OPPM 8000 – Information Resources and Technology
Table of Contents

Section

SKAGIT VALLEY COLLEGE
POLICY/PROCEDURE
FOR
Information Resources and Technology

Section: **8000**	**Initial Date of Approval:** **Revision Date(s): 6/14/10**

PURPOSE

This section sets forth the policies and procedures related to the appropriate and acceptable use of technology at SVC.

REFERENCES

RCW 43.105.041
RCW 42.52
RCW 43.105.017
RWC 4.24.405
RCW 9A.36.080
RCW 7.42.010
17 U.S.C. (2007). [Copyright]
17 U.S.C. § 1201 et. seq. (2007). [Digital Millennium Copyright Act]
17 U.S.C. §110 (2007). [Technology, Education, and Copyright Harmonization Act]
17 U.S.C. § 107 (2007). [Fair Use Guidelines]

POLICY

It is the policy of Skagit Valley College to provide a comprehensive range of appropriate technologies to support instruction, learning, and the efficient management and administration of the College's internal and external business and operations. Users will abide by all college, state, and federal regulations regarding the acquisition and use of information resources and technology.

PROCEDURES

8010 General Computing Procedures

Application of Policies

To remain in full compliance with the Information Services Board (ISB) of the Washington State Department of Information Services (DIS) Skagit Valley College (SVC) Information Technology is required to implement and maintain Policies and Standards set forth by the ISB. These Policies and Standards, maintained by the Information Technology Security Administrator, help SVC Information Technology remain in compliance with security and audit requirements.

Policies related to Faculty, Staff and Administrator will be available on the SVC portal. Policies related to Students will be made available on the SVC website.
The provision and use of computing and networking privileges is governed by Skagit Valley College's policies and standards as provided by the State of Washington or other governmental agencies. Supervisors, system and facility managers are responsible for ensuring compliance with these policies and standards.

Institutional Purposes

Use of computing resources is for purposes related to Skagit Valley College's mission of education and public service. All computer service users may use computing resources for purposes related to their Skagit Valley College studies, their instruction, their duties as employees, their official business with the College.

8020 Lab Access and Computer Use

With the exception of information kiosk stations and library reference and research terminals, Skagit Valley College does not make computers available for public use. Unauthorized use of computers or computer equipment may result in corrective and/or disciplinary action.

General purpose computer labs are made available quarterly for Skagit Valley College educational purposes to those students who have paid the appropriate fee, have current student validation, and who have signed and agreed to lab policies.

Computers located in special-use classrooms, offices or other non-public areas are not intended for general access. Computer labs designed to support specific classes or courses of study may be made available for general use during times when they are not otherwise utilized. At such times, authorized students needing access to those specific programs residing on specific machines in those labs will have preferential access.

8030 Electronic Mail Procedures

Global or group messages shall be limited to the students' studies or work assignments Students may not send 'random' email messages. Users may not send messages that could be interpreted as harassing, threatening, or obscene, or which create a hostile environment.

College email capabilities shall not be used for non-College-sanctioned purposes including non-College-related fundraising, non-College related commercial purposes, or for political lobbying.

Electronic mail systems shall not be disrupted, used for chain letters or used to conduct illegal activities.

8040 Web Pages Procedures

Faculty or students in classes may publish web pages on the World Wide Web within limits established by the Public Information Office and Information Technology, and within the reasonable physical limits of the systems involved. For operational safety the College Webmaster will have full server access to any page being hosted on the Colleges' wide area network (www)

An official College-Hosted web page represents Skagit Valley College and its official programs and departments. Official College Hosted Web Pages are treated as publications, and must comply with standards, procedures, and policies set forth by the College. The Public Information Office approves the information on these pages prior to posting and retains editorial control of appearance and content of College web pages.

A faculty web server which contains individual course and faculty information does not require pre-approval nor is it monitored by the Public Information Office. Content of faculty web pages is subject to the approval of the appropriate department. The server and software for the faculty web information pages is maintained by Information Technology.

Student web pages may be maintained and sponsored by various college departments. These pages must meet appropriate college, and state and federal regulations. These pages are not maintained or evaluated by the Public Information Office or Information Technology.

Use, Responsibility and Content

Users assume responsibility for the content of their web pages. They must abide by all college, state, and federal laws that pertain to communication and publishing. Users of the College's information systems are subject to such laws and that the consequences of violations can be severe.

Users may not use home pages for non-College related commercial activity. This includes but is not limited to running any sort of private business through a home page.

Users may not use web pages for fund-raising or advertising for commercial or non-commercial organizations, except for College-related events.

Responsibility for the content of users' web pages resides solely with the author(s). The views and opinions expressed by users on their personal pages are strictly the views and opinions of the authors and do not carry the official sanction of the College.

Users may not use the College name in their web pages in any way that implies endorsement of other organizations, products, or services. Permission to use the College name, logos, and seal in any way shall be granted by the Public Information Office only.

8050 Electronic Citizenship Procedures

Usage

Computing resources should be used appropriately in accordance with the high ethical standards of the College. College networks and equipment must comply with the standards of State ethics laws and use policies of those networks which provide service.

