

A. ADMINISTRATIVE COMPUTING PROCEDURES

1. **PURPOSE** - This document establishes rules and prohibitions that define acceptable use of Santa Rosa Junior College (SRJC) computing systems whose primary users are faculty and staff using the system for College business (i.e. the main computer in Computing Services). Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions under Federal, State, and local law.
2. **AUDIENCE and AGREEMENT** - All users of this system must read, understand, and comply with the policies outlined in this document. **BY USING THIS SYSTEM, USERS AGREE THAT THEY UNDERSTAND, AND WILL COMPLY WITH, THESE POLICIES.**
3. **RIGHTS** - This system is owned and operated by SRJC. SRJC reserves all rights to this system, including termination of service without notice.

Users of this system have rights that may be protected by Federal, State, and local law. Statements required by some acts of law can be found in section 14 of this document: "Disclaimers."

4. The computing facilities at Santa Rosa Junior College are provided for the use of Santa Rosa Junior College students, faculty and staff in support of the programs of the College. All students, faculty and staff are responsible for using these computing facilities in an effective, efficient, ethical, non-discriminatory and lawful manner.
5. Computer facilities and accounts are owned by Santa Rosa Junior College and are to be used for educationally related matters only. (As regards administrative systems, educationally related matters include, for example, assigned work projects, professional contacts, research, and information dissemination about College activities.) Commercial uses are specifically excluded. All access to central computer systems, including the issuing of passwords, must be approved through Computing Services.
6. Any account assigned to an individual by Computing Services must not be used by others without explicit permission from the administrator requesting the account. The individual is responsible for the proper use of the account, including proper password protection.
7. Programs and files are confidential unless they have explicitly been made available to other authorized individuals. The district reserves the right to access all information stored on district computers. File owners will be notified, in advance, if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if violations are discovered, they will be reported immediately to the appropriate supervisor.
8. Electronic communications facilities (such as MAIL) are for College related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.
9. No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any College computer system.

10. Loopholes in computer security systems or knowledge of a special password should not be used to damage computer systems, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.
11. Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.
12. An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate supervisors.

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College, and legal action. Violations of some of the above policies may constitute a criminal offense.

13. The Computer and Telecommunications Review Group will approve/disapprove more detailed guidelines, as needed, for specific computer systems and networks.

These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval and other items related to administering the system.

14. **DISCLAIMERS** - The following are statements regarding this system that are mandated, or may soon be mandated, by federal and state law. In some cases, local policy is also promulgated.

This policy and these procedures shall not be construed as a waiver of any rights of SRJC.

- a. **Electronic Mail Privacy** - Two accounts on this system have the ability to read your mail: your own account, and the system administrator account. While reasonable attempts have been made to ensure the privacy of your electronic mail, this is no guarantee that your electronic mail is private. This is not a secure system, nor is it connected to a secure network.
- b. **Nondiscrimination** - All users have the right to be free from any conduct connected with the use of SRJC computing systems which discriminates against any person on the basis of race, color, national origin, sex, or disability.

Discriminatory conduct includes, but is not limited to, written or graphic conduct that satisfies both the following conditions: (1) harass, denigrates or shows hostility or aversion toward an individual or group based on that person's gender, race, color, national origin or disability, and (2) has the purpose or effect of creating a hostile, intimidating, or offensive educational environment. "Harassing conduct" and "hostile educational environment" are defined below.

"Harassing conduct" includes, but is not limited to, the following: epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts, that relate to race, color, national origin, gender, or disability. This includes acts that purport to be "jokes" or "pranks," but that are hostile or demeaning.

A "hostile educational environment" is established when harassing conduct is sufficiently severe, pervasive or persistent so as to interfere with or limit the ability of an individual to participate in or benefit from the SRJC computing systems.

Any user who believes he or she has been subject to discrimination on the basis of race, color, national origin, gender, or disability may inform the system administrator or the SRJC District Compliance Officer. Upon receiving any such complaint, SRJC shall process the complaint in accordance with the SRJC "Discrimination and Grievance" Procedures.

Any user who files a complaint or otherwise protests against discrimination has the right to be free from any retaliatory action because of the complaint or protest. The SRJC administrator who receives a complaint of discrimination shall inform the complainant of this right and that the complainant may file an additional complaint if he or she experiences retaliatory conduct.

