

## SEATTLE COMMUNITY COLLEGE DISTRICT PROCEDURE

NUMBER: 259.10-40

### TITLE: SCCD ELECTRONIC INFORMATION RESOURCES

#### 259.10 Definitions:

- **259.10.01 Electronic Information Resources (EIRs).** All electronic hardware, software and associated data that support or include the following: administrative information systems; desktop computing; library automation; multi-media, data, video and voice networks, including Washington State Department of Information Services (DIS) SCAN network; phone terminals; voice mail; electronic mail (E-mail); Internet access; scanners; electronic publications, including video; or any similar electronic based medium. The use of these resources is a privilege, not a right. It is the user's responsibility to use these resources in a manner that is efficient, ethical and legal.
- **259.10.02 User.** Any SCCD student, employee (including a District officer), contractor, visitor, volunteer or other person who uses the District's electronic information resources. Users as defined, may use District EIRs only for authorized purposes. It is the obligation of College employees to be aware of the governing law, rules, and guidelines set forth in Chapter 42.52 RCW, Ethics in Public Service act; WAC 292-110-010, Use of state resources (Both located at URL: <http://ethics.wa.gov/rules.html>); District policies, and these procedures.
- **259.10.03 Authorized Account.** A user account established by District staff with appropriate password protection that authorizes use of District EIRs.

#### 259.20 Acceptable Use:

- **259.20.01** SCCD's EIRs are to be used for legitimate District business, and for facilitating the exchange of information to further the District's educational, research, administrative and community service purposes. Such uses shall at all times be consistent with state law and the stated purposes and objectives of the District. In accordance with RCW 42.52.160, no employee may use District EIRs that are in his/her custody or control for the private benefit or gain of that employee or of any other person, unless such use (a) is part of the employee's official duties or (b) is consistent with applicable ethics rules. These rules include, without limitation, WAC 292-110-010, Use of State Resources, which can be viewed at <http://ethics.wa.gov/rules.html>.
- **259.20.02** Employees may make occasional but limited uses of the District's EIRs to send personal messages when there is little or no cost to the District; such use does not interfere with employee's official duties; the use is brief in duration, occurs infrequently and is not disruptive to conducting District business; such use

does not compromise the security and integrity of District property, information or software; and provided that employee complies with all other requirements of state law, the EIR policy, and these procedures. Examples of such permissible incidental personal use includes (but is not limited to):

- a. Notice of public interest and public service events, such as lectures, Combined Fund Drives, blood drives, etc.
  - b. Notice of office social gatherings (lunches, birthdays, receptions, etc.)
  - c. District-wide notifications which are used for communicating good will among employees (holiday greetings, birth announcements, congratulatory messages, etc.)
  - d. Making a local telephone call or sending an e-mail message to make sure that the employee's child has arrived safely home from school.
- **259.20.03** Employees may not make private use of the District's computers or other equipment to access networks, databases, electronic bulletin boards, or the Internet, for purposes that are personal to the employee and unrelated to the employee's District work, except under the following conditions. Employees may make occasional but limited uses of District EIRs to access networks, databases, electronic bulletin boards and internet using same criteria as in 259.20.02 above.
  - **259.20.04** District EIRs shall be used in compliance with this procedure, with all collective bargaining agreements, with district regulations and with local, state and federal laws and regulations.
  - **259.20.05** EIR users shall not share their authorized accounts or account passwords with others.
  - **259.20.06** Users of SCCD electronic information resources must not intentionally seek information about, browse, obtain or retain copies of, or modify personal or private files, records, messages, or passwords belonging to other people, whether at any of the campuses or facilities of the SCCD or elsewhere, unless specifically authorized in advance to do so by those individuals.
  - **259.20.07** Users shall not interfere with the performance of any EIR, or block access to any EIR for purposes allowable under these guidelines.
  - **259.20.08** No user shall introduce invasive computer software such as viruses into any EIR. Furthermore, all EIR users are encouraged to utilize any anti-virus software provided by the District to protect electronic information.
  - **259.20.09** All use of data and software on District EIRs must comply with related licensing agreements and with copyright laws.
  - **259.20.10** Users shall be responsible for information they transmit through the District's EIRs and shall comply with the acceptable use policies of the Internet and any rules of discussion forums in which they participate. Furthermore, all such data transmissions shall conform with all local, state and federal laws and regulations.
  - **259.20.11** Users shall not conceal or falsify their identity (spoofing, using anonymous re-mailers, providing false identifications, etc.) when using the District's EIRs.
  - **259.20.12** EIRs of the District shall not be used for transmission or storage of information that constitutes or promotes:

