Rogue Community College

AP 3720 Computer and Network Use

References:

17 U.S. Code Sections 101 et seq.;
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45;
NWCCU 2020 Standard 2.I.1;
ORS 341.290(4);
RCC College Policy – AP-037;
ORS 192.410 – 192.505 Oregon Public Records Law;
ORS 646A.600 – 646A.628 Oregon Consumer Identity Theft Protection Act;
ORS 646A.622 Requirement to Develop Safeguards for Personal Information;
ORS 646A.624 – Powers of Directors, Penalties;
Homeland Security Act;
FERPA (Family Educational Rights and Privacy Act);
ACCJC Guide to Evaluating Distance Education and Correspondence Education

The Chief Information Officer directs that the following regulations and procedures apply to all Rogue Community College students, faculty, staff, administrators, consultants, authorized guests and to any other persons granted use of College information resources. This group can be generally referenced as "users". The College is responsible for making sure these procedures and policies are readily accessible to all users prior to their use of the College Network. These regulations and procedures refer to all College Network resources whether individually controlled or shared, stand-alone or networked. It applies to all online communication systems, computer and computer communication facilities owned, leased, operated, or contracted by the College. This includes, but is not limited to, personal computers, laptops, workstations, tablets, servers, network devices, mobile devices, and associated peripherals, printers, fax machines, software and information resources, regardless of whether used for administration, research, teaching or other purposes. Hereinafter, this system and all of its components shall be referred to as the "College Network."

I. **Legal Parameters.** Abuse of computing, networking, or information resources contained in or part of the College Network may result in the loss of access to the College Network. Additionally, abuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable College policies, procedures, State and Federal laws, or collective bargaining agreements. Complaints alleging abuse of the College Network will be directed to those responsible for taking appropriate disciplinary action. Illegal reproduction of material protected by U.S. Copyright Law is subject to civil damages and criminal penalties, including fines and imprisonment.

A. **Property.** The College Network systems are the sole property of the Rogue Community College ("College"). They may not be used by any person without the

proper authorization of the College. Except as provided in Board Policy, collective bargaining agreements, or as pursuant to Federal or State law pertaining to intellectual property rights. Employees and students have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the College Network.

B. Regulations. This administrative procedure exists within the framework of College Board Policy and state and federal laws. A user of College Network resources who is found to have violated any of these administrative procedure's regulations will be subject to disciplinary action up to and including, but not limited to, loss of College Network privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

i. **Copyrights and Licenses.** Computer users must respect copyrights and licenses to software and other online information. In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

ii. **Copying.** Software protected by copyright may not be copied or published, except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, from, or by any College facility or system, except pursuant to a valid license or as otherwise permitted by copyright law, as it pertains to "fair use" guidelines.

iii. **Network Usage.** Downloading, uploading, file sharing, copying, or publishing unlicensed or copyrighted movies, music, and "codes" for other than legally authorized uses or uses authorized by the College is prohibited.

iv. **Number of Simultaneous Users.** The number and distribution of software copies must be handled in such a way that the number of simultaneous users in a department/class does not exceed the number of original copies purchased by that functional area unless otherwise stipulated in the purchase contract.

v. **Removal of Equipment.** Computer users must not attempt to and/or remove computer equipment, software, or peripherals without management authorization (expressed or implied), this includes, but is not limited to, College purchased and/or owned personal computers, laptops, tablets, mobile devices, etc.

II. Unauthorized Computer and Network Use

A. Interference with Access. Computer users must not interfere with others' access and use of the College Network. This includes, but is not limited to, excessive email

messages, running and/or installing grossly inefficient programs when efficient alternatives are known by the user to be available; excessive printing of documents, files, data, or programs; unauthorized modification of system facilities, operating systems, or network storage devices; attempting to crash or tie up a College computer or network; and damaging or vandalizing College computing facilities, equipment, software or computer files.

B. Disruptive Programs. Computer users must not intentionally develop or use programs which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not intentionally use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program may result in disciplinary action as provided in this procedure and may further lead to civil or criminal legal proceedings.

