BP 2720 COMPUTER AND NETWORK USE

References:

Education Code Section 72400
Penal Code 502
17 U.S. Code Sections 101, et seq.

It shall be the policy of Riverside Community College District Board of Trustees to require that employees, faculty and students agree to and adhere to the applicable District Computing and Internet Policy. Employees and students who use District computers and networks and the information they contain, and related resources have a responsibility not to abuse those resources and to respect the rights of others.

The Chancellor shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. These procedures shall also be in accordance with the CTA Collecting Bargaining Agreement.

The District will supply, as specified in the procedures its employees with computers and other electronic devices to assist in the fulfillment of their responsibilities. It is understood that these computers and electronic devices are District property and are to be used for job related duties. The District will respect the privacy of email, voice-mail and computers designated for employees' use and will not monitor the use of District-owned computers, email, voice-mail, Internet or WWW connections without substantial justification.

Date Adopted: May 19, 2009
(Replaces RCCD Policy 3060)
Formerly: 3720

AP 2720 COMPUTER AND NETWORK USE

References:

Government Code Section 3543.1(b);
Penal Code Section 502;
17 U.S.C. Sections 101 et seq.;
Cal. Const., Art. 1 Section 1;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, and 45

The District Computer and Network systems are the sole property of the District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

I. General Principles

A. Information technology plays an increasingly important role in higher education. This procedure is intended to support that role while providing necessary security for the District's information resources, employees, students and community. All users of District information resources are expected to be familiar with this procedure.

B. Access to and use of the District network infrastructure, software, hardware, data and communications networks, attached devices, installed software, cloud storage resources (non-RCCD web storage sources), e-mail, Internet, Extranet, and Intranet (hereafter referred to as information resources) is provided to staff, and faculty as a necessary part of their assignment**.** The access and use granted to students, and approved others, is a privilege, not a right. The lawful purposes for the access and use, include, but are not limited to:

1. teaching
2. research
3. administrative and District business purposes
4. expanding communication among colleagues, students and the community.
5. Counseling Support

C. All information resources, whether individually controlled or shared, stand-alone or networked**,** are owned by RCCD and are government

property. Use is subject to all constitutional and statutory controls and prohibitions pertaining to governmental conduct. RCCD is the owner of all data on RCCD Internet, Extranet, and Intranet pages, subject to the intellectual property rights of faculty, staff, and students.

Computer transmissions and electronically stored information on any District computer, or District-owned mobile devices, such as, but not limited to, cell phones, Blackberry's and PDA's, may be discoverable in litigation. If necessary, legal counsel will be sought with regard to accessing information. (See also III.C. below.)

D. Conditions of Use: Individual departments within the District may define additional conditions of use for information resources under their control. These statements must be consistent with this overall procedure, but may provide additional detail, guidelines and/or restrictions.

E. The District recognizes the value of academic freedom and extends it to faculty use of the information resources for purposes related to teaching and research.

F. Labs, schools and other District entities may provide procedures and/or guidelines for student use of RCCD computers as it relates to their respective missions.

G. All existing local, state, federal and international laws and RCCD regulations and policies apply, including not only those laws and regulations that are specific to information resources, but also those that may apply generally to personal conduct, including the Electronic Communications Privacy Act of 1986, the Family Educational Rights and Privacy Act (FERPA) of 1974, and the Digital Millennium Copyright Act of 1998.

H. Reproduction and/or distribution of copyrighted works, including but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties, including fines and imprisonment. Intentional violations of copyright law are federal crimes. Users should consider the following:

1. There may be individual liability for monetary damages for violation of copyright or breach of a license agreement.
2. Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc. is forbidden by law.
3. Violating terms of applicable software licensing agreements or copyright laws is illegal.

a. Prohibited uses of copyrighted software include making copies for gift or sale, copying a computer program purchased for use at the District for personal use, or copying a computer program purchased for use in one department or school for use in another department or school.
b. Permissible uses of copyrighted software owned by or licensed to the District or its faculty include copying it by using it in a computer's memory, making a backup or archival copy, making adaptations in order to use a particular machine.
c. Software used on District owned computers must be legally purchased and/or licensed and a record of this must be maintained. A site license should be negotiated to allow multiple uses on campus whenever possible. The distribution of software must be handled in such a way that the number of installations does not exceed the number of licenses purchased, unless otherwise stipulated in the purchase contract.
d. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

I. The content of all Internet, Extranet and Intranet pages will be consistent with District image and policies. The requirements of law for accessibility of the disabled to public services and facilities apply to the District's computer resources and networks pursuant to the definition of "access" in Section 508 of the Rehabilitation Act of 1973.

