

# South Seattle Community College

## Acceptable Use of Information Technology

*All users of Information Technology (IT) resources are expected to abide by the full current version of this policy.*

### **Provision of Services**

SSCC provides IT resources in support of its mission to continuously improve student understanding and capabilities that lead to purposeful lives, contribute to a vital community and pursue lifelong learning. As an institution of higher education, the college intends to provide the community with open and unrestricted avenues of communication as long as such use is in compliance with state and federal laws, other SSCC policies and SCCD policies. The college reserves the right to summarily limit or suspend access to facilities, equipment and services, as necessary, to comply with applicable laws, to protect the interests of SSCC and other members of the community and to preserve the integrity and performance of IT systems.

### **Priority of Use**

While the college does not strictly limit the use of IT services, activities related to the college's educational mission take precedence. Use of IT resources for personal or recreational activities may be limited depending on the capacity of the IT systems to support such activities.

### **Rights and Obligations**

All users are responsible for using SSCC IT resources in an appropriate manner. All applicable laws, statutes and policies related to personal behavior apply to electronic communications. Such laws and policies prohibit, among other things, lewd or indecent conduct, threat of physical harm, stalking, forgery, and disruption of college services, damaging or destroying of property, discrimination and sexual harassment. All users are expected to respect the integrity of all security controls and abide by all security measures that have been implemented, as well as adhere to all end-user license and contractual agreements associated with SSCC IT resources.

### **Enforcement**

SSCC may deny members of the community who violate this policy or otherwise use SSCC IT resources to violate other established policies or laws access to IT resources. Violations that constitute a breach of the Code of Conduct or other SSCC policy may be referred to the respective campus authority for review and possible disciplinary action.

### **Reporting and Notification**

If a potential violation occurs in a college classroom or lab, violations should be reported to the faculty or staff monitoring the facility, or to the Director of Educational Technology and Information Technology Services. If a potential violation occurs in a non-instructional area, the situation should be reported to the supervisor of the area.

### **Complaints or Grievances**

Complaints relating to personal harassment or similar behavior should be filed directly with the responsible authority, using established procedures. Staff and administrators will not file complaints on behalf of aggrieved parties.

### **Principles of Responsible Behavior**

The following principles of responsible behavior are derived directly from the same standards of commonsense and common decency that apply to the use of any public resource.

**Principle #1:** Respect the privacy and rights of others

Users **may not** use any SSCC IT resources to:

- \* Attempt to gain unauthorized access to any system, network, service, or data inside or external to SSCC
- \* Monitor network traffic or undertake comparable measures without specific permission from the Director of Educational Technology and Information Technology Services
- \* Store or run programs that are designed to capture keystrokes, passwords, mouse clicks or data
- \* Send e-mail that is intimidating or harassing
- \* Create a hostile working or learning environment by displaying sexually explicit images or sounds
- \* Violate any laws pertaining to child pornography, obscenity and defamation
- \* Duplicate or install software except in strict accordance with applicable licensing agreements and with permission from the Director of Educational Technology and Information Technology Services
- \* House or distribute unauthorized software, music, video or other information resources

**Principle #2:** Respect other people’s ability to benefit. Users **may not** use any SSCC IT resources to:

- \* Engage in activities that compromise institutional systems or network performance
- \* Interfere with the institution’s ability to provide the best possible service to the overall community
- \* Run programs that introduce a virus, worm or another destructive or disruptive program
- \* Launch "denial-of-service" attacks against internal or external systems
- \* Create, transmit or forward electronic chain letters, "spam" or mail bombs

**Principle #3:** Identify yourself truthfully. Users **may not** use any SSCC IT resources to:

- \* Falsely identify themselves in communications
- \* Attempt to "spoof" or otherwise represent their network activities as originating from a network address other than The actual source

**Principle #4:** Unauthorized commercial use is prohibited. Users **may not** use any SSCC IT resources to:

- \* Conduct commercial activities without prior written authorization from the president of the college
- \* Market a home business
- \* Host a commercial web page
- \* Allow anyone who does not have authorized use to access any IT resource or service
- \* Share password or account (if done account will be disabled)
- \* Conduct political campaigns
- \* Operate unauthorized information services
- \* Printing- Daily limit of ten (10) pages maximum

Users are encouraged to read and comply with the full "Use of Electronic Resources" policy at <http://sccdweb.sccd.ctc.edu/services/includes/procedures/259pro.asp>

I have read and understood the Acceptable Use Policy. I understand that **I must not share my account/password with anyone else.** I understand that I will be held responsible for violations of this policy by me or by anyone using my account. In particular, I understand that I am responsible for violations of law and SCCD policy. It is SCCD policy that students not modify configurations of electronic resources, such as installing software, except as directed by appropriate staff.

I understand there is no expectation of privacy on this (or any) computer network - SSCC staff may monitor communications in the performance of their duties and the results of such monitoring may be used in disciplinary proceedings, including criminal prosecution.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
First Name (Please Print)

\_\_\_\_\_  
Last Name

\_\_\_\_\_  
Student ID Number