Procedure: **INFORMATION TECHNOLOGY–ACCEPTABLE USE (AP-037)**
Contact: Chief Information Officer, College Services, Ext. 7238

Rogue Community College ("RCC", "the College") provides numerous information technology resources (IT resources) to support its educational mission. IT resources includes, but is not limited to, all College electronic hardware, software and associated data that support the following: administrative information systems, desktop computing, library automation, multimedia, data, video and voice networks, e-mail, Internet access, scanners, telephone systems, voice mail, copy machines, fax machines, electronic publications including video, websites, or any other similar electronic based functionality.

The use of these resources must be consistent with the goals of the College. Employees and students are encouraged to utilize these resources in support of the College mission. The use of these systems is a privilege and all users are expected to act responsibly and to follow the College's guidelines, policies and procedures in utilizing information technology and electronic networks accessed by such technology, as well as applicable Federal and State laws and regulations. The College's Information Technology Acceptable Use Procedure ("Procedure") requires that anyone using these resources:

1. **Accept responsibility for learning how to use information technology.** The College provides education on the use of information technology. All users are encouraged to learn the proper use of information technology by individual learning, attending training sessions or attending classes. Access to certain IT resources may be limited to those demonstrating an appropriate skill level. Each user is responsible for checking any software they introduce to any computer or the College network for computer viruses. If a user introduces a virus because they did not follow standard checking procedures, their access to information technology resources may be restricted or suspended.

   Users who believe virus, spyware, or other such issues have been introduced to College systems shall notify IT as soon as possible.

2. **Accept responsibility for backup and security of your own work.** The College regularly backs up many IT resources. However, the contents of local hard drives, thumb drives, and other such storage media are not backed up by the College. Each user is responsible for the backup and/or archive of their information stored on such devices and/or media.

3. **Use resources efficiently and respectfully.** Users must accept limitations or restrictions on computing resources, such as storage space, time limits or amount of resources consumed when so instructed by the College. Each e-mail user is responsible for managing their message storage. Such restrictions are designed to ensure fair access for all users. Any attempt to evade, change, or exceed resource quotas or disk usage quotas is prohibited.

   Degrading, disrupting, or vandalizing the College's equipment, software, materials, or data, or those of any other user of the system is prohibited.

   Loading or installing any programs, personal files, personal data, or software on any computer or network must receive prior authorization of IT management. IT management will maintain a list of allowable software. Technical support will not be provided for any privately owned software.

Attaching any unauthorized equipment to the College's networks is prohibited. Persons may use their own privately owned equipment to attach to the wireless network, but must adhere to all RCC policies and procedures regarding computer use. Connection of any privately owned equipment to any portion of the College's networks must receive prior authorization of IT management. IT management will maintain a list of allowable equipment. Technical support will not be provided for any privately owned equipment. RCC is not responsible for privately owned equipment or its damage when attached to any portion of the College's networks.

4. **Abide by all security provisions.** Distributing or making your password or another person's password or access code available to unauthorized persons or otherwise attempting to evade, disable or "crack" passwords or other security provisions or assisting others in doing so threatens the work, privacy and well-being of others and is prohibited. Users may not supply false or misleading data, or improperly obtain another's password in order to gain access to computers or network systems, data, or information. Obtaining access to an account name or password through the negligence or naiveté of another is a specifically prohibited use.

   Using IT resources to obtain unauthorized access to records, data, and other forms of information owned, used, possessed by, or pertaining to the College or individuals is prohibited.

   Users who believe their password or other security has been breached shall notify IT as soon as possible.

5. **Respect software copyright laws.** Software licensed by the College must only be used in accordance with the applicable license agreement(s).

6. **Respect proprietary information of others.** A user may, subject to College policies and authorization, upload software files or otherwise distribute to on-line networks only information, software, photographs, videos, graphics, music, sounds and other material (collectively "content") not subject to any copyright, trademark, trade secrets, or other proprietary rights of others, or content in which the author has given express written authorization for on-line distribution. Any copyrighted content submitted, used, copied or distributed with the consent of the copyright owner should contain a phrase such as "Copyright owned by [name of owner]; used by permission." Unauthorized transmission of copyrighted or other proprietary content is prohibited.

7. **Respect the rights of others to have freedom from harassment or intimidation.** Sending abusive or unwanted material is a violation of College policies, may violate the law, and is prohibited. Targeting another person, group or organization to cause distress, embarrassment, injury, unwanted attention or other substantial discomfort is harassment, which is prohibited. Personal attacks or other actions that threaten, intimidate or embarrass an individual, group or organization, or attacks based on a person's race, national origin, ethnicity, handicap, religion, gender, veteran status, sexual orientation, or other such characteristic or affiliation are prohibited. RCC will be the arbiter of what constitutes proper conduct. Issues concerning harassment should be brought to the attention of the RCC Human Rights Network.

