POLICY

FRANKLIN TOWNSHIP
BOARD OF EDUCATION

File Code: 6142.11

DATA BREACH

It is the policy of the Franklin Township School District ("School District") that employees comply with the New Jersey Identity Theft Protection Act. Employees are required to protect the sensitive personal about employees from inadvertent, negligent and willful disclosure or breach of such information, data or records.

Definition

Data Breach - Disclosure of personally identifiable information (PII) pertaining to students or staff is accessed by any unauthorized person.

Personally Identifiable Information - The first name or first initial and last name of any student or staff in combination with and linked to any one or more of the following: (a) social security number; (b) driver's license number or State identification card number; and (c) financial account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

Guidelines Data Breach Notification

All employees must protect and secure all electronic resources and information, data and records of the School District from an inadvertent disclosure when they are under the supervision and control of the School District, and when they are not under the supervision or control of the School District, for example, but not limited to, working at home, on vacation, or elsewhere.

If any employee becomes aware of the release of School District information, data or records the release must be reported to the School Business Administrator immediately.

If there is a breach of security of the information, data, or records of the School District, the School District must disclose any breach of security of personal records after discovery or notification of the breach to any New Jersey resident whose personal information was or is reasonably believed to have been accessed by an unauthorized person.

Before disclosing a breach of security, the School District must report the breach of security and any information pertaining to the breach to the local or state law enforcement agency for investigation or handling in advance of the disclosure to the customer or others. The School District may be required to delay notification if a law enforcement agency determines that the notification will impede a criminal or civil investigation.

The School Business Administrator must then determine whether a data breach notification will be issued. Notifications may be made through a written notice, telephone notice, electronic notice, or a substitute notice (only if the requirements of the New Jersey Identity Theft Protection Act are met).

A notice of the security breach must be provided to New Jersey residents whose unencrypted and unredacted computerized personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that the School District believes has or could cause loss or injury.

All records of the School District must be destroyed pursuant to the School District document retention and destruction policy, schedule and procedures. Destruction means shredding, erasing, or modifying the personal information in the records to make them unreadable, undecipherable or non-reconstructionable through generally available means.

Social Security Number Requirement

Unless otherwise permitted by law, School District employees must protect the privacy of Social Security numbers.

A. The School District may not do any of the following:

i. Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available the Social Security number to the general public.

ii. Print an individual's Social Security number on any card required for the individual to access products or services provided by School District.

iii. Require an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

iv. Require an individual to use his or her Social Security number to access an Internet website unless a password or unique personal identification number or other authentication device is also required to access the website.

v. Print an individual's Social Security number on any materials that are mailed to the individual unless Federal or State law requires the Social Security number to be on the document to be mailed. However, Social Security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the Social Security number. A Social Security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer

not requiring an envelope, or visible on the envelope or without the envelope having been opened.

B. The School District may collect, use, or release a Social Security number as required by federal or state law, or may use the Social Security number for internal verification, administrative purposes or for law enforcement investigations.

C. This requirement does not apply to a document that is required by law to be open to the public, and originates with, or is filed, recorded or maintained by any governmental agency, instrumentality or taxing authority.

The Board of Education recognizes that data security and data management are becoming increasingly prominent concerns as technology becomes more integral to the management of education records and education data systems.

The District shall provide ongoing staff training in accordance with the New Jersey Identity Theft Act. Any breach of the District's computerized data which compromises the security, confidentiality, or integrity of personal information will be handled in accordance with state law.

Date adopted: 5/22/17