Passwords

Passwords shall not be shared or made available to others. Student users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, whether on the Skagit Valley College campus or elsewhere.

Identification

Users must not forge or otherwise attempt to send mail that contains false address information, or represent themselves as others.

Harassment

Campus computer resources shall not be used for the purpose of harassing other users or creates a hostile work or learning environment, either on the campus or elsewhere.

System Misuse

College computer resources shall not be used for the purpose of impairing the use or operations of any computing system or network on the campus.

Hacking

Campus computing users shall not, by any means, attempt to infiltrate or 'hack' into a computing system or network at College facilities or elsewhere. Users may not capture, record, or monitor any traffic on any network in an attempt to violate the system or security, or to gain access to private communications.

Alterations

Users shall not attempt to damage or intentionally alter the hardware or the software components of a computing system or network, either on the Skagit Valley College campus

Equipment Attachment

Users may not physically attach non-College computers to College-owned computer equipment, peripherals or the network without Information Technology authorization.

Users may not reconfigure or reconnect Skagit Valley College systems or equipment without Information Technology authorization.

Compliance

Lab users are expected to comply fully with the instructions of facility staff and system managers. In particular, users will vacate terminals, workstations, or the facility and will surrender other resources (such as printers and software) promptly when asked to do so, both at closing times and when necessary to permit access by others.

8060 Right to Privacy

In the normal course of operating and maintaining the network and the systems connected to it, the contents of files and of data on the network will not be examined unless such files or data are causing network difficulties. Employees can expect to be notified when support personnel accessed their College-provided computers or files for maintenance or operational purposes.

In preserving the integrity and security of computing systems, SVC network staff may copy or move network-stored user files for routine backups and preservation. Program files, or files containing viruses, may be examined if such files appear to be creating network difficulties. Mail files cannot be opened by Skagit Valley College staff without the owner's knowledge.

Non-mail file contents may become known during the course of systems operations or maintenance. Program files may be examined if they are causing network difficulties.

All Skagit Valley College files, including mail files, are subject to search and seizure by law enforcement agencies without notification. State and Federal legal agencies, using

appropriate legal processes, may require access to mail files without user or Skagit Valley College knowledge.

8070 Network Resources and Operational Limits

Computing and networking resources will vary depending on need and the determinations of the Dean of Technology and eLearning and the administration.

System managers have discretion to set and revise reasonable usage priorities and operational procedures (such as hours of operation, usage time limits, populations to be served, etc.) as may be reasonably necessary for the operation of their systems or facilities.

Network operations and configurations will be determined by the Dean of Technology & eLearning and the administration taking into account security and operational efficiencies as well as College needs.

Equipment operating in violation of network policies, or which poses a risk to the network, may be removed from the network.

8080 Adjudication, Enforcement, and Sanctions

The responsibility for investigating alleged non-compliance with the provisions of these policies rests with the appropriate administrator. The investigation of alleged non-compliance with any policy in this section will be conducted in accordance with College policy, procedures and collective bargaining agreements.

Suspended Service

System managers may suspend service to users without notice when found necessary in the operation or integrity of the system or the networks connected to it. Cessation of service, whether by network disconnection or disablement of log-in capability, shall be utilized in preference to file inspection when remedying or investigating instances of alleged disruption.

Violations

Violation of the policies described herein for legal and ethical use of computing resources will be dealt with in accordance with appropriate sanctions. . Individuals accused of violations will be subject to the normal disciplinary and grievance procedures of the College or negotiated agreements. Illegal acts involving Skagit Valley College computing resources may also be subject to prosecution by State and federal authorities. Skagit Valley College will cooperate with local, State or federal agencies in ensuring that users of the SVC network are in compliance with appropriate laws and regulations.

8090 Copyright

Copyright Officer

The chief administrator of the library shall serve as the copyright officer for the college. The copyright officer shall:

Exercise general oversight of the copyright function for the college and provide training for employees, and

Ensure that information about the law and guidelines are available in appropriate instructional offices, libraries, copy centers, and college bookstores and other designated areas, and

Serve as the final authority for approval or denial of college services or requests made through the college bookstores, libraries, copy centers or other campus offices that have copiers for student and employee use, and
Serve as the final authority on appropriate use of intellectual property in both onsite and online instructional settings.

Copying Prohibitions

Copying of materials or other uses not specifically allowed by the law, fair use, license agreement, or the permission of the copyright holder is strictly prohibited.

If after a study of the law and/or guidelines there is uncertainty as to whether reproduction or use of materials meets the requirements of the law; the copyright officer shall be consulted.

If the copyright officer determines that the requirements of the law have not been met, the college employee or student requesting to copy the material must seek written authorization to copy or use the material from the copyright holder in the manner set out in college guidelines.

If the material is to be reproduced and sold in the college bookstores, the written request for authorization must state that the material is to be reproduced and sold. Permission costs for course packs will be recovered through retail distribution. An Indemnity Agreement will be required to be signed before materials will be sold in the college bookstore.

