POLICY 4126

FACULTY AND STAFF ACCEPTABLE USE POLICY FOR INFORMATION TECHNOLOGY RESOURCES

Shoreline Community College (SCC) provides information technology resources (ITRs) to support the instructional and administrative activities of the institution. The ITRs are intended for the sole use of college faculty, staff and other authorized users. ITRs include but are not limited to host computer systems, web sites, desktop computers and workstations, communications networks, electronic software, electronic hardware, library automation systems, multi-media equipment, electronic data, computer files, video networks, telephones, voice mail, e-mail, and internet resources. Shoreline Community College reserves the right to monitor its information technology resources and to take appropriate action to protect the integrity of its computing systems, workstations, and lab facilities in accordance with existing procedures and any notification requirements. ~~-~~Use of SCC's ITRs, as state resources, does not confer a right to privacy in those resources. Information technology resources will be used according to state laws and guidelines.

Approved and adopted by Board of Trustees 5/25/01

PROCEDURAL GUIDELINES

1. ~~Acceptable Use of ITRs.~~ ITRs are to be used only for legitimate college business. ITR use will be consistent with state law and the guidelines and objectives of the college (See e.g., RCW 42.52.160). Use of ITRs must also be consistent with state ethics rules. These rules include, without limitation, WAC 292-110-010, Use of State Resources, which can be viewed at http://www.wa.gov/ethics.

2. Accounts issued to individuals (users) are intended for the sole use of that user and are non-transferable. Account passwords for individual accounts are not to be shared with others. Passwords for shared accounts must only be used by college authorized users.

3. The user is responsible for all known usage o~~f~~n his/her assigned account.

4. Users will not conceal or falsify their identity when using the college's ITRs.

5. College regulations apply to all information technology resources owned or held through agreement by the college

6. The College reserves the right to monitor use of ITRs in accordance with

existing procedures and any notification requirements. The SCC administration may specifically authorize and direct appropriate personnel to monitor user activities or examine ~~or~~ files, records, messages, or passwords for evidence of violations of applicable laws, regulations, policies, or procedures, upon determining that reasonable basis exists for such monitoring or examination. If authorized monitoring of user activities or the examination of files, records, messages, or passwords reveals evidence of possible violation of any applicable law or regulation, or any other ITR misuse, the SCC administration may provide such evidence for use in law enforcement investigations or by other authorities. If authorized monitoring reveals evidence of violation of College policy or procedure, the College may use that evidence in accordance with existing procedures

7. SCC Technology Support (TSS) personnel may monitor user activities or examine files, records, messages, or passwords when there is a system or network problem requiring maintenance or corrective action or when a user requests technical support staff assistance with an ITR problem which may involve those records. Such examination may reveal prior misuse of ITRs. TSS technical support personnel are not authorized to routinely conduct monitoring or examination of user records for the purpose of seeking evidence of user violations of either SCC policies or state or federal law.

8. If monitoring reveals possible evidence of violations of these procedures or criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials or College administration.

9. The College cannot guarantee that messages are private or secure, although the College will make reasonable efforts to maintain the confidentiality of communications. The College will abide by the following statements from WAC-292-110-010:

   Electronic mail, facsimile transmissions, and voice mail are technologies that may create an electronic record. This is what separates these from other forms of communication such as a telephone conversation. An electronic record is reproducible and is therefore not private. Such records may be subject to disclosure under the Public Disclosure Law, or may be disclosed for audit or legitimate state or management purposes.

   Public records contained on electronic message systems should be maintained according to retention schedules approved by the appropriate records committee in accordance with RCW 40.14 Preservation and Destruction of Public Records.

   While all electronic messages may be considered writings and all writings may be public records, the public does not have a right to examine every public record. RCW 42.17.260 exempts broad categories of records while

other statutes provide for confidentiality of specific records. Authorized personnel shall have access to data under users' control, as provided elsewhere in this Procedure. Electronic messages ordinarily will be backed up and retained under retention schedules in accordance with RCW 40.14. Users should assume that all electronic messages may be stored for a period of at least six months on disk or tape.

10. Files, records, messages, and passwords also may be disclosed when required by law. Electronic messages created or placed on the College's ITRs may be considered writings, and all writings are public records subject to disclosure to any requester in accordance with Washington State's Public Disclosure Act, chapter 42.17 RCW. Electronic messages also may be legally required to be disclosed to third parties in other circumstances, such as in discovery conducted during litigation.

11. It is important that members of the College community be aware of the intellectual rights involved in the unauthorized use and copying of computer software. The EDUCOM Code is a widely accepted guideline for software and intellectual rights.

    The EDUCOM Code (EDUCOM, 1987) Software and Intellectual Rights

    "Respect for the intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to all works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and the right to determine the form, manner, and terms of publications and distribution.

    Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

12. The following types of activities including but not limited to the activities below are examples of behaviors using ITRs that are unethical and unacceptable, and in some cases may violate state or federal law:

    - Accessing another individual's account, private files, or e-mail without permission of the account user.
    - ~~owner~~Misrepresenting one's identity in electronic communication.
    - Violating copyright and/or software agreements.
    - Violating rules or codes set by services subscribed to by the College.
    - Using computing resources to threaten or harass others.

- Using the College systems for non-college work, including but not limited to commercial or profit-making purposes without written authorization from the College administration.
- Surfing the Internet for personal use.
- Using e-mail and telephone for personal purposes beyond deminimus use.
- Disobeying lab and system policies, procedures, and protocol (e.g., limits on workstation usage). Intentionally and without authorization, to crash, access, alter, interfere with the operation of, or damage or destroy all or part of any computer, computer system, computer network, computer software, computer program, or computer database (SCC or otherwise). Installation of unauthorized network services (i.e., webservers, FTP servers, Telnet server, etc). Tampering with systems or files in an attempt to hide activities. Any attempt to circumvent, bypass or compromise security (SCC or otherwise). Intentional use or installation of hacker tools, viruses or system misconfigurations (e.g. trojan horses, backdoors, viruses or exploit programs) to any SCC computer. Campus Standards can be viewed at: http://intranet.shore.ctc.edu/intgovtechcom/.
- Intentionally or knowingly and without authorization, give or publish a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or database.
- Discrimination on the basis of race, creed, color, age, sex or gender, religion, disability, or sexual orientation.
- Sexual harassment.
- Copyright infringement.

Approved by President's Staff 5/14/01