- a. Discrimination on the basis of race, creed, color, age, sex or gender, religion, disability, or sexual orientation;
  - b. Sexual harassment;
  - c. Copyright infringement;
  - d. Any use for the purpose of supporting, promoting the interests of, or soliciting for an outside organization or group, including, but not limited to: A private business, a nonprofit organization, or a political party (unless provided for by law, authorized by an agency head or designee, or as provided in 259.20.01 or 259.20.02 above);
  - e. Any use for the purpose of assisting a campaign for election of a person to an office or for the promotion of or opposition to a ballot proposition. Such a use of state resources is specifically prohibited by RCW 42.52.180, subject to the exceptions in RCW 42.52.180(2);
  - f. Any use for the purpose of participating in or assisting in an effort to lobby the state legislature, or a state agency head. Such a use of state resources is specifically prohibited by RCW 42.17.190, subject to the exceptions in RCW 42.17.190(3);
  - g. Solicitation of political financial contributions;
  - h. Personal business interests; or
  - i. Any use related to conduct that is prohibited by a federal or state law or rule, or a state agency policy; and
  - j. Any private use of any district or state property that has been removed from district or state facilities or other official duty stations, even if there is no cost to the state.
- **259.20.13** Employees can use EIRs to communicate with a member of the legislature at the request of that member; or communicate to the legislature, through the proper official channels, requests for legislative action or appropriations necessary for the efficient conduct of their professional duties. Employees can also provide information or communicate on matters pertaining to official business to any elected official or officer or employee of any agency. Employees may also advocate the official position or interests of the agency to any elected official or officer or employee of any agency.
  - **259.20.14** No user shall transmit unsolicited and unwanted messages to any recipient except in the normal and appropriate execution of her/his official duties. Examples of such inappropriate transmissions include, but are not limited to, phone calls, faxes or e-mails that are both unsolicited and unwanted, e-mail mass mailing (spamming), and the transmission of invasive computer software.
  - **259.20.15** E-mail messages will be kept in employees e-mail account according to the Second Quarter Rule (SQR). The SQR is:
    - a. Since we are based on the Quarter System, employees will have at least two quarters of e-mail messages. On the Saturday after the 10th day of each quarter, e-mails older than two quarters will be deleted from the e-mail account.
    - b. E-mails include anything in the “Drafts”, “Inbox”, “Sent Items” and any folders created (other than Personal .pst files) within Exchange/Outlook.

- c. Tools or means available to ensure necessary e-mails are not deleted include:
  - Setup Personal Folders on work station and either establish rules to move messages to folders or move messages manually;
  - Forward messages to home e-mail;
  - Save messages to work station hard drive or write to floppy;
  - Save messages as text files to CD and read as Word documents.

**259.30 Violations and monitoring:**

- **259.30.01** Violation of any of these procedures may result in the temporary or permanent denial of access to SCCD's EIRs, the imposition of appropriate disciplinary action (i.e., discipline of a student or employee), and/or civil and/or criminal sanctions.
- **259.30.02** SCCD EIR technical support personnel may monitor user activities or examine personal or private 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 EIR problem which may involve those records. EIR 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 SCCD policies or state or federal law.
- **259.30.03** The District reserves the right to monitor the use of any EIR under certain conditions. The SCCD administration may specifically authorize and direct appropriate EIR technical support personnel to monitor user activities or examine personal or private 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. Users are advised that if such authorized monitoring reveals possible evidence of violation of any District policy or procedure or any other applicable law or regulation, or any other EIR misuse, the SCCD and its administration may use or provide such evidence in appropriate investigations and sanctions.
- **259.30.04** SCAN monthly report monitoring is conducted by a designated campus or department administrator who visually reviews the report. If a charge appears excessively high or unusual, the responsible administrator will contact the department or the individual who placed the call to confirm whether or not the call is business related, and therefore allowable. If it determined not to be an allowable SCAN call, the caller will reimburse the college.
- **259.30.05** DIS provides a SCAN authorization code audit every six months, listing all SCAN authorization codes that have had no usage within that six month period. These reports are reviewed by the responsible system administrator, and SCAN Authorizations Codes for individuals no longer with Seattle Community Colleges are deleted. If appropriate, the report is also forwarded to the department administrators, who are asked to identify any other SCAN codes that can be

deleted. The administrator reviewing this audit must provide appropriate protection for the data being analyzed, as it is extraordinarily sensitive.

#### **259.40 Privacy and Access:**

- **259.40.01** District EIR's are not generally provided for sending or receiving confidential messages. EIR systems may not be secure from unauthorized access, and the District cannot guarantee that messages are private or secure. The District will, however, make reasonable efforts to maintain the confidentiality of communications. 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. Electronic messages ordinarily will be backed up and retained under retention schedules approved by the appropriate records committee in accordance with state law. Users should assume that all electronic messages may be stored for a period of at least six months on disk or tape.
- **259.40.02** Users shall respect the privacy of others in accordance with PRO 259.20.06. Users should assume, however, that their own files, records, messages or passwords may be seen by others, in accordance with PRO 259.30.02 and PRO 259.30.03, or when recipients or others choose to forward or disclose items that have been sent.
- **259.40.03** Files, records, messages, and passwords also may be disclosed when required by law. Electronic messages created or placed on the District's EIRs may be considered writings, and all writings are public records subject to disclosure to any requester in accordance with **Washington'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.

*Adopted: December 1, 1998 : Presented to Board of Trustees as an Information Item 12/01/98*

*Amended: November 1999; November 2005*

[RETURN TO TOP](#) | [CLOSE WINDOW](#)