C. Abuse of Computing Privileges. Users of College Network resources must not knowingly access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of College computing privileges. Additional examples of behaviors constituting abuse that violate this Board Policy include, but are not limited to, the following activities:

i. Using a computer account that one is not designated or authorized to use.

ii. Obtaining a password for a computer account that one is not authorized to have and/or knowingly or carelessly allowing someone else to use your account.

iii. Using the College Network to gain unauthorized access to any computer systems.

iv. Knowingly performing an act which will interfere with the normal operation of the College network resources.

v. Knowingly running or installing on the College Network, a program intended to take control of the College Network resources, or giving another user, a program intended to damage or to place excessive load on the College Network. This includes, but not limited to, programs known as malware: computer viruses, Trojan horses, zombie software and worms.

vi. Masking the identity of an account or machine or forging email messages.

vii. Attempting to circumvent data protection schemes or uncover or exploit security and/or loopholes.

viii. Deliberately wasting College Network resources by file sharing schemes, participating in email chains, spamming, and/or excessive bandwidth usage such as audio or video streaming.

ix. Attempting and/or accessing, without College authorization to monitor or tamper with another user's electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal under Federal or Oregon State Computer Crime Laws.

x. Using the College Network for gambling purposes.

xi. Use of College Network for political purposes shall be subject to state and federal law and College Board approval where the law is permissive.

D. Unlawful and Prohibited Messages. Users may not use electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or College policy, or which constitute the unauthorized release of confidential information. The sending of chain letters or excessive messages either locally or off campus is also prohibited.

i. **Information Belonging to Others.** Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs or passwords belonging to other users, without the permission of those users.

ii. **Rights of Individuals.** Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization. However, both the nature of electronic communication and the public character of College business make electronic communication less private than many users anticipate, and may be subject to public disclosure.

iii. **Political, Personal, and Commercial Use.** The College is a non-profit, tax-exempt organization and, as such, is subject to specific federal, state, and local laws regarding sources of income, political activities, use of property and similar matters.

iv. **Political Use.** College information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

v. **Commercial Usage.** College electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or

promotions. Commercial use means for financial remuneration or designed to lead to financial remuneration.

E. Prohibited Activities

i. **Personal Use.** College Network resources should not be used for activities not related to appropriate College functions. Although personal use is not an intended use, the College recognizes that the network will be used for incidental personal activities provided that such use is within reason and provided that such usage is ordinarily on an employee's own time, is occasional at most, and does not interfere with or burden the College's operation, and not otherwise contrary to College policies, procedures, or law.

ii. **Commercial Use.** College information resources are not to be used for any commercial purposes. Users are reminded that the College's license for the ".edu" domain on the Internet prohibits commercial use, and users may not conduct commercial activities with those domains.

iii. **Harassment.** Using College Network resources to harass others is explicitly prohibited and can be subject to legal ramifications. Examples of such activity include, but are not limited to, the use of the College Network to:

1. Threaten others via telephone, email, voicemail, or text.
2. Publish defamatory information about another person.
3. Knowingly downloading, displaying or transmitting communications, images, drawings, depictions that contain sexually explicit materials, ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability, religious or political belief as it pertains to College discrimination and harassment policies, as well as State and Federal regulations.

III. College Users Rights and Responsibilities. This procedure applies to all members of the Rogue Community College community utilizing the College Network. The procedure covers the use of all College software, technology systems, computer equipment, and communications systems throughout RCC. If any provision of this procedure is found to be legally invalid it shall not affect the other provisions of the procedure.

A. Ownership Rights. This procedure is based upon and shall be interpreted according to the following fundamental principle: the entire College Network, and all hardware and software components with it, is the sole property of the College which sets the terms and conditions of its use consistent with the law. Except as provided in Board Policy or collective bargaining agreements pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to

the information they contain by virtue of their use of all or any portion of the College Network.

