gateways, and related and forthcoming systems and technology.

**User:** An eligible individual who is authorized to use one or more systems or technologies, and is granted appropriate access by following the approval steps prescribed for each system or technology.

**User–id:** A unique identifier assigned to a user for access to a College system or technology.

### **Guidelines**

In general, the same ethical conduct that applies to the use of all College resources and facilities applies to the use of Cascadia's systems and technology.

In making acceptable use of the College's systems and technology you must:

1. Use College systems and technology only for authorized purposes. Employee's uses of Cascadia's systems and technology are subject to the Ethics in Public Service Act (RCW 42.52), including prohibitions on the use of state resources for private gain.
2. Protect your user–id and system from unauthorized use. You are responsible for all activities on your user–id or that originate from a system.
3. Access only information that is your own, that is publicly available, or to which you have been given authorized access.

4. Use only legal versions of copyrighted software in compliance with vendor license requirements.
5. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

In making acceptable use of the College's systems and technology, you must NOT:

1. Use another person's system, user-id, password, files, or data without permission.
2. Violate the privacy of another person by disclosing or disseminating user-ids, personal identifiers, images or data without permission or authorization.
3. Use computer programs to decode passwords or access control information.
4. Attempt to circumvent or subvert system or network security measures.
5. Engage in any activity that might be purposefully harmful to systems and technology, or to any information stored thereon, at Cascadia, or that of any other company, organization, or individual, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to College or personal data.
6. Use College systems and technology for commercial or political purposes.
7. Make or use illegal copies of copyrighted software, **music or videos**, store such copies on College systems, or transmit them over College networks.
8. Use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or user-id.
9. Waste computing, network, technology resources, for example, by intentionally placing a program in an endless loop, **outside of a classroom assignment**, printing excessive amounts of paper; **configuring a college computer or connecting an outside computer to act as a server that shares files, music or movies via the Internet**; or by sending chain letters or unsolicited mass mailings (**spamming**).
10. Use the College or university's systems or networks for personal gain; for example, by selling access to your user-id or to the College's systems, network or technology, or by performing work for profit with College resources in a manner not authorized by the College.

11. Engage in any other activity that does not comply with the guidelines presented above.

### Privileges

Access to use the College's systems and technology is assigned and managed by system administrators. All access, including the issuing of user-ids, must be approved by the appropriate system administrator. Users may not, under any circumstances, transfer or confer these privileges to other individuals.

### Responsibilities

All authorized users are expected to read and comply with the responsibilities set forth in this policy, as well as any additional guidelines established by individual departments or by individual instructors. By using any College system or technology, users agree that they will comply with all applicable rules and responsibilities.

Changes to system and technology policies or procedures will be broadcast and posted. Users are responsible for checking policies and procedures whenever changes are announced or when they return from an extended absence.

All authorized users will be required to sign a **Computer Use Policy Acknowledgement**. Failure to abide by the terms and conditions specified by [the Computer Use Policy Acknowledgement](#) and this policy may result in temporary or permanent denial of access to the College's systems and technology. Punitive or legal action may also be taken in accordance with College policies and procedures and all federal, state and local laws. **Copies of the signed Computer Use Policy Acknowledgement for employees will be retained in the Human Resources Office. The Computer Use Policy Acknowledgement for students is captured electronically at the Open Learning Center as part of the network account activation process.**

Copies of signed Account Requests will be retained in the Information and Learning Systems and Technology Office.

### Rights

Cascadia Community College reserves all rights, including termination of service, to all systems and technology, facilities and accounts owned or operated by the College. The College reserves the right, without notice, to limit or restrict individual use and hours of operation; to inspect, copy, or remove data, file or system resources; and to log and audit activities on its systems and technology.

All users of the College's systems and technology resources are advised that you have no legitimate expectation of privacy. When given cause, the College reserves the right to monitor an individual's use of its systems and technology resources.

Cascadia Community College makes no warranties of any kind, whether expressed or implied, for system and technology resources or services, or the contents therein, nor shall the College be liable in any event for incidental or consequential damages, direct or indirect, resulting from the use of system and technology resources or services. This includes but is not limited to: loss of data, a breach of security, the transmission of misinformation or the receipt of offensive material. The College cannot guarantee that messages or files are private and secure.

The College cannot protect individuals against the existence or receipt of material that may be offensive to them. As such, those who make use of electronic communications are warned that they may encounter or be the recipients of material they find offensive or objectionable in nature or content.

Electronic mail (email) messages and web site activities are public records subject to disclosure under Washington's Public Disclosure Act. While there are limited exceptions to the disclosure requirements, state law favors broad disclosure of public documents. Users should be aware that deleted email messages and files can be recovered and will be disclosed pursuant to state law.