PENN MANOR SCHOOL DISTRICT

ADMINISTRATIVE REGULATION

APPROVED: March 8, 2013

REVISED:

800-AR-0. RECORDS MANAGEMENT

In order to effectively implement the Records Management Plan, building administrators, department heads, and/or designated employees will be responsible for identifying and routing the various types of records and data that each department creates, gathers, uses or disseminates. Requests to add, revise or delete records will be approved and initialed by the Records Coordinator.

All records, whether created or stored on electronic systems, must be retrievable and available for the entire retention period listed on the Records Retention Schedule.

Before any record is converted to a different medium, i.e. paper to electronic, the district will determine that the authorized disposition of the records can still be implemented after conversion.

Electronic Records

The Records Management Committee will recommend appropriate media and systems for storing electronic records throughout their life.

The specific requirements for selecting storage media for electronic records include the following:

1. Permits retrieval in a timely fashion.

2. Facilitates the distinction between records and nonrecords as well as the distinction between employee records and school district records.

3. Retains the records in a usable format for the length of their required retention period.

The following factors will be considered before selecting storage media or when converting records from one medium to another:

1. Required retention period for the records.

2. Maintenance necessary to retain the records in that format.

3. Ability to index and search records.

4. Costs of storing and retrieving the records stored in that format.

5. Density of the record.

6. Access time necessary to retrieve stored records.

7. Ability of the medium to run on equipment produced by multiple manufacturers.

8. Ability to transfer information from one medium to another.

9. Flexibility of the software to be used.

10. Compliance of the storage medium with current industry and/or government standards.

Before a document is created and maintained on an electronic records system, documents will be identified sufficiently to enable authorized personnel to retrieve, protect and carry out the disposition of documents in the system. Appropriate identifying information for each document maintained on electronic media may include: office of origin; file code; key words for retrieval; addressee, if any; signature; author; date; authorized disposition, coded or otherwise; and security classification, if applicable.

The district will ensure that records maintained in such systems can be correlated with related records on paper, microform, or other media.

The district must provide for the usability of image and index data for records stored on an electronic recordkeeping system over time by establishing:

1. Methods for all authorized users of the system to retrieve desired records.

2. Appropriate levels of security to ensure integrity of the records.

3. A standard interchange format when necessary to permit the exchange of records on electronic media using different software/operating systems and allow for the conversion or migration of records from one system to another.

4. Procedures for the disposition of records in accordance with the Records Retention Schedule.

5. Procedures for regular copying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their required retention period.

6. Similar security precautions required of paper records to be used when destroying or reusing electronic media that contain privacy-protected or confidential information. Electronic storage media containing such information must be electronically wiped clean or physically destroyed in such a manner that the information cannot be reconstructed by generally available means.

Record And Data Integrity

The district's records security program will:

1. Ensure that only authorized personnel have access to electronic records.

2. Provide for backup and recovery of records to protect against information loss.

3. Ensure that district personnel are trained to safeguard sensitive or classified electronic information.

4. Minimize the risk of unauthorized alteration or erasure of electronic records.

5. Ensure that electronic record security is included in a computer systems security plan.

6. Ensure that duplicate copies of permanent records are maintained in separate buildings or systems.