PROTECTION OF CONFIDENTIAL DATA

1. The District expressly prohibits indiscriminate or unauthorized access to, or disclosure of, personal data or otherwise, from any source regarding employees, retirees, students or applicants.

2. The District is required to collect, use, maintain and disseminate information relating to individuals in accordance with laws and regulations and take the necessary safety measures to protect and maintain this data.

3. Unauthorized access, modification or use of computerized records is prohibited by federal and state law. The Information Practices Act (IPA), the Family Education Rights and Privacy Act (FERPA) and Title 5 regulations that govern the protection of confidential, sensitive, personal employee, retiree, student and applicant data.

Definitions

1. **Personal data** means any information that is maintained by the District that identifies or describes an individual, including, but not limited to, name, social security number, birth date, age, ethnicity, disability, citizenship status, marital status, dependents or household members, gender, home address, telephone number, physical description, education, medical/employment history and/or financial matters. It includes statements made by, or attributed to, the individual. The information may be in electronic form (be it stored in computers or recorded media), written or other printed form, or information obtained orally during the course of , and pertinent to the course of business.

2. **Employees** are defined as managers, faculty, classified staff, student workers, consultants, or volunteers employed by the District and include other persons provided access to District personal, confidential, sensitive data.

3. **Disclosure** means to disclose, release, transfer, disseminate or otherwise communicate all or any part of confidential, private, sensitive, personal data orally, in writing, electronically, or by any other means to any person or entity not authorized to received the information.

4. **Student information** means all student information. Any requests for disclosure of student information should be referred to the Admissions and Records Office of the college.

5. **Third Party** is defined as any person, group or agency not previously authorized by District Human Resources to access such data.

Responsibilities

1. The District shall maintain records of personal data relating to employees, retirees, students or applicants that is relevant and necessary to accomplish the purposes of the District and that is required or authorized by the Governing Board, California Constitution, statute or mandated by the federal government.

2. No employee shall access confidential or private information about any employee, retiree, student or applicant without proper authorization. Employees who have been authorized access to such data must have a legitimate need to have such access as part of their required job responsibilities. Information obtained orally, in writing, by electronic or any other means is subject to this procedure and access shall be strictly limited to business need.

3. All employees with access to personal data shall sign a Confidentiality Agreement as a condition of employment. The signed agreement shall be maintained as part of the employee's personnel file.

4. During new employee orientation, the college Human Resources Office shall ensure that a Confidentiality Agreement is completed by anyone who will have access to confidential information as designated by their supervisor. No employee shall be permitted access to confidential and private data until the Confidentiality Agreement is completed.

5. District Human Resources shall be responsible for maintaining compliance with the provisions of this procedure.

6. Each manager and supervisor shall be responsible for orienting their employees in the areas of responsibility under Board policy, statute, state and/or federal law.

7. Each manager and supervisor shall be responsible for certifying that an employee's access to personal confidential information is needed to perform the assigned duties of that employee.

8. Employees with access to personal confidential data shall not modify or delete the data unless authorized to do so.

9. No employee shall alter or delete their own or their immediate family or domestic partner's personal data.

10. In no case will a person authorized to access data delegate or enable another person's access to the data.

11. In no case will a person authorized to access data disclose confidential data to third parties which enable the third parties to identify the individual employees and their personal confidential data.

12. Careless, accidental or intentional disclosure of information to unauthorized individuals, unauthorized modification or deletion of information or unauthorized access to personal data or violation of any provisions of these statues or guidelines may result in disciplinary action.

13. Unauthorized disclosure may make an employee susceptible to independent civil or criminal actions by third parties.

14. Where provisions of this procedure are in conflict with the Collective Bargaining Agreements reached pursuant to Chapter 12 (commencing with Section 3560) of Division 1 of the Government Code, Higher Education Employer-Employee Relations Act (HEERA), the Collective Bargaining Agreements shall take precedence. However, HEERA shall not be construed to exempt an employee from the provisions of state or federal law protecting confidential and private data.

California Civil Code Section 1798
California Penal Code Sections 484j; 503
Electronic Communications Privacy Act of 1986
(18 USC Section 2510021, 2701-08)
Family Education Rights and Privacy Act of 1974
(20 USC Section 1232g)
Federal Privacy Act of 1974 (5 USC 552a)
Information Practices Act of 1977 (Civil Code Section 1798)
Title 5, Sections 42396, 67100

Historical Annotation:
Personnel 8003.00, 12/89, 11/6/90
Revised 2/5/02
Second Revision 12/7/04

Related Board Policies:
Board Policy 5030

Related Procedures:
Business Procedure 10.06