POLICY 2.036

4-P I recommend that the Board adopt the proposed new Policy 2.036, entitled "Breach of Personal Identification Information."

[Contact: Darron Davis, PX 48953, Dianne Howard, PX 48414, Sharon Swan, PX 48214, Michael Burke, PX 48584, Deepak Agarwal, PX 48773.]

Adoption **CONSENT ITEM**

- The Board approved development of this revised Policy at the development reading on February 3, 2010.

- This proposed new policy implements Sec. 817.5681, FS, entitled "breach of security concerning confidential personal information in third-party possession".

- Sec. 817.5681, FS, requires any person who conducts business within Florida and maintains personal information in a computerized data system to disclose a breach in the security of the data to any Florida resident subject to certain exceptions. When a disclosure is required, it must be made without unreasonable delay, and no later than 45 days following the determination that unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person and the acquired information materially compromises the security, confidentiality or integrity of personal information.

- The proposed policy sets out procedures for various work units of the School District to report any breach of confidential personal identifiable information. Personal identifiable information includes an individual's first name, first initial and last name, or any middle and last name, in combination with and linked to any one or more of the following, when not encrypted or redacted:

    1. Social security number.

    2. Driver's license number or Florida Identification Card Number.

    3. Financial account number, 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 identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

- Directors of various work units which receive the above information for the discharge of the unit's duties and responsibilities have been identified as the privacy officer for such data and for the reporting of any security breach to the security officer. The Chief Information Officer will serve as the security officer for the purposes of the policy.

POLICY 2.036

BREACH OF PERSONAL IDENTIFICATION INFORMATION

1. **Purpose**. The School Board regards security and confidentiality of personal data and information to be of utmost importance. Palm Beach County School District (District) increasingly provides for the maintenance of personal information of students, parents/guardians, employees or retirees, job applicants, vendors and volunteers in an electronic format, as well as other formats. Thus, the School Board desires to provide for any potential risk of a breach in the District's electronic system security and the possible disclosure of personal information regardless of its format. This policy addresses the manner in which the District will respond to an unauthorized access and acquisition of computerized data that compromises the security and confidentiality of unencrypted personal information. This policy is consistent with Fla. Stat. § 817.5681 and federal laws.

2. **Definitions.** For the purposes of this policy, the following definitions shall apply:

   a. *Breach of the system's security* means unauthorized or unlawful acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the District as part of the database of personal information. Good faith acquisition of personal information by an employee or agent of the District for a legitimate business purpose or the purpose of the District is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the District and is not subject to further unauthorized disclosure.

   b. *Person/Individual* means a student or former student, a parent or guardian, job applicant, employee or retiree, vendor or volunteer of the District, firms, associations, joint ventures, partnerships, estates, trusts, business trusts, syndicates, fiduciaries, corporations, and all other groups or combinations, on which the District maintains personal information.

   c. *Personal identifiable information* includes an individual's first name, first initial and last name, or any middle and last name, in combination with and linked to any one or more of the following, when not encrypted or redacted:

      i. Social security number.

      ii. Driver's license number or Florida Identification Card Number.

      iii. Financial account number, 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 identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

d. *Records* means any material, regardless of its physical form, on which information is recorded or preserved by any means, including written or spoken words, graphically depicted, printed or electromagnetically transmitted. This term does not include publicly available directories containing information that an individual has voluntarily consented to have publicly disseminated or listed, such as name, address or telephone number.

e. *Unauthorized user/person* means any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains.

3. **Policy Statement.** It is the policy of the School Board to ensure the District's treatment, custodial practices, and uses of personally identifiable information are in compliance with all relevant state and federal laws. The District shall provide notice of any system security breach, following discovery, to any student or former student, parent/guardian, job applicant, employee or retiree, vendor or volunteer whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

a. *Time of Notice*. The District shall provide notification, as provided in section 5 herein, not more than forty-five (45) days after a determination of any computerized system security breach to any state resident whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed or acquired by unauthorized persons, in compliance with Fla. Stat. §817.5681, as now or hereafter amended. This policy also applies to information maintained on behalf of the District by a third party or vendor.

b. *Law Enforcement Measure*. Regardless of the above notice time period, such notice shall be made without a reasonable delay, except when a law enforcement agency determines and advises the District in writing that the notification would impede a criminal or civil investigation, or the District must take necessary measures to determine the scope of the breach and to restore the reasonable integrity of the data system.

c. *Encryption Breach*. The District will also provide notice of the breach if the encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of security of the encryption, or if the security breach involves a person with access to the encryption key.