Nothing contained herein shall be construed as violating any person's rights of expression set forth in the Equal Access Act or the First Amendment of the United States Constitution.

B. INSTRUCTIONAL COMPUTING PROCEDURES

1. PURPOSE

Santa Rosa Junior College (SRJC) owns and operates a variety of instructional computing systems which are provided for the use of Santa Rosa Junior College students, faculty, and staff in support of the educational programs of the College and are to be used for such related activities only. Commercial uses are specifically excluded. All students, faculty and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner. This document defines acceptable use of these instructional computing systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as prosecution under Federal, State, and local law.

2. AUDIENCE and AGREEMENT

All users of SRJC instructional computing systems must comply with the policies outlined in this document, as well as any additional guidelines established by the administrators of each system. Such guidelines will be reviewed by the chair/supervisor and, if necessary, the component administrator, and may become subject to Board approval as a District policy or procedure. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES.

3. RIGHTS

SRJC reserves all rights, including termination of service without notice, to the instructional computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of SRJC, nor shall they conflict with applicable acts of Law.

Users of these systems have rights that may be protected by Federal, State, and local law. Statements required by some acts of law can be found in Section 6 of this document: "Disclaimers."

4. PRIVILEGES

Access and privileges on SRJC instructional computing systems are assigned and managed by the administrators of specific individual systems. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

Users may not, under any circumstances, transfer or confer these privileges to other individuals. Any account assigned to an individual shall not be used by others without explicit permission from the systems administrator. The authorized user is responsible for the proper use of the system, including any password protection.

5. RESPONSIBILITIES

Users are responsible for maintaining the following:

- a. An environment in which resources are shared equitably between users;

The system administrator of each system sets minimum guidelines within which users must conduct their activities.

- b. An environment conducive to learning;

A user who harasses, or makes defamatory or derogatory remarks, shall bear full responsibility for his or her actions. Further, by using this system, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that SRJC's role in managing this system is only as an information carrier, and that they will never consider transmission through this system as an endorsement of said transmission by SRJC.

Many of the SRJC instructional computing systems provide access to outside networks both public and private which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that SRJC does not assume responsibility for the contents of any of these outside networks.

The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through SRJC systems.

Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through the SRJC campus-wide information system and through specific individual networks.

The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service).

The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not SRJC, which is acting solely as the information carrier.

- c. An environment free of illegal or malicious acts;

The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized, or any attempt to deprive other authorized users of resources or access to any SRJC computer system shall be regarded as malicious, and may be treated as an illegal act.

- d. A secure environment.

Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.

Users are responsible for proper password maintenance, including periodic changes and safeguarding the password.

Users are responsible for backup of their own data.

6. DISCLAIMERS

The following statements regarding this system are mandated, or may soon be mandated, by federal and state law. In some cases, local procedures are also included.

a. Privacy

1. Electronic Mail

While reasonable attempts have been made to ensure the privacy of user's electronic mail, this is no guarantee that electronic mail is private. The instructional computing systems and/or networks to which they are connected are not necessarily secure.

System administrators will respect user's privacy to the extent possible, and will not examine mail except in the following circumstances:

Investigating an apparent violation of these procedures; Disc capacities are exceeded, and user's mail storage is a contributing factor; Performing any necessary maintenance of the mail system; Forwarding a misdelivered message; Closing an account which contains unread mail.

In the first four circumstances, users affected will be notified that mail was examined by a system administrator.

2. Other forms of data

Programs and files are confidential unless they have been made available explicitly to other authorized individuals. SRJC reserves the right to access all information stored on district computers. File owners will be notified, in advance, if such notice is practical. When performing maintenance, every effort will be made to insure the privacy of user's files. However, if violations are discovered, they will be reported immediately to the appropriate college official(s).

b. Nondiscrimination - All users have the right to be free from any conduct connected with the use of SRJC computing systems which discriminates against any person on the basis of race, color, national origin, sex, or disability.

Discriminatory conduct includes, but is not limited to, written or graphic conduct that satisfies both the following conditions: (1) harass, denigrates or shows hostility or aversion toward an individual or group based on that person's gender, race, color, national origin or disability, and (2) has the purpose or effect of creating a hostile, intimidating, or offensive educational environment. "Harassing conduct" and "hostile educational environment" are defined below.

