

## **Acceptable Use Policy** (Updated November 15, 2010)

Santa Rosa Junior College strives to provide a computing environment that supports the goals and the mission of the College. Members of the Santa Rosa Junior College computing community are expected to comply with all local, state, and federal laws as well as Santa Rosa Junior College Board Policies and rules in their use of college networks and computer systems associated with SRJC. This document summarizes the main points of acceptable use found in "Policy 2.13P Computer and Communications Technology Use," but users are also expected to familiarize themselves with the full text of SRJC policies. Policies are subject to change as needed and are subject to annual review, and as such, this document may change to reflect any change in policy.

The term "user" applies to anyone using SRJC computing or networking resources. The definition of "college computing and networking resources" includes personal computing equipment as long as it is associated with the College. For example, a student's laptop or smartphone connected to SRJC's wireless network are associated with the College.

1. Individual departments and system administrators may further define rules governing acceptable use of their resources. For example, an academic department may have rules allowing or disallowing recreational Web browsing in their student labs.
2. All use is subject to monitoring by authorized college personnel for the purpose of network/system management or security, with reasonable efforts made to maintain user privacy. Interception of traffic for unauthorized purposes is prohibited.
3. Copyright, obscenity, libel, and other laws governing communication and publication apply to electronic media as well. Users are personally responsible and liable for such infringing activities. For example, you may not pirate software (use software in violation of pertinent software licensing agreements),

or distribute pirated software with College resources. Downloading illegal copies of music, video, or text is prohibited and the owner may sue you for infringement.

4. You may only access files, data, and resources to which you are legitimately entitled. You may not attempt to gain access to systems, accounts, passwords, or data that you have not been authorized to access. For example, you may not 'sniff' the network to gain information such as logins and passwords of other people. You may not distribute 'backdoor' programs to gain access to another person's machine or files.
5. Users are responsible for all activities originating from their accounts or personal systems. No unauthorized sharing or selling of personal access to College resources is allowed. Protect all user ids, passwords, and systems from unauthorized use.
6. Any activity which negatively impacts the operation of the network or systems is prohibited. You may not monopolize or overload resources. Excessive use is use which prevents other people or systems from being able to work. For example, excessive use of network bandwidth while playing network games is prohibited.
7. You may not use electronic resources to harass, intimidate, or annoy people. This includes transmission or printing of violent, threatening, defaming, obscene, or otherwise illegal or harmful material. Electronic chain letters are not allowed, nor is spam. If you receive a piece of e-mail that says to send it on to all of your friends, even if it seems to be a warning about a virus, it is generally a hoax and should not be forwarded.
8. You may not use electronic resources for commercial use or personal gain. For example, you may not run a business using SRJC computing resources, or even register a domain name to a network address in the college address space.
9. All attempts to subvert system or network security measures are strictly prohibited.
10. If you suspect your account has been compromised, or feel you have been violated by others, keep copies of all relevant documents, unplug your computer network connection from the

wall jack (where applicable), and contact the Information Technology Help Desk (call (707) 524-1765) as quickly as possible. You are responsible for reporting all violations. IT will work with appropriate College officials to resolve any reported violations.

11. Violations can result in the loss of computing privileges, initiation of legal action by the College, and/or appropriate disciplinary action.