

EvCC7010P: ACCEPTABLE USE OF THE EVERETT COMMUNITY COLLEGE NETWORK, COMPUTERS AND DATA MANAGEMENT SYSTEMS PROCEDURE

Original Date: August 22, 2009

Revision Date: May 28, 2013

Procedure Contact: Executive Director of Information Technology

RESPONSIBILITIES

All users of the Everett Community College network and Everett Community College data management systems have a responsibility to comply with this policy and to understand their responsibilities and all expectations including the requirement for confidentiality, retention and access to public records.

Utilizing the Everett Community College network and the Everett Community College data management systems for uses and/or communications which violate any other Everett Community College policy and/or state and federal rule or law is strictly prohibited. Specifically prohibited uses of the Everett Community College network and Everett Community College data management systems include:

- Subverting, attempting to subvert, or assisting others to subvert or breach the security of any Everett Community College data, network, or technology resource, or to facilitate unauthorized access;
- Use of any Everett Community College network or Everett Community 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 Everett Community College or to another individual without permission;
- Individuals allowing another individual (whether they might otherwise be authorized to use the Everett Community College network and/or Everett Community 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 an Everett Community College position.
- Unauthorized disclosure of information to a third party.
- Bypassing the Everett Community College data management systems "time-out" feature, unless specifically authorized by the executive director of information technology.

Personal Use

Everett Community College allows de minimus personal use of the Everett Community 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 Everett Community College acceptable use of state resources policy.

Guidelines for Determining Unacceptable Use

The following examples provide guidelines for determining whether a particular action is deemed unacceptable, but are not a complete list of all unacceptable uses.

1. Do not obtain, use or share any other users' password.
2. Attempt either directly or indirectly through use of any software or equipment to gain access to files, transmissions or other resources to which you have not been granted permission.

3. Download, modify, transmit, reproduce, publish or distribute information, software or materials which are protected by copyright without permission of copyright owner.
4. Use email, listservs, web sites or other Internet services to transmit any communication where the meaning of the message, its' transmission or distribution is intended to be or is perceived to be abusive, offensive or harassing to the recipient(s).
5. Directly or indirectly restrict, inhibit or interfere with the ability of the college, college constituents, employees or students to conduct college business or to access and use the Internet, college servers or services by hosting unauthorized services or transmitting software or information containing a virus, bomb, worm, Trojan or other harmful feature, or otherwise engaging in a DOS (denial of service) attack.
6. Change or add cabling (e.g. unplugging state equipment and plugging in personal equipment without prior authorization.)
7. Use the system for commercial gain.
8. Steal, vandalize or obstruct the use of computing equipment, services or documentation.
9. Use any software obtained illegally or not properly licensed.
10. Installing any software on state computers without prior authorization by IT
11. Any activity using excessive network band-width.

Violations of Acceptable Use Policy

Violators of this policy by anyone will be subject to the normal disciplinary procedures of the College, including those described in the Student Handbook in the section titled Student Rights and Responsibilities and employees as per the relevant collective bargaining agreement and/or those described below. Violations of this policy will be dealt with in a serious and appropriate manner according to one of the four categories described below. Illegal acts involving College computing resources may also be subject to prosecution by local, state or federal authorities. Additionally, each violation will be entered and submitted using the Incident / BIT reporting form.

Category 1 Offense: These offenses generally show a lack of consideration of computing resource and/or other computer users, but do not threaten privacy, computer integrity or violate ethical principles. Violators will be issued a verbal, Email or hardcopy warning regarding their actions. Repeated offense in this category will result in a Category 2 disciplinary action.

Category 2 Offense: These offenses often involve violations of ethical actions, for example, where user privacy or computer integrity was violated. Violators will have their user account and computer access (including access to the computer labs) suspended until a formal session with the Executive Director of Information Technology. A copy of this policy will be provided to the user with the specific area of offense highlighted. Repeated offense in this category will result in a Category 3 disciplinary action.

Category 3 Offense: These offenses generally warrant an investigation and an incident report by the Director of Security and/or the Dean of Student Development and Diversity Advocacy. Violators will have their user account and computer access (including access to the computer labs) suspended. The violator **MUST** attend a session with the Director of Security and/or the dean of student development and diversity advocacy. All computer privileges will continue to be

suspended until the completion of the investigation and issuance of a report by the Director of Security. In most cases the appropriate College official will make the determination if computer privileges are to be returned to the violator. Repeated offense in this category will result in a Category 4 disciplinary action.

Category 4 Offense: These offenses generally warrant an investigation and an incident report by both the Director of Security and local, state or federal law enforcement. Violators committing a Category Four offense will forfeit all rights to computer privileges. Any and all information requested by the Director of Security, local, state or federal law enforcement will be provided. If the violator is found guilty of the offense under investigation, any future access to College computer resources must be first approved by the appropriate College official, and that official may stipulate usage only under supervised circumstances.

Any computer offense not explicitly classified in this policy will be reviewed on a case-by-case basis. The College reserves the right to stiffen or lessen the penalties based on situations involved in the offense.

RELEVANT LAWS AND OTHER RELATED INFORMATION

[RCW 42.52](#)

[WAC 292-110-010 \(3\)](#)

[WAC 292-110-010 \(6\)](#)

[Washington State OCIO Securing Information Technology Assets Policy](#)

[Everett Community College Ethics Policy](#)

REVISION HISTORY:

Original Date: August 22, 2009

Revision Date: May 28, 2013

APPROVED BY:

VP Staff