II. Network Computing Safeguards

A. All users of the District network information resources are hereby informed of privacy limitations on e-mail and electronic transmissions. The District will maintain reasonable security measures for District databases stored in networked systems, including those of faculty, but users of these systems must be aware that limitations exist to security:

1. Users cannot assume absolute confidentiality or anonymity of information on any computer.
2. Each computer user is responsible for all matters pertaining to the proper use of his/her computer or network access account including choosing passwords, ensuring that file protections are set correctly, and taking appropriate action to maintain secure backup files.
3. Individuals should consider the demand that their use has on available information resources, particularly during peak access times (between 10 am and 2:00 pm on weekdays and the first week of classes of the fall and spring terms). Those using the Internet

are asked to be considerate of others who may wish to access and use these resources.

4. E-mail and data stored on District systems are subject to disclosure under the Public Records Act, and when relevant, to discovery in civil or criminal litigation.

B. The District is not responsible for the content of e-mail that passes through the District E-mail Systems or Services. Views and opinions expressed may not be representative of the views and values of the District. The District is not responsible for financial obligations resulting from the unauthorized use of the system.

III. Network Administrator's Powers to Protect the System

A. The computers operated by District administrative systems contain academic, financial, and personal data that is sensitive and confidential. Access to the administrative system is limited solely to authorized District employees and contract personnel whose jobs require them to record, review, or retrieve this data, or who are involved with system development or operation, and who receive prior clearance from the appropriate District administrative systems department. This authorized use is a trust; misuse or unauthorized access to the system will not be tolerated. Use of the network computing access may not be monitored by the authorizing entity, to ensure network integrity, without substantial justification.

B. To protect the information resources from viruses, hackers and other external attacks, the District network administrators may access user files to suspend or remove content on computers as required to protect the integrity of computer systems, or to examine accounts that are suspected of unauthorized use, misuse, or have been corrupted or damaged. In such instances the affected employee(s) and their supervisor(s) will be notified and asked to be present during the review whenever possible. Every effort to respect the confidentiality of the individual's files will be made.

The District will respect the privacy of email, voice mail and computers designated for all employees' use and will not monitor their use of District-owned computers, email, voice-mail, Internet or WWW connections without substantial justification.

C. The Chancellor or his designee may authorize RCCD personnel to access user files for business, litigation (under the Federal Rules of Civil Procedure for securing of electronic data in Federal litigation cases), or security related reasons when there is substantial need or justification.

D. It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.

E. Undeliverable e-mail will be directed to the system administrators for purposes of assuring reliable e-mail service.

F. Use of the RCCD computer facilities by outside individuals or organizations requires permission from the local system administrator. If necessary, the system administrator should inform the campus network administrator.

G. Any defects discovered in system accounting or system security must be reported promptly to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

H. On-line counseling will be afforded the same rights and protections as face-to-face counseling, with regard to confidentiality.

IV. Forbidden Activities

A. The following activities are expressly forbidden and will be treated as a cause for discipline and/or legal prosecution:

1. Any activity that violates local, state, federal, or international laws;
2. Seeking to gain unauthorized access to any computer or computer user's account not assigned to them;
3. Forging the identity of a user or machine in an electronic communication or using another individual's user account for any purpose without his/her specific approval;
4. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's e-mail, files or software without the explicit agreement of the assigned user;
5. Any unauthorized attempts to circumvent data protection schemes or uncover security loopholes, including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data or to use any RCCD computer system by means of unauthorized dial-up access;
6. Accessing or causing access to the system to devise or execute any scheme to falsely alter, add, delete, damage, or destroy data contained therein;
7. Transmitting materials that are slanderous or defamatory in nature or that otherwise violate existing laws or District regulations;
8. Using e-mail to harass or threaten others or e-mail that violates existing District harassment policies;

