A. PURPOSE AND SCOPE

1. To outline administrative procedures governing safeguarding of district information processed electronically and/or stored on district files and equipment.

2. **Related Procedures:**
   Access to, release of, and confidentiality of
   nondirectory-type student information 6527
   Centralized automated personnel records 7101
   Release of directory-type student information 6525

B. LEGAL AND POLICY BASIS

1. **Reference:** Board policy: G-8000, H-8900, I-1200.

2. **Student Information.** Under provisions of the Family Educational Rights and Privacy Act of 1974 (Procedure 6525), information shall not be released by "processors" of information; requests must be referred to the school or department having custody of the record.

C. GENERAL

1. **Originating Office.** Suggestions or questions concerning this procedure should be directed to the Information Technology Department, Business Operations Division, Office of School Site Support.

2. **Definitions.** (These definitions are specific to the uses of computer technology within San Diego Unified School District.)

   a. **Server**: A computer that provides shared services to workstations over networks (e.g., file server, print server, mail server). A file server can be a repository for district information that can be viewed and/or managed by authorized users. Servers used to manage district information must be maintained in a manner that will provide physical security of the unit and integrity of the data and applications within.

   b. **Local area network (LAN)**: Computers and peripherals located within a limited geographical area connected for the purpose of sharing processing and

information.

c. **Wide area network (WAN)**: A network that connects computers, servers, and local area network at various locations across a large geographic area.

d. **SanDiNet**: The district's wide area network that connects schools and support offices for communication of information. SanDiNet provides access to the Internet and to the district's intranet, e-mail, and business applications.

e. **Database**: A collection of data with a designed structure for managing, storing, and providing, on demand, data for one or more users. A database structure for district information must include provisions for maintaining the security and integrity of the data.

f. **Electronic data**. Information maintained in a manner suitable for communication, processing, or storing by computer and peripheral devices.

g. **District data**. Information maintained and processed in the conduct of district business as required by state or federal mandate and/or district procedure. Confidentiality restrictions apply to information maintained as official records and to all copies of those records.

3. **Security.** Protection from theft, unauthorized view, or access of district information, whether in database files on a computer or server, on disks or other electronic storage, or in printed form. Servers containing database files of district information (original or copies) must be protected from theft, unauthorized access, and loss of data integrity.

4. **Backup of Official District Records.** Duplicate files of all computer programs, master data files, and operating system backups shall be stored in an area other than the location of the computer or server upon which the data resides. This area will have fireproof construction and be secured under lock and key. Access will be limited to authorized personnel only.

5. **Information Technology Responsibility for Networks, Systems, and District Applications.** The primary objective of the Information Technology Department is to provide required information processing capabilities to users of district systems. Information Technology Department is responsible for maintaining the district networks and local area networks connected to it for the delivery of district information. Information Technology Department is responsible for meeting service requirements, performance standards, and processing schedules of each system.

6. **Processing Requirements.** Information Technology Department is responsible for defining and enforcing recognized industry standards for safeguarding district data to ensure integrity of collected data and its management, the control of access to authorized users, and the physical security of the data, including adequate disaster recovery methods.

7. **Physical Security of Electronic Documents, Files, and Computer Equipment.** Information Technology Department will maintain a secure, climate-controlled area to house servers containing district data. The department operations center shall be comprised of the following security areas:

   a. **Maximum security**: Contains computer equipment and master files for both computer programs and master data files. Access shall be limited to those individuals authorized by persons designated by the Information Technology t Director.

   b. **Limited security**. Contains data entry equipment and the control section. Access shall be limited to those individuals authorized by persons designated by the Information Technology Director.

8. **Release of Information.** All data maintained on any district computer or server is the property of the organization responsible for the origination and maintenance

D. IMPLEMENTATION

E. FORMS AND AUXILIARY REFERENCES

F. REPORTS AND RECORDS

G. APPROVED BY

Kerry B. Flanagan

Chief of Staff, Kerry Flanagan
For the Superintendent of Schools