Liability and Sanctions for Liability and Sanctions for Willful infringement

In the case that an individual uses a college service to violate copyright law, the liability for willful infringement of the copyright law and guidelines shall rest with the individual requesting the work.

Skagit Valley College will impose sanctions on any student or employee where there is a finding of willful infringement of the copyright policy consistent with appropriate college policies, collective bargaining agreements and other contractual arrangements.

Copyright Authorization Files

Permanent files of all written copyright authorizations, permissions, releases, waivers, responses to requests for permissions and licensing agreements will be held in locations designated by the college president or designee.

College users are responsible for complying with the license and copyright provisions of the software that they use. No software copy is to be installed, made or distributed by any user without a prior determination that such an activity is in fact permissible. All users must respect the legal protection provided by copyright and license to programs, images, sounds and data, including protections extended to those materials which may be found on the network and internet.

The information technology department will maintain licenses of software in the general labs in Ford Hall, general labs at Oak Harbor and other lab facilities as may be determined by the College. Divisions and departments are responsible for maintaining the records of software licenses applicable in their labs or areas, as well as departmental or specific software that is placed on the network for their specific use.

8100 Limits of Liability

Skagit Valley College makes no warranties of any kind, expressed or implied, that the functions or services provided through the SVC network system will be error free or without defect. The College will not be responsible for any damages users may suffer, including, but not limited to, the loss of network services or access. The College will not be responsible for the accuracy of any information obtained through or stored on the College network system or computers.

Administrative Responsibility: Director of Information Technology

SKAGIT VALLEY COLLEGE

POLICY/PROCEDURE

FOR

Usage of Electronic Signatures

Section: 8000 **Subsection: 8110**	**Initial Date of Approval: 4/20/17** **Revision Date(s):**

PURPOSE

The purpose of this policy is to allow for electronic signatures at Skagit Valley College by methods that are practical and secure, balance risk and cost, streamline administrative processes, and comply with applicable laws.

REFERENCES

RCW 19.360.010
RCW 19.360.020
RCW 19.360.040
RCW 19.360.050
RCW 19.360.020(2)

DEFINITIONS

Term	***Definition***
Electronic signature	An electronic process, symbol, or sound attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Examples may include, but are not limited to: 1. The act and the resulting record of initiating or approving an electronic record in a college system (e.g., enterprise resource systems); or 2. The act and the resulting record of using special electronic signature software or systems (e.g., electronic signature platforms, point-of-sale electronic signature pads, biometric systems) to sign an electronic record.
Authentication	The assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.
Authorization	When an individual has verified permission and the requisite authority to sign a record (electronically or otherwise), access specific electronic college services, and/or perform certain operations, including executing agreements to bind the college.
Electronic record	d A record created, generated, sent, communicated, received, or stored and signed by electronic means

POLICY

I. Electronic signature use:

A. The use and acceptance of electronic signatures and electronic submissions of records shall be consistent with the guidance and requirements put in place by the Washington State Office of the Chief Information Officer (OCIO).

B. Transactions may be approved for electronic signatures based on the following five factors:

1. An analysis of the need for signatures
2. An analysis of the risks inherent in the process.
3. A description of the processes and methods proposed.
4. A list of specific groups or people that can or cannot use the process and alternative opt-out procedures.
5. A description of the impact to privacy and consistency with existing privacy policies

C. The college may designate specific college transactions to be executed by electronic signature.

1. Employees, including student employees, may be required to use an electronic signature for transactions with the college or to conduct college business.
2. External parties (individuals, including students, and entities not employed by the college) must use an electronic signature to conduct business with the college, unless the college or the external party opts out of conducting business electronically as provided in the Procedure section.

D. An electronic signature may be accepted in all situations when the requirement of a signature or approval is stated or implied, except when law or regulation specifically requires a hand-written signature.

E. To the fullest extent permitted by law, the college recognizes an electronic signature as legally binding.

F. When a college policy, rule, procedure, standard, law, or regulation requires or requests that a record have the signature of a responsible person that requirement or request is met by an electronic signature, except when law or regulation specifically requires a hand-written signature.

G. An electronic signature may not be valid if the individual did not have the authorization to sign an electronic record.

H. An electronic signature must employ a college-approved authentication method at the time of signature.

II. Specific methods and transactions for electronic signatures must be approved on a case by case basis by the Vice President of Administrative Services in consultation with the Business Office, and the Director of Information Technology.

III. Falsification

A. Falsification of electronic records or electronic signatures is prohibited.

B. It is a violation of this policy for an individual to sign as if they were another individual.

IV. Violations

A. Employees who falsify electronic signatures or otherwise violate this policy are subject to disciplinary action, including and not limited to termination of employment and/or potential criminal prosecution under applicable federal, state, and local laws.

B. Students who falsify electronic signatures or otherwise violate this policy are subject to disciplinary action under the Code of Student Conduct and/or potential criminal prosecution under applicable federal, state, and local laws.

C. Other individuals and entities to whom this policy applies who falsify electronic signatures or otherwise violate this policy are subject to appropriate sanctions, including but not limited to termination of the relationship and/or potential criminal prosecution under applicable federal, state, and local laws.

Administrative Responsibility: President