

5150 ACCEPTABLE USE OF THE BELLVUE COLLEGE NETWORK AND BELLEVUE COLLEGE DATA MANAGEMENT SYSTEMS

Original Date: 6/10/2003 * Last Revision Effective: 5/21/09

Policy Contact: Dean, Information Resources

POLICY

Bellevue College owns the Bellevue College network systems and applications. This policy is intended to provide Bellevue College network users with guidelines for responsible and appropriate utilization of this resource. This policy supplements the Bellevue College Acceptable Use of State Resources Policy; all of its tenets and any 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 the Bellevue College network and any computing access and 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 non-employees who may be authorized to use the Bellevue College network 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 or attempted use of the Bellevue College network, regardless of point of origin. Bellevue College users shall also apply this policy when using the Bellevue College network to navigate thorough networks beyond the local systems.

Use of the BCC Network and Data Management Systems

Use of the Bellevue College network and Bellevue College data management systems shall be for the purpose of facilitating the exchange and storage of information, including information on students and/or employees, and compliance with and furtherance of, the education, research, and administrative missions of the college. The use of the Bellevue College network and Bellevue College data management systems 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 the Bellevue College Network and Bellevue College Data Management Systems Policy are to:

- Help assure the integrity and reliability of the Bellevue College internal networks, hosts on those networks, the Bellevue College databases, legacy systems, web-accessible resources, and any computing resource connected to them.
- Ensure the security and privacy of Bellevue College computer systems, networks and data.
- Ensure the protection and retention of sensitive college data.
- Establish appropriate guidelines for the use of the Bellevue College network and Bellevue College-owned data, whether accessed from on or 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 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 networks, computers, programs and data to which each individual has authorized access;
- Use Bellevue College provided networking, including access to the internet;
- Use these computing and networking facilities and resources in a manner that is consistent with the mission and educational purpose of Bellevue College.

Prohibitions

Utilizing the Bellevue College Network and the Bellevue College Data Management Systems for uses and/or

communications that are specifically proscribed in the Bellevue College Acceptable Use of State Resources Policy or which violate any other Bellevue College policy and/or state and federal rule or law is strictly prohibited. Specifically prohibited uses of the Bellevue College Network and Bellevue College Data Management Systems include:

- Subverting, attempting to subvert, or assisting others to subvert or breach the security of any Bellevue College data, network, or technology resource, or to facilitate unauthorized access;
- Use of any Bellevue College network or Bellevue College data management system 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 network and/or Bellevue College data management systems or not) to use their login account password.
- Accessing data for any purpose other than to perform the official duties of a Bellevue College position.
- Unauthorized disclosure of information to a third party.
- Bypassing the Bellevue College data management systems "time-out" feature, unless specifically authorized by the dean of Information Resources.

Personal Use

Bellevue College allows de minimus personal use of the Bellevue College network by employees consistent with [WAC 292-110-010 \(3\)](#) and [WAC 292-110-010 \(6\)](#), unless such use is specifically prohibited by this policy. This personal use is defined in the Bellevue College Acceptable Use of State Resources Policy.

RESPONSIBILITIES

All users of the Bellevue College network and Bellevue College data management systems 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. These include the responsibilities for logging and monitoring, for the monitoring of data management systems and for the monitoring of electronic messaging systems as enumerated in the Bellevue College Acceptable Use of State Resources. Additional specific responsibilities include:

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.
- **Student Services (SS)**
The dean of Student Services is responsible for reviewing any updates and changes to this policy and procedures in light of current data management 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:

Bellevue College Data Management Systems

- This includes the student management system, human resources, finance, cashiering, degree audit and individual databases created by individual departments or the College.

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.

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, 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 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 Services IT Security Policy](#)

[Washington State Department of Information Services IT Security Audit Standards](#)

[Washington State Ethics Board Rules](#)

Bellevue College IT Security Policy

Bellevue College IT Security Strategy

Bellevue College Acceptable Use of State Resources Policy

REVISION HISTORY

Original 6/10/2003

Revision 3/22/2005; 9/20/22005; 5/21/2009

APPROVED BY

President's Staff