

Employees and students are advised that parameters regarding the specific application of the Privacy and Access Policy may vary from area to area at the College. The procedures offered here should be viewed as significant protections, but they may also be subject to a more permissive interpretation when dictated by local application or to a more rigorous interpretation when the duties of the work group or area require it.

1. OFFICES AND WORK SPACE

Offices and work space assigned to individuals or shared by a small number of individuals shall generally have access limited to custodial, technical, maintenance, safety, or security personnel fulfilling their usual duties. However, local application of this policy may allow greater access (see paragraph below). When a staff member or instructor is ill or inaccessible for an extended period of time, an appropriate supervisor is permitted to access items such as office resources, media material, student papers, or other necessary work. Such entry must have a specific purpose and be reported to occupants in a prompt and reasonable fashion (examples: a written note, e.mail, personal communication, or phone call).

Offices or work spaces in departmental service centers or open administrative areas that sustain complex activities are typically used by several individuals. Locations of this nature should have a specific practice or policy indicating who is allowed access to space and/or materials.

2. DESKS

Desks within an office or work space are typically personal and private space. Where this is not the case, individuals may designate private space such as a drawer to lock or store confidential or personal items. Designated personal space must be labeled in writing, locked, or otherwise identified.

3. LIBRARY MATERIALS

The Santa Rosa Junior College Library shall maintain a written policy regarding materials checked out to individuals.

4. GRAPHICS

Materials sent to Graphics are considered private and may be inspected by Graphic Services' staff only in the performance of their duties. Exams and quizzes receive special confidentiality as provided by present Copy Center procedures.

5. TELEPHONES

Telephone and voice mail service is provided by the District for calls that are related to work or reasonable personal necessity. The contents of telephone calls and voice mail are regarded as private. Voice mail directed to a department or general area shall be treated as non-private. Lists

containing telephone numbers and the actual identities of persons or agencies who have received telephone calls from the District may be subject to routine budgetary inspection. In the interest of budgetary considerations, the supervisor may take note of patterns of calling that appear excessive or unwarranted and query those responsible about the purpose of the calls. A supervisor may, if dissatisfied with the response, extend the inquiry by seeking the identity of the recipients of the calls in lawful and ethical ways.

6. MAIL

Sealed, individually addressed mail is considered private and to be opened by the addressee. Sealed mail directed merely to a titled position, such as "chair" or "program director", should be delivered to the person who fills that position; however, at the direction of this person, access to such mail may be delegated to a surrogate. After a staff member retires or leaves the District employment, all individual addressed mail delivered to the District shall be opened unless an alternative arrangement has been made with the District. (See Policy/Procedures 7.6.1 - Mail Handling.)

Flyers and announcements should be treated as personal mail. However, a high degree of privacy for unsealed material cannot be assured, and the material may be inspected to determine if it meets the District's policy regarding political and commercial material. (See also Procedures 8.5.6 - Distribution of Literature on Campus.)

7. FAX TRANSMISSIONS

General fax transmissions should be treated as personal mail and handled in an appropriate fashion, including placing the material in an envelope at the earliest possible opportunity or routing to appropriate individuals according to local application of this policy. However, a high degree of privacy for FAX materials sent to general or shared offices cannot be assured, since the material may be subject to minimal inspection to determine the appropriate recipient use.

Confidential material received at a FAX location within the District must be labeled as such on the envelope, or otherwise secured in accordance with local application of this policy. Confidential FAX material sent by District staff requires special handling and must include a cover sheet indicating the confidential nature of contents.

8. STUDENT RECORDS

Student records are protected by District policy and state law. (See Policy and Procedures 8.2.9 - Student Educational Rights and Privacy.)

9. PERSONNEL FILES

Access to personnel and other employment records is protected by District policy, negotiated contract, and state law. (See Policy 4.2 - Personnel Files and Confidentiality and contracts between the District and recognized bargaining units.)

10. LOCKERS AND STORAGE AREAS

Lockers and storage areas assigned to a specific individual over a period of time shall be regarded as private except for overriding public interests of health, safety, and law enforcement. Individuals are advised to use locks if there is public access and/or if the materials contained therein are confidential or personal.

Lockers assigned to more than one individual, or that include communally used supplies cannot be assured of maximum privacy. Lockers assigned for a specific work shift, semester, or other designated time period shall be posted or labeled as such. When that time period is over and

materials remain, the contents will be vacated in a manner in keeping with local applications of this policy or posted announcement.

11. PRIVATELY OWNED VEHICLES

Non-District vehicles on campus shall be treated as private and given the same protection as they would have on public streets, allowing entry or visual inspection from without only for purposes of health, safety, or possible criminal violation.

12. CLASSES, CONFERENCES, MEETINGS

These gatherings span the entire continuum that has been delineated. At one extreme, closed sessions of the Board of Trustees or a bargaining unit is accorded maximum privacy and confidentiality. Department and committee meetings may be open only to the members, although greater access may be permitted or mandated by law. Meetings, lectures, and other events intended for the campus community or larger public are granted maximum access.

Conferences and conversations between staff members or between staff members and students or between students shall be regarded as private, although the degree of privacy may be mitigated by the participants' choice of place.

13. CLASSROOM INSTRUCTION

Classroom access is defined by the District's enrollment procedures. Classroom space includes typical examples such as lecture halls, laboratories, playing fields, or studios as well as office areas when allied faculty are meeting professionally with their students. Access for students or the presence of other individuals in a classroom is further defined by various codes of conduct and policy. (See Policy 7.16 - *Children and Visitors in the Classroom* and Policy 8.2 - *Student Rights and Responsibilities*.)

Access by administrators or other staff members is limited to permission from the instructor, class evaluation periods, or to legitimate concerns about health, safety, or legality as mandated by Education Code or other state and federal laws.

Classroom activity is protected by academic freedom. (See *Academic Freedom* article in District/bargaining unit contract.) The information presented in a classroom is not regarded as private or protected, and it is permissible for a student to relate that information to others on a non-commercial basis. However, students may not make an audio or visual recording of classroom activity without first receiving permission from the instructor or obtaining authorization for such recording through appropriate disability code regulations.

14. COMPUTERS AND ELECTRONIC MAIL

It should be noted that the confidentiality of electronic mail cannot be assured. Such confidentiality may be compromised by applicability of law or policy, by unintended redistribution, or by the inadequacy of current technologies to protect against unauthorized access. Users, therefore, should exercise extreme caution in using e.mail to communicate confidential or sensitive matters. (See Policy and Procedures 2.13 - *Computer and Communications Technology Use* for more complete parameters of computer use, privacy, and access.

In addition, users should be aware that occasionally network and computer operations personnel and system administrators might, during the performance of their duties, inadvertently see the contents of e.mail messages. They are not permitted to do so intentionally, or to disclose or otherwise use what they have seen. One exception, however, is that of systems personnel (such as "postmasters") who may need to inspect e.mail when rerouting or disposing of otherwise

undeliverable e.mail. This exception is limited to the least invasive level of inspection required to perform such duties.

15. MECHANICAL AND ELECTRONIC DEVICES

Mechanical and electronic devices for recording sound or activity in a campus area shall be limited to concerns of public safety and are subject to all appropriate statutes and codes governing such devices. Where personal safety or theft risks have been identified, the District reserves the right to utilize motion detectors, intrusion alarms, and other similar security systems.

Nothing in this policy should be construed as limiting the public's right of access to public records under Government Code, Section 6250, nor student rights under Education Code 7600; nor should anything in this policy be construed as prohibiting access to those meetings that are required to be open to the public under the Brown Act.