d. *Reporting of Breach*. An employee shall immediately report a breach of personal information as provided in this policy to the responsible person(s), as

privacy officers, identified in section 4 for the personal identifiable information and a breach of personal identifiable information. The responsible person, as privacy officers, shall immediately inform the Chief Information Officer, as Security Officer for the District of the breach. In such reporting, the employee and privacy officer shall complete the *Personal Identification Security Breach Reporting Form, PBSD Form 2344*, attached and incorporated hereto.

e. *Security Officer*. The Security Officer shall review, and implement if necessary, administrative, technical and physical safeguards to ensure the confidentiality, integrity and availability of the personal identifiable information that is maintained in electronic form by the District, and implement any necessary steps or security measures to protect the electronic personal identifiable information against any reasonably anticipated threats or hazards, unauthorized uses or disclosures, during storage, processing or transmission. The Security Officer may designate local security officers to work with the necessary privacy officials and work units as necessary to facilitate the implementation of procedures and security measures.

f. *Employee Confidentiality Agreement.* All current and future employees must preserve the security and confidentiality of the personal identification information he or she has access to and uses in the performance of District duties and job responsibilities. Future and current District employees shall sign and be bound by the *Employee Confidentiality Agreement for Handling of Personal Identification Information, PBSD Form 2345*, attached and incorporated hereto.

g. *Failure to Report Breach*. An employee who fails to report a breach or to comply with this Board policy will be subject to disciplinary action, up to and including dismissal, and may also be subject to criminal prosecution. A consultant or another person who fails to report a breach related to the performance of his/her duties with the School District may be barred from work for the District and may also be subject to criminal prosecution.

4. **Designated Privacy Officials.** The following employees shall be responsible for personal identifiable information, serving as privacy officers, for any related security breaches in their respective areas of responsibility. The work units shall be responsible for controlling access to, and security of, the personal identification information.

a. Employee personnel information - Chief of Human Resources or designee.

b. Information on students - Chief Academic Officer or designee.

c. Free or reduced lunch program – Director of Food Services, or designee.

d. Purchasing proposals and related contracts - Director of Purchasing.

e. Computer system authentication, authorization, access, usage, profile, cookie, or other such files or in telecommunications or network records – Chief Information Officer or designee.

f. For the administration of federal and state income taxes – Chief Financial Officer or designee.

g. Information in grant proposals - Chief Academic Officer or designee.

h. Financial account numbers, debit and credit cards - Treasurer.

i. Retirees, health or workers' compensation information – Director of Risk and Benefits Management

j. Volunteer information - Volunteer Coordinator.

If a work unit does not have a privacy officer designated within this policy, the department head shall be responsible for ensuring the duties of the privacy officer are performed if there is a breach of personal identification information occurring within the department.

5. **Notice and Notification Methods.**

a. The District, through the responsible person identified in section 4 herein as the privacy officer, shall provide notice to any affected student or former student, parent/guardian, job applicant, employee or retiree, vendor or volunteer by at least one (1) of the following methods:

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

ii. E-mail notice, if a prior business relationship exists and the District has a valid e-mail address for the individual and the individual has agreed to accept communications electronically.

iii. Substitute notice, if the District determines that the cost of notice exceeds $250,000, the affected individuals exceed 500,000 people, *or* the District does not have sufficient contact information. Substitute notice shall consist of a written notice as above; an electronic or e-mail notice when the District has an electronic mail or email for the subject persons; conspicuous posting of the notice on the District's web site; and notification to major statewide media.

iv. 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.

b. The notice shall be clear and conspicuous and shall include the following information:

i. A description of the incident in general terms;

ii. A description of the type of personal information that was the subject of the security breach;

iii. A description of what the District has done to protect the individuals' information from the security breach;

iv. A telephone number or other contact information so that recipients of the notice can call for further information and assistance; and

v. A reminder to the recipient to review account statements or monitor credit reports and to immediately report any suspicious activity or incidents of suspected theft to law enforcement and consumer reporting bureaus.

6. **District Vendors or Third Parties with Access to Personal Information**. Any District vendor maintaining computerized data that includes personal information on behalf of the District shall disclose to the District any breach of security of its system as soon as practicable, but not later than three (3) days following the determination, if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice to the District shall be to the Superintendent and to the responsible work unit, and the notice shall include the information as provided in section 5b of this policy. The vendor shall be responsible for any costs associated with the providing of notice related to a breach of security of its system.

a. When agreements are established with vendors or third parties, those agreements shall include satisfactory assurances that the contracting third party will appropriately safeguard personal identification information