Computer Use Policy

Computer and Network Use
The College provides computers, software, peripherals, and network services for use by RSC students, faculty, and staff to support academic and administrative functions. Personal use of these resources for other purposes is permitted when it does not consume a significant amount of these resources (to be determined by the network administrator), does not interfere with the performance of the user’s job or other college responsibilities, and is otherwise in compliance with this policy. These resources may not be used for personal commercial purposes or for personal financial or other gain. Further limits may be imposed upon personal use in accordance with normal supervisory procedures.

User guidelines:

1. Network logons are automatically created for each student upon enrollment. Faculty and staff (part-time or regular) may obtain a network logon upon request of the immediate supervisor. Students, faculty, and staff are responsible for any access code assigned to them, which includes not sharing any network or computer system logons and passwords. An access code includes any form of information used to authenticate, secure, or control electronic information technology resources. Examples include network logon IDs, passwords, keys, and door codes.

2. Copyrighted software must only be used in accordance with its license or purchase agreement and must not be copied or altered except as permitted by law or by the software licensing agreement. ITS staff will install college-approved software on college-owned computers. Upon request, ITS staff will install personal software as long as it is licensed.

3. Inappropriate conduct that will not be tolerated includes, but is not limited to:
   - Unauthorized access, alteration or destruction of another user’s data, programs, electronic mail, or voice mail.
   - Attempts to obtain unauthorized access to either local or remote computer systems or networks.
   - Attempts to circumvent established security procedures or to obtain access privileges to which the user is not entitled.
   - Obscene, offensive, threatening, harassing, or intimidating material entered into the computer and sent by electronic means.
   - Intentional viewing of pictures of an erotic or sexual nature when such images can be viewed by others who are offended by them; and, mailing, printing, or copying obscene materials.
   - Knowingly running, installing, or giving to another a program or data file which could be classified as or contain a computer virus, worm, or Trojan horse.
   - Activities that embarrass, denigrate, or libel an individual or organization.
   - Activities that imply College endorsement of any commercial products other than those approved by the appropriate Executive Council member.