Shoreline
COMMUNITY COLLEGE

PROCEDURE

Policy Name:	Acceptable Use of Technology & Data
Policy Number:	4126
Applicable Code/Law:	RCW 42.52.160, WAC 292.110.010, RCW 40.14; RCW 42.17.260

Definitions

Technology, Communications Resources, and Communication Services - Any hardware, software, or services implemented for supporting campus functions or operations. Such resources and services include, but are not limited to, client workstations, laptops, or mobile devices; server hardware, network storage and share provisioning; audio, video, or other multimedia hardware and software; library automation and assistive devices; all data and communications networks and network infrastructure and hardware; operating systems and supporting application packages; all information and data files, electronic correspondence (email, instant messages, voice mail); and campus or affiliated services internet web sites and storage repositories.

Procedural Guidelines

1. Expectations of Privacy

   a. *Employees:* Shoreline Community College does not grant, implicitly or explicitly, any ownership or expectation of privacy with regards to digital communications (email, texting, voicemail, etc.), computing resources (file server shares, information and data files, or campus provided services), or Internet browsing activities.

   b. *Students:* Shoreline Community College provides students with means and accesses to technology resources for educationally-based purposes. All provided resources used for educational advancement housed, accessed, and/or maintained on campus owned resources are provided with no implied expectation of privacy.

2. Mobile devices on SCC networks

Administrative policies implemented on campus owned mobile devices apply appropriate and adequate access to ensure any / all software updates, application deployments or updates, support, or required services to maintain the device within campus defined technology policies and ensure device recovery in the event of misplacement or misappropriation.

3. Access and Use Compliance

Use of College technology implies consent and acceptance of all policies, procedures, and guidelines and agree to be bound by all regulations therein.

4. Sensitive Information

Any individual being granted access to sensitive or personally identifiable information shall adhere to all standards and accessibility requirements as established by Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children’s Online Privacy Protection Act (COPPA); any applicable policies and procedures set forth by SBCTC, and any applicable SCC policies and procedures established concerning access, use, and/or release of an individual’s information.

In accordance with law, the College will make every reasonable effort to ensure and maintain the confidentiality of sensitive data and communications.

5. De minimus Use

Utilizing principles outlined in RCW 42.52.160 and WAC 292-110-010, de minimus use of the College’s technology and communications resources and services may allow for the occasional and limited personal use when there is no cost to the district, the use does not interfere with the employee's official duties, does not interfere with the official duties of other employees, and the use otherwise complies with all applicable laws and regulations. It should be explicitly understood that all College technology and communications resources shall not be used for commercial, illegal, or political purposes.

6. Network Services (Wired and Wireless), Internet Accessibility

These service are provided for the purpose of conducting such business as necessary to complete assigned campus related tasks, functions, and responsibilities. Utilization of personal network-based shared service (iTunes, Windows Media Service, etc.) primarily focusing on audio and video streaming services are not permitted unless it is identified and documented as an exception that such services are vital to student development or job completion. Authorized users of these services are bound by College policies and any/all applicable state and federal laws.

Shoreline Community College’s Technology Support Services regularly monitors network traffic to assist in identifying abnormalities or other issues that may impact the integrity of the network and/or access to provided services. Any activity that improperly or inappropriately uses up network bandwidth, interferes with normal campus business operation, or degrades the capacity for student capability to complete their course of studies is considered to be in violation of the acceptable use policy and may result in loss of access privileges and may be subject to other punitive measures. All information and technology resources may be subject to monitoring without prior notification under the following circumstances:

- There exists a reasonable need, necessary or appropriate, to protect the integrity, security or functionality of campus technology resources.
- There exists a reasonable need, necessary or appropriate, to maintain compliance with any legal requirements protecting Shoreline Community College from liability or service disruption.
- An account appears to be engaged in unusual or unusually excessive activity.
- There exists a reasonable need, necessary or appropriate, to access an account or activity and the access is reasonable in relation to the need.

7. Traffic Monitoring

Shoreline Community College's Technology Support Services reserves the right to monitor, inspect, review, or take any action deemed appropriate upon any communications, device, software, data, etc. for the purpose of identifying any non-compliance, illegal, illicit, or malicious traffic or actions.

The results of any such general or individual monitoring, including but not limited to the contents and records of individual communications, may be released pursuant to a public records request. In addition, the College may, at its discretion, disclose the results of any such general or individual monitoring for any legitimate purpose to appropriate and authorized College personnel or law enforcement agencies and may use those results in appropriate external and internal disciplinary and other proceedings.

8. Violations

The following types of activities are considered a limited subset of inappropriate and unethical behavior that are in violation of established campus policies and potentially state and / or federal law:

- Utilization of another individual's account and / or credentials to access their private files, assigned resources, email, etc. without permission or explicit knowledge of the account owner.
- Using any tactics to misrepresent an existing network identity in any form of electronic communication.
- Accessing any such sites that provide for the distribution of illegally or illicitly acquired data or applications that when used are in violation of the manufacturer's End User License Agreement (EULA).
- Utilization of any campus or state provided resources with the intent to harass, bully, threaten, or promote violence against another person or classification of persons
- Performance or instantiation of any hardware, software, or service-based process that violates, directly or indirectly, any College, State Board for Community & Technical Colleges, State, or Federal policy or regulation; with intent, known or unknown, causing interfere with the normal operation or use of campus technology resources or services. Such process may include, but are limited to routers or switches (wireless or other); packet capturing, peer-to-peer sharing, key loggers; server services such as WWW, FTP, Telnet, SSH, DHCP, or DNS.

Any violations of the acceptable use policy, other campus policies, or established campus or technology procedures will be provided to the appropriate agency to be dealt with appropriately.