PENN MANOR SCHOOL DISTRICT

ADMINISTRATIVE REGULATION

APPROVED: August 19, 2013

REVISED:

830-AR-0. BREACH OF COMPUTERIZED PERSONAL INFORMATION

The district will take reasonable security measures to guard against the foreseeable loss or exposure of restricted personal information about staff, students and parents/guardians. The district will implement and maintain practices regarding physical, technical and administrative safeguards for both paper and electronic records.

The Superintendent or designee will direct and monitor a process to identify the following information, to be kept on file in the administration office:

1. What information is considered restricted.

2. Where it currently resides.

3. How it is protected.

4. Maximum amount to be spent in notifying individuals of a breach, as designated in the district budget.

5. Who is responsible for providing each level of security for each piece of restricted information.

Employees will promptly report to the Superintendent any breach of the district's computerized data that compromises the security, confidentiality or integrity of personal information maintained by the district. The Superintendent will immediately inform the Board of such breach of information.

Identifying Security Breach

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized individual or an individual without valid authorization, the district will consider the following indications:

1. Information is in the physical possession and control of an unauthorized individual, such as a lost or stolen computer or other device containing information.

2. Information has been downloaded or copied.

3. Information was used by an unauthorized individual, such as fraudulent accounts or reported identity theft.

4. Other factors the district deems appropriate and relevant to such determination.

Procedure For Notification

Notice of a breach of information security will be provided to the individual whose restricted personal information has been acquired by an unauthorized person.

Once it has been determined that a security breach has occurred, the following steps will be taken by the designated employee:

1. If the breach involved computerized data owned or licensed by the district, the district will directly notify those residents whose private information was or is reasonably believed to have been acquired by a person without valid authorization.

2. If the breach involved computer data maintained by the district, the district directly will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been acquired by a person without valid authorization.

3. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system. Notification should be provided within three (3) working days of discovery of the breach, when possible, but not later than thirty (30) working days.

4. The required notification will include:

    a. District contact information.

    b. Description of the categories of information that were or are reasonably believed to have been acquired without authorization.

    c. Which specific elements of personal or private information were or are reasonably believed to have been acquired.

5. The notification requirement may be delayed if a law enforcement agency determines that such notification will impede a criminal investigation. The required notification will then be made after the law enforcement agency determines that such notification does not compromise the investigation.

The district will provide notice by at least one (1) of the following methods:

1. Written notice to last known home address for the individual.

2. Telephone notice if the individual can be reasonably expected to receive the notice and the notice is given in a clear and conspicuous manner; describes the incident in general terms; verifies the personal information but does not require the individual to provide personal information; and provides a telephone number to call or Internet website to visit for further information or assistance.

3. Email notice, if a prior business relationship exists and the school district has a valid email address for the individual.

4. Substitute notice if the district determines that the cost of notice exceeds $18,900, the affected individuals exceed 40,000 people, or the district does not have sufficient contact information. Substitute notice shall consist of an email notice, conspicuous posting of the notice on the district's website, and notification to major statewide media.

5. If the district provides notification to more than 1,000 persons at one (1) time, the district shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices, without unreasonable delay.