

5000 ACCEPTABLE USE OF BELLEVUE COLLEGE COMPUTERS

Original Date: 6/10/2003 * Last Revision Effective: 5/21/2009

Policy Contact: Dean, Information Resources

POLICY

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

Applicability

This policy applies to all Bellevue College employees, students and/or non-employees who may be authorized to use any Bellevue College technology resources as defined by this policy. They shall be notified in writing of these policies before being granted permission to access this resource. No part of this policy supersedes the Acceptable Use of State Resources policy.

This policy shall also apply to the use of all state resources at Bellevue College facilities as defined by policy and/or as defined by state or federal law. Its principles extend to and include any use of Bellevue College technology resources, regardless of its location. Bellevue College users shall also apply this policy when using Bellevue College technology resources to navigate through networks or computing systems beyond the local systems.

Use of Bellevue College Technology Resources

Use of the Bellevue College technology resources shall be for the purpose of facilitating the exchange of information and furtherance of education, research, and administration missions of the college. The use of Bellevue College technology resources will be consistent with the purposes and objectives of Bellevue college and 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 Bellevue College Computers policy are to:

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

Permission

It is not the intent of this policy to limit academic freedom in any way, but to provide an appropriate framework for the proper exercise of those freedoms. Furthermore, it is not the intent of this policy to impinge on the intellectual property rights of authorized users.

Bellevue College employees and students may:

- Use Bellevue College owned computers, programs and data to which each individual has authorized access;
- Use Bellevue College 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 Bellevue College.

Prohibitions

Utilizing Bellevue College technology resources for uses and/or communications that are specifically proscribed in the Bellevue College Acceptable Use of State Resources policy or violate any other Bellevue College policy and/or state and federal rule or law is strictly prohibited. Specifically prohibited uses of Bellevue College technology resources include:

- Subverting, attempting to subvert, or assisting others to subvert or breach the security of any Bellevue College network or technology resource, or to facilitate unauthorized access;
- Use of any Bellevue College 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 Bellevue College or to another individual without permission;
- Individuals allowing another individual (whether they might otherwise be authorized to use the Bellevue College technology resource or not) to use their login account password.

Personal Use

As defined in the Bellevue College Acceptable Use of State Resources policy, Bellevue College allows “de minimis” personal use of Bellevue College technology resources by employees consistent with [WAC 292-110-010 \(3\)](#) and [WAC 292-110-010 \(6\)](#), unless such use is prohibited by this policy, or is specifically identified as a prohibited use in the Bellevue College Acceptable Use of State Resources policy.

RESPONSIBILITIES

All users of the Bellevue College network have a responsibility to comply with this policy and to understand their responsibilities and all expectations as spelled out in the Acceptable Use of State Resources policy. This includes the requirement for confidentiality, retention and access to public records detailed there.

Bellevue College and its representatives also have responsibilities under this policy, including:

Policy Maintenance

- **Information Resources (IR)**
 - The primary responsibility for maintenance and administration of this policy rests with the dean of information resources. IR is responsible for drafting any updates and changes to the policies and procedures, with input from the Technology Advisory Committee. After appropriate campus review and final approval by the college president, IR will announce the new or revised policy to the campus providing a brief description of the policy and its implications for employees and other affected individuals or groups.
- **Technology Advisory Committee (TAC)**
 - The Technology Advisory Committee (TAC) is responsible for reviewing Bellevue College technology strategies and serving as a conduit for dialogue between IR and the campus regarding all technology policies and procedures. Membership of this group is representative of the campus, and supports the dean of information resources by advocating for and presenting the campus technology needs.
- **Human Resources (HR)**
 - The vice president of human resources is responsible for reviewing any updates and changes to this policy and procedures in light of current policies, providing input on the policy and its implications for employees and other affected individuals or groups.

DEFINITIONS

All terms defined in the Acceptable Use of State Resources policy are applicable in this policy. 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.

Bellevue College Network

- This includes the administrative and academic local area networks (LAN), the wide area networks (WAN) supporting sites separated from the main Bellevue College 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 Bellevue College employees and students.

Bellevue College Technology Resources

- Includes, but is not limited to, Bellevue College-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; voice mail systems; fax machines; Bellevue College network resources, whether wire-based or wireless; Internet connections, accounts or access; and documentation photocopiers authorized by Bellevue College to be used by employees, students and/or other campus users.

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 him/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](#)

[Washington Administrative Code](#)

[Washington State Department of Information Resources IT Security Policy](#)

[Washington State Auditor's Office IT Security Audit Standards](#)

[Washington State Ethics Board Rules](#)

Bellevue College Policy # 5250: Information Technology (IT) Security

Bellevue College Policy # 4400: Acceptable Use of State Resources

Bellevue College Policy # 5150: Acceptable Use of Bellevue College Networks and Systems

Bellevue College Policy # 5100: Software Licensing Compliance

Bellevue College Policy # 1500: Access to Public Records

Bellevue College Procedure # 5000P: Acceptable Use of Bellevue College Computers

Bellevue College IT Security Standard: Security Program and Strategy

Bellevue College IT Security Standard: Connecting Non-Bellevue College Equipment to the Bellevue College Networks

Bellevue College IT Security Standard: Security Privileges

Bellevue College IT Security Standard: Software Management

Bellevue College IT Security Standard: Use of Bellevue College Resources Off-Campus

REVISION HISTORY

Original 6/10/2003

Revision 5/21/2009

APPROVED BY

President's Staff