8. **Identify yourself clearly and accurately in electronic communication.** Anonymous or pseudo-anonymous communications do not dissociate any user from responsibility for their actions. Communication under a false name or designation or a name or designation which the user is not authorized to use, including instances in conjunction with representing that the user is somehow acting on behalf of or under the auspices of RCC is prohibited.

9. **Present a proper image for the College.** Information that is published electronically using World Wide Web, kiosks, bulletin board systems, or similar electronic applications for broad general consumption outside of the College will be used to promote the College and as an educational tool. As such, they shall be subject to the same standards as conventional publications with respect to the representation of the College.

10. **Recognize limitations to privacy in electronic communications.** Users may have an expectation that the contents of what they write or otherwise create, store, and send be seen only by those to whom they intend or give permission to view; however, the security of electronic information on shared systems and networks is approximately that of paper documents in an unsealed or sealed envelope – generally respected, but breachable by someone determined to do so. All electronic communications, including those marked "private", "personal", or "confidential" are considered College records, and subject to public records laws and subpoenas.

    The College may, at any time, inspect and/or retrieve all data and information stored on any equipment owned and/or operated by the College. Anyone choosing to place information of a personal or confidential nature on College equipment cannot expect that the information will be kept private or confidential. Also note that, as part of their responsibilities, technical staff or other persons may need to view the contents of documents or messages to diagnose or correct problems, or for use in disciplinary or criminal proceedings.

11. **Cooperate as necessary.** When necessary in the College's discretion to maintain continued reasonable services, or in cases of irresponsible use, the College may suspend user privileges and may disallow access to or connection of computers (even personal ones) to the campus network or take or recommend other action deemed necessary or appropriate. All users are expected to cooperate with investigations by resource managers or others at the College, either of technical problems or of possible unauthorized or irresponsible use as defined in this Procedure, College guidelines, other College policies and procedures, or Federal and State laws and regulations.

12. **Observe proper on-line etiquette.** On-line networks shall be used only as permitted by the College, only in accordance with applicable College policies and procedures, and only for lawful purposes. Any conduct that in the College's discretion restricts or inhibits others from using an on-line network or violates College policies or procedures or applicable law is not permitted. Users are prohibited from intentionally receiving, posting on, or transmitting through any on-line network any unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, sexually explicit, pornographic, profane, hateful, racially or ethnically demeaning or threatening, or otherwise objectionable material of any kind, including without limitation, any material which encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law or College policies or procedures.

13. **Refrain from certain kinds of communications.** Transmission of chain letters and pyramid schemes of any kind are prohibited.

    Use of any on-line network to send unsolicited advertising, promotional material, or other forms of solicitation to others is prohibited, except as permitted by law and when not prohibited by College policies or procedures.

    Downloading and/or manipulation of, or the creation, sending, or forwarding of messages or other content which pertain to or act on behalf of organizations not part of the mission of RCC (such as religious, fraternal, political, private, or athletic organizations, etc.) is prohibited.

Personal Use

IT resources are primarily for the educational use of students, and business use of employees in the performance of their College jobs. Limited, occasional, reasonable, or incidental use of IT resources for personal, non-business use is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their educational and business purposes. Students and employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

The College email system is to be used for purposes related to the College mission. Personal email messages should not be sent or received through the College email system.

Use of IT resources for personal, for-profit purposes is not permitted.

All personal use is subject to College policies and procedures, and applicable Federal and State laws and regulations.

Information Content/Third-Party Supplied Information

Opinions, advice, services, and all other information expressed by IT resource users, information providers, service providers, or other third party individuals are those of the providers and not the College.

The College does not warrant that the function or services performed by, or that the information or software contained on, IT resources will meet the IT resource user's requirements or that the IT resources will be uninterrupted, error-free, or that defects can be corrected.

RCC is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and/or inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with offensive content. In addition, having an email address may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk.

Summary

College information technology resources may be used for lawful and permitted purposes only. Non-compliance with any of the provisions of this Procedure may subject the user to sanctions including immediate loss of computing and/or network access, personnel or student disciplinary action up to and including dismissal from employment or expulsion from college in accordance with applicable RCC policies and procedures. In addition, unlawful or unauthorized use may subject the user to personal or criminal liability in certain circumstances.

The College reserves the right to restrict and/or interrupt communications through or by use of any College computers or information technology services, which the College believes to be harmful to the College or to others.

This Procedure applies to information technology and systems outside the College accessed via College facilities.

Issues concerning improper use of IT resources should be brought to the attention of Information Technology management.