MiraCosta Community College District

COMPLIANCE STATEMENT FOR ACCESS TO DISTRICT DATA & INFORMATION SYSTEMS (September 2005)

Responsibility of Administration

Managers and administrators throughout the college are primary custodians of student data, employee data, business data, and vendor data contained within District information systems. It is the responsibility of administration to strive diligently to meet both the ethical and legal responsibilities to the District and its students, employees, and business partners. To that end, the following guidelines governing access and protection of this data are effective for all offices and employees within the District. The principle governing legislation regarding these standards is the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended. In addition, Board Policy IV.H and Procedures IV.H-01a - H-01d, have been adopted in regard to accessing District data and information systems.

The Family Educational Rights and Privacy Act of 1974 (FERPA), as amended, establishes strict conditions on District policies and practices of disclosing student education records. FERPA protects the privacy of education records, establishes the students' rights to inspect their records, provides guidelines for correcting inaccurate or misleading data through informal hearings, and permits students to file complaints with the Family Policy Compliance Office (FPCO) concerning alleged failures of the institution to comply with this Act. Education Records are all records which contain information directly related to a student and are maintained by an educational agency or institution. These include, but are not limited to, records kept by individuals such as instructors or records pertaining to a particular program or function.

Confidentiality

Education Records may not be released to any unauthorized party, organization or entity (including law enforcement personnel and parents). Under certain circumstances, information classified as directory information may be released with approval from either of the FERPA coordinators: the Registrar or the Dean of Admissions and Records. Education Records should not be shared between departments except within the scope of department responsibilities. Prior to responding to an inquiry from outside the District, Board Procedures must be followed and written authorization obtained to release data.

Employees, whose District-designated responsibilities require access, may use District data and information systems for research or service functions. Any employee engaged in activities which require access to Education Records must have prior approval before information may be accessed. If District data is released for research, the results of that research may never individually identify any person (except when determined acceptable by a FERPA coordinator). It is imperative that District employees understand the legal responsibilities they assume when they receive access to Education Records or personal data in any form. To that end, before an individual is granted access to such data, the individual is required to read and sign this statement. This affidavit will clearly state their understanding of ethical and legal responsibilities. The following guidelines must be followed for the use and/or release of any District data:

- Student information can be used for educational purposes only
- Student or employee information including, but not limited to names, addresses, phone numbers, Social Security Numbers, credit card numbers, grades, employment, payroll and/or financial aid data must be protected from unauthorized modification, disclosure, and/or deletion. Such data must be appropriately stored and/or destroyed after use, and may not be saved, stored, or copied for other purposes
- Student or employee information may only be accessed as required to conduct official business, and may not be used to look up any further information within District information systems
- When granted access to student or employee information for a specific purpose such as a mailing or for research, all information must be destroyed after approved use (e.g., you may not file unused labels or returned mail for later use)

If you have any doubt about the permissibility of access to, use of or the release of any District data, you should always check with your appropriate manager or administrator per District Board Procedures.

Computer Access

Your user ID(s) and password(s) must remain confidential. You must log off or lock the console when leaving your computer workstation. Each individual will be responsible for the security of his or her user ID(s) and password(s). They must NOT be given to any other person. If temporary help or student workers need to access District information systems, access procedures must be worked out with the Systems and Security Administrator in AIS, and this statement must be read and signed in advance of access and filed with the Human Resources for each temporary or hourly worker. If personal computing equipment is used to access the District's data and information systems, the same policies, procedures, and guidelines shall apply.

Access to District Data and Information Systems

Employees granted access agree to:

- store information only in pre-approved or authorized locations
- affirmatively ensure the confidentiality of student, employee, and vendor records
- use information only as appropriate within assigned District responsibilities or as described in the request for data or
- access to District information systems • only properly released data by the appropriate manager or administrator will be considered "official" District data
- department head or designated liaison must immediately notify the Help Desk if an employee with access to the student information system is leaving the District, or is no longer serving in the intended capacity, so that his/her access can be deactivated or adjusted as appropriate

Violations

Violation of the *Compliance Statement for Access to District Data and Information Systems* constitutes grounds for rescinding your access to records or imposing disciplinary action, up to and including dismissal and prosecution, and may result in civil liability to the employee. Violations include, but are not limited to, the following offenses and any other comparable action:

- altering District data without appropriate supporting documentation/authorization
- accessing District data outside of your assigned duties
- releasing suppressed or confidential data without authorization
- publicly discussing suppressed or confidential data in a way that might personally identify a student or employee

Compliance Statement Acknowledgement

It is imperative that the MiraCosta Community College District has a signed affidavit on file from all employees who have District-designated responsibilities which require access to District Data and Information Systems.

Employees must be informed of, understand, and acknowledge, the Compliance Statement regarding Access to District Data and Information Systems.

I have read and will comply with the Compliance Statement for Access to District Data and Information Systems.

Employee Printed Name	
Employee Signature	
Employee Phone No.	
Employee E-mail address	
Date	
Department	
Supervisor Name	

Please complete, sign, and return this form by fax, e-mail, or in person to:

MiraCosta College -- Attn: Human Resources

- ***fax:*** ***(760) 795-6867***
- ***e-mail:*** ***hr_department@miracosta.edu***
- ***location:*** ***in Building 1000 at One Barnard Drive, Oceanside, CA 92056***