

## **Policy Approval Form**

Executive Summary. (Type a short summary of the process followed to develop this policy, identify those involved in its development, reason for undertaking the process, and key features of the policy). This section is to be completed by the group or individual assigned to develop this policy.

### **Appropriate Use Policy**

The Evergreen State College has a history of the extensive use of technology in support of teaching, learning and administrative processes. To date, we have over 1,600 individual computing devices, over 50 servers centralized within our data center and numerous other computing related devices across campus. This large hardware inventory provides the computing resources for a large and diverse inventory of software applications. These computing devices and applications use the extensive campus intranet connections for transmitting data across campus and the internet to communicate around the world. The use of these technology resources is governed by state statute, administrative codes and Evergreen policies. Evergreen's Appropriate Use Policy provides guidelines for faculty, students and staff in the use of technology.

The Appropriate Use Policy was drafted and implemented in November of 2005. Since its drafting technology as well as the state rules around the use of technology have changed significantly. The purpose of the attached redraft to the Appropriate Use Policy is to update the policy to be consistent with current state law and administrative codes.

There are two proposed changes to Evergreen's Appropriate Use Policy. The first proposed change is to provide the campus community with guidelines on the storage of confidential data. Examples of confidential data may include but are not limited to, Social Security Numbers, Driver License Numbers, credit card numbers, date of birth, etc. The revision to the policy prohibits the storage of confidential, personal identifiable data on portable devices because of the high risk for loss of data. Loss of personal identifiable data can have significant impact on the individuals whose data is lost or stolen and the college in general. Examples of portable devices include removable hard drives, "thumb" drives, laptops, tablet PCs, etc. The policy does allow faculty and staff to gain an exception to this policy by working with Technical Support Services to ensure the data stored on a portable device is secure.

The second proposed change to our Appropriate Use Policy is in response to the Department of Information Services (DIS) requirement that all institutions make security awareness training available to all employees. The purpose of this training is to provide technology users with the information necessary to reduce the potential of data loss. The training is required by DIS policy to be provided to all employees annually. Training is currently available in a video format on the Evergreen Human Resource webpage at <http://www.evergreen.edu/employment/training.htm> . Classroom training will also be made available quarterly and will be included in all New Employee Orientation sessions.

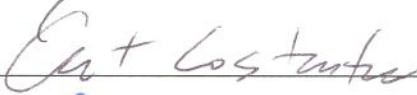
Please contact Aaron Powell, Director of Computing and Communications at 867-6238 with questions about the proposed changes to Evergreen's Appropriate Use Policy.

**Appropriate Use Policy**

**October 2007**

Vice President for Academic Affairs and Provost  Date 11-13-07

Vice President for Finance and Administration  Date 11/13/07

Vice President for Student Affairs  Date 11/13/07

Vice President for College Advancement  Date 11/13/07

President  Date 11-16-07

Date policy becomes effective \_\_\_\_\_