B. College Rights. System administrators may access user files or suspend services they manage without notice only during one or more of the following occurrences:

i. To protect the integrity and/or security of the College Network resources

ii. Under time-dependent, critical operational circumstances

iii. As required by and consistent with the law or College policy

iv. Where evidence exists that violations of the law or College policy or procedures have occurred. For example: System administrators following organizational guidelines may access or examine individual files or accounts based on evidence that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases, without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or College policy and/or to protect system integrity. This may or may not include personal electronic storage owned by or under control of individuals, including cloud storage.

C. User Rights. While the College monitors electronic usage as part of its normal network operating procedures, the College does not routinely inspect or monitor users' computer hardware or files, email, instant messaging, and/or voicemail message system, nor disclose information created or stored in such media without the user's consent. The College shall attempt to notify users before accessing computer hardware and files or prior to suspending service. In the event that the College acts without consent, it shall notify the user as soon as possible of its access and provide the reason for its action.

D. User Responsibilities. The College recognizes that computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users; respect the integrity of the systems and related physical resources, and observe all relevant law, regulations and contractual obligations.

The interaction of a user's personal computing equipment connected to the College Network, is subject to the procedures in this document. Contents of a user's personal computing equipment are subject to search by the College only by reasonable means.

For College employees, the intended uses of the College Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional activities.

"Unauthorized uses" include prohibited uses and any other use for a prohibited purpose, including illegal activities, messages which may constitute discrimination or harassment under state or federal law or anything that interferes with the intended use. These types of prohibited uses and purposes are further defined herein and within the College Acceptable Computer Use Guidelines.

IV. Disclosure

A. Privacy Interests. The College recognizes the privacy interests of its employees and students and their rights to freedom of speech, shared governance, and academic freedom, as well as their right to engage in protected union and concerted activity. The College reserves the right to monitor all use of the College Network and resources to assure compliance with these policies. The College will exercise this right only for legitimate College purposes; including but not limited to court-ordered discovery proceedings, freedom of information act disclosures, and ensuring compliance with this procedure and the integrity and security of the system, etc. The College seeks to afford email communications privacy protections comparable to those it traditionally affords paper mail and fax communications, consistent with State and Federal statutes.

B. Possibility of Disclosure. Users must be aware of the possibility of unintended disclosure of communications. The College Network can be subject to authorized and unauthorized access by both internal and external users. There are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the College Network is not to be relied upon as completely confidential and private.

C. Retrieval. 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.

D. Public Records. The Oregon Public Records Law (ORS 192.410 – 192.505) includes computer transmissions in the definition of "public record" and nonexempt communications made on the College network and computers must be disclosed if requested by a member of the public.

E. Litigation. Computer transmissions and electronically stored information may be discoverable in litigation.

F. Dissemination and User Acknowledgement. All users of the College Network must comply with Board Policy, as well as this Administrative Procedure 3720, and

any additional policies or guidelines established by the College. Such policies or guidelines will be reviewed by the College and may become subject to Board approval as a College policy or procedure. All users shall be provided copies of these regulations, policies, procedures, and guidelines; be directed to familiarize themselves with them, and agree to terms of usage. By using any part of the College Network, users agree that they will comply with the policy and procedures.

i. **Procedure.** A process addressing these procedures shall be installed. The process shall appear prior to accessing the secured system. Users shall acknowledge after reading the associated policy (AP-3721) and will comply with it and its associated regulations. This acknowledgment shall be in the form as follows:

ii. **RCC Information Technology – Acceptable Use Policy.** At each workstation login users receive and must acknowledge the ***RCC Information Technology – Acceptable Use Policy*** **(AP-3721)** adopted XX/XX/XXXX.

The user must read and then click "Okay", thus recognizing that they understand the guidelines. The user thus agrees to abide by the standards set in the Policy for the duration of my employment and/or enrollment. The user is aware that violations of this Policy may subject me to disciplinary action, including but not limited to revocation of their network account up to and including prosecution for violation of State and/or Federal law. A user choosing to "lock" their workstation rather than logging off and back on is not held harmless from AP-3721 and any changes made to the policy between logins.

Rescinds Procedure Number: None

Approved: April 7, 2020

Revised: December 6, 2022