CCS Administrative Procedure
7.30.05-A Acceptable Use of Information Technology Resources

Implementing Board Policy 7.30.05
Contact: District Director of Information Systems, 533-8018

1.0 Purpose

This procedure establishes guidelines for the acceptable use of the Information Technology Resources (IT Resources) of Community Colleges of Spokane (CCS).

2.0 Limitations and Requirements

CCS IT Resources are provided to support the instructional, support and administrative activities of the district. IT Resources are intended for the sole use of faculty, staff, students and other authorized users. IT Resource use will comply with CCS policies and procedures and state and federal laws. Use of IT Resources does not confer a right to privacy in those resources. CCS reserves the right to monitor IT Resources and take appropriate action to protect the integrity of the IT Resources in accordance with laws, policies and procedures.

3.0 Acceptable and Prohibited Uses of IT Resources

3.1 IT Resources owned or held by CCS and defined in Board Policy 7.30.05, are state property provided to enhance instructional, support and administrative activities. IT Resources will be used only for legitimate student, instructional and support activities and administrative functions. IT Resources use will be consistent with state Ethics in Public Service laws and policies and procedures of CCS, its institutions and departments. IT Resources are to be used in accordance with Community and Technical College Network Acceptable Use Policy as well as the K20 Network Conditions of Use and Acceptable Use Policies.

3.2 CCS supports the principles of intellectual freedom. CCS IT Resources are provided to support and foster the CCS mission. CCS reserves the right to discontinue user's access if the use violates state or federal law or the policies or procedures of CCS, its institutions or departments.

3.3 Network and application logon 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. The user is responsible for all known usage of his/her assigned account.

3.4 CCS IT Resource users will not conceal or falsify their identity when using CCS IT Resources.

3.5 CCS IT Resources may not be used to violate or circumvent U.S. Copyright laws.

3.6 CCS IT Resources shall not be used for commercial, illegal or political purposes. Examples of commercial use include, but are not limited to, advertising, selling or buying for personal gain or benefit. Examples of illegal activity include, but are not limited to, accessing or creating obscene material or material likely to contribute to a hostile environment. Examples of political use include, but are not limited to, opposing or supporting political candidates, issues or ballot measures.

3.7 The following types of activities are examples of CCS IT Resources use that are unethical and unacceptable and in some cases may violate state or federal law.

3.7.1 Accessing another individual's account, private files, or e-mail without permission of the account user.

3.7.2 Misrepresenting one's identity in electronic communication.

3.7.3 Violating copyright and/or software agreements.

3.7.4 Violating rules or codes set by services subscribed to by CCS.

3.7.5 Using computing resources to threaten or harass others.

3.7.6 Using the CCS IT Resources for non-college work, including but not limited to commercial or profit-making purposes without written authorization from the administration.

3.7.7 Activities that are not CCS mission related that unnecessarily use network bandwidth or storage, including but not limited to audio or video broadcasts and the downloading or sharing of data, music or videos.

3.7.8 Faculty and staff use of e-mail, the Internet or telephone for personal purposes beyond de minimus use.

3.7.9 Lobbying or engaging in political activity.

3.7.10 Violating lab and network system procedures and protocols (e.g. limits on workstation usage).

3.7.11 Intentionally and without authorization, crashing, accessing, altering, interfering with the operation of, or damaging or destroying all or part of any computer, computer system, computer network, computer software, computer program, or computer database of CCS or others.

3.7.12 Installing unauthorized network services (e.g. web servers, FTP servers, Telnet server,)

3.7.13 Tampering with systems or files in an attempt to hide activities.

3.7.14 Attempting to circumvent, bypass or compromise security of CCs or others.

3.7.15 Intentionally using or installing hacker tools, viruses or system misconfigurations (e.g. Trojan horses, backdoors, viruses or exploit programs) to any CCS IT Resource.

3.7.16 Intentionally or knowingly and without authorization, giving or publishing a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network or database.

3.7.17 Intentionally and with intent to defraud, accessing protected IT Resources without authorization, or exceeding authorized access and by means of such access further fraud and obtains anything of value.

3.7.18 Downloading unsupported programs which impair the security and integrity of IT Resources.

3.7.19 Discriminating or harassing on the basis of race, creed, color, age, sex or gender, religion, disability, or sexual orientation.

4.0 Monitoring and Implementation

4.1 CCS reserves the right to monitor use of IT Resources in accordance with its policies and procedures. CCS does not guarantee that messages are private or secure, although CCS will make reasonable efforts to maintain the confidentiality of communications. Files, records, messages, and passwords will be disclosed when required by law. Electronic messages created or placed on CCS IT Resources are considered public records subject to disclosure. Use of CCS IT Resources for electronic messages is subject to the state ethics law.

4.2 CCS will implement hardware and software technologies that monitor, prioritize, shape and/or control network bandwidth. Such tools will be used to ensure that IT Resources are used effectively and efficiently to support the mission, policies and procedures of CCS.

5.0 Violations

Violation of the policies and procedures of CCS or its institutions could result in loss of access to IT Resources. Student violation is subject to disciplinary action under the Code of Student Conduct. Violation by employees is subject to the appropriate discipline process up to and including dismissal, consistent with the provisions of the respective collective bargaining agreement or disciplines under WAC.

6.0 Related Information

6.1 Board Policy 7.50.20 - US Copyright Laws, Use of Copyrighted Materials

6.2 Chapter 42.52 RCW - Ethics in Public Services

6.3 Chapter 42.56 RCW - Washington Public Records Act

6.4 42.17.190 RCW - Disclosure Campaign finances lobbying

6.5 Title 292 - Agency Substantive Rules, Use of State Resources

6.6 Title 357- Personnel Department of Personnel Resources Board-Discipline

6.7 Acceptable Use Policy - K20 Network Conditions of Use

Originated: January 2006
Cabinet approval: January 2006