"Harassing conduct" includes, but is not limited to, the following: epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts, that relate to race, color, national origin, gender, or disability. This includes acts that purport to be "jokes" or "pranks," but that are hostile or demeaning.

A "hostile educational environment" is established when harassing conduct is sufficiently severe, pervasive or persistent so as to interfere with or limit the ability of an individual to participate in or benefit from the SRJC computing systems.

Any user who believes he or she has been subject to discrimination on the basis of race, color, national origin, gender, or disability may inform the system administrator or the SRJC District Compliance Officer. Upon receiving any such complaint, SRJC shall process the complaint in accordance with the SRJC "Discrimination and Grievance" Procedures.

7. COPYRIGHT

Computer software protected by copyright shall not be copied from, into, or by means of SRJC computing facilities, except as permitted by law or by the contract with the owner of the copyright. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users exceeds the number of original copies purchased.

8. VIOLATIONS

Any user's privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate college official(s).

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available including the loss of computer use privileges, dismissal from the College, and legal action. Violations of the procedures above may constitute a criminal offense.

Any user who files a complaint or otherwise protests against discrimination has the right to be free from any retaliatory action because of the complaint or protest. Any user who protests against discriminatory conduct and who is subsequently subject to retaliatory action because of the protests may file an additional or amended complaint with the system administrator or the SRJC District Compliance Officer.

9. ADDITIONAL GUIDELINES

System administrators may develop additional detailed guidelines, as needed, for any of the SRJC instructional computing systems. These guidelines will cover such issues as allowable connect time and disk space, handling of unretrievable mail, responsibility for account approval and other items related to administering the system.

C. DIAL-UP COMPUTING PROCEDURES

Background:

Computing Services maintains two computer systems with dial-up access: Garfield and Nermal. Garfield is the HP3000 which is the campus administrative computer system. Nermal is the host on a microcomputer network. Nermal can be used to send E-Mail and to access the Internet, but cannot be used to access the HP3000 (other than to send mail). Nermal is intended to support instructional use of the Internet and to promote staff development. It is not intended for campus administrative use.

Procedure:

Any regular SRJC employee, with the approval of their supervisor or chair and the Director of Computing Services may be given access to Nermal. Any expenses regarding the use of at-home equipment is the employee's responsibility. The district does not guarantee access to Nermal (downtime, insufficient ports, etc. may cause a person to be unable to connect), but will attempt to make it available, with sufficient dial-in lines, for employee and class related student access.

Adjunct employees will be afforded the same access when it is related to a class they are taking/teaching or if approved in the fashion specified for regular employees. Adjunct employees, when approved, will be approved for a specific length of time.

Credit students currently enrolled in one or more classes at SRJC are eligible for an account on Nermal. Accounts are created by Computing Services. Students who are no longer registered or who are inactive in their account will be deleted.

Dial-up access to the HP3000 will be given only for work related reasons. This access is restricted to regular employees and is subject to the same approval chain as specified above. Such access may be terminated at any time. A classified employee, given such access, must first sign a statement regarding an understanding that access to the computer system is not an implicit approval of overtime - that overtime requires specific approval of the supervisor.

As regards costs, Computing Services will budget for costs relating to the HP3000 and Nermal. Any costs at the employee end must be borne by the employee. District funds, even if available at the department level, are not to be used to upgrade employee owned computers.

Computing Services will maintain laptop computers for loan on work related projects. Users approved for home access may request loan of one of these machines from the Director of Computing Services. These are for short term loan and, due to demand, may not be available when requested.

Remote access to the HP3000 requires the use of a terminal emulator program such as the campus standard - Reflections. Since this software is required to access the HP3000 and would not normally be part of an employee's computer system, SRJC will purchase several copies for checkout. Any other software would be the employee's responsibility. Any exceptions to this policy must be approved, in writing, by the supervisor, dean, vice president and the Director of Computing Services.

Computing Services will not provide software or hardware assistance for home use beyond providing basic instructions on dial-up access.

An employee requesting access should write a brief justification and submit it to their supervisor, dean and, if appropriate, vice president for approval. It is then forwarded to the Director of Computing Services for final approval.

Formerly procedure 2.13