9. Initiating or propagating electronic chain letters;
10. Viewing, storing, or transferring information which contains pornographic material not specifically related to course work and teaching;
11. Knowingly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network, including but not limited to, programs known as computer viruses, Trojan Horses, and worms;
12. Using District resources for commercial activity such as conducting a personal business enterprise, creating products or services for sale, developing programs, data processing or computations for commercial use, and preparation and presentation of advertising material;
13. Disruptive or inconsiderate conduct described in District Board Policies or Administrative Procedures for computer labs or terminal areas;
14. Connecting unauthorized equipment to computing resources without prior approval by the systems administrator (Information Services must approve all networking devices, including but not limited to, servers, routers, switches, hubs, printers and wireless devices);
15. Internet, Extranet, and Intranet activities that violate the policies of RCCD including the inappropriate use of District resources or the District name or reputation.
16. A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system administrator.
17. Users must not release individual's (student, faculty or staff) personal information to anyone without proper authorization.
18. District information resources must not be used for partisan political activities where prohibited by state, federal, or other applicable laws.
19. District information resources should not be used for commercial purposes. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within those domains.
20. All users have the right to be free from any conduct connected with the use of the District's network and information resources which discriminates against any person on the basis of the categories listed in Board Policy/Administrative Procedure 6410, titled Nondiscrimination. No user shall use the District network or information resources to transmit any message, create any communication of any kind, or store information which violates any

District Policy or Administrative Procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

21. When Virtual Private Network (VPN) access has been given to any user to access RCCD's information resources from off-campus, it is the user's responsibility to prevent unauthorized users from obtaining access to their computer (laptop or PC).

V. Penalties for Abuse

A. Users will be held accountable for their conduct under applicable RCCD policies, procedures, and/or collective bargaining agreements. Violation of any local, state, federal or international laws relating to information resource use can lead to the suspension of network account(s), and discipline ranging from disciplinary suspension to dismissal from District employment, suspension or expulsion from enrollment, and/or civil or criminal prosecution.

B. Individuals with knowledge of a violation of this policy should report the violation to their supervisor, or in the case of a student, to any RCCD employee.

Definitions As They Apply to the Computing and Internet Policy

Access: For purposes of this policy: to instruct, program, communicate with, store data in, or retrieve data from the computing resources.

District E-mail Systems or Services: District e-mail services include messaging systems that depend on District owned servers and computing facilities to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print computer records that facilitate communication across computer network systems between or among individuals or groups, that is either explicitly denoted as a system for e-mail or is implicitly used for such purposes. For purposes of this document it also includes services such as electronic bulletin boards, list servers, and newsgroups.

Extranet: The RCCD Extranet is a computer network operated by RCCD to provide its students, faculty, staff, administration, and selected others with learning opportunities, research information, and other resources through restricted (password) access from off-campus or on-campus computers of any type. (Technically, the Extranet can also be defined as one or more largely platform-independent enterprise zones with web-based and other resources that serve selected members of the organization and Internet community by means of restricted access [where the enterprise and organization is RCCD].)

Intellectual Property Rights: Intellectual property includes property that derives from the work of the mind or intellect including an idea, invention, trade secret, process, program,

data, formula, patent, copyright, or trademark or application, right, or registration relating thereto.

Internet: The Internet is the global collective of computer networks, available to millions of users world wide. Official RCCD pages on the Internet are prepared and/or approved and maintained by RCCD employees. Audiences for RCCD Internet pages include, but are not limited to prospective and current students and their families, professional colleagues, government leaders, the media, historians, other educational institutions and the community at large.

Intranet: The Intranet is the campus collective of computer networks, available to RCCD campus students, faculty, staff, and administration. (Technically, the Intranet can also be defined as one or more platform-independent enterprise zones with largely web-based resources that serve only the internal members of an organization [where the enterprise and organization is RCCD].)

Network: The network consists of the cables, servers, routers, switches, etc., which are used to connect campus computers to each other and to external Internet and other computer-related connections.

Receipt of E-mail: Receipt of E-mail before actual viewing is excluded from this definition of "use" to the extent that the recipient does not have advance knowledge of the contents of the e-mail record. E-mail users are not responsible for e-mail in their possession when they have no knowledge of its existence or contents.

Dissemination and User Acknowledgment:

All users shall be provided copies of this Administrative Procedure and be directed to familiarize themselves with it.

Users shall sign and date an acknowledgement stating that they have read and understand this Administrative Procedure, and will comply with the standards set. A sample of the acknowledgement is below:

/ / / / /

/ / / / /

/ / / / /

/ / / / /

/ / / / /

/ / / / /

Computer and Network Use Agreement

I have received and read a copy of Administrative Procedure 2720, titled Computer and Network Use, and understand the contents of this document. I agree to abide by the standards set in the Procedures for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Network Usage Administrative Procedure may subject me to disciplinary action, including, but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.

Dated:_____ _____

(signature above the line, print name below the line)

Office of Primary Responsibility*:* Vice Chancellor, Business and Financial Services
Associate Vice Chancellor, Information Services

Administrative Approval: June 1, 2009
(Replaces RCCD Regulations 3060/4060/6060)
Revised: April 2014 (job titles only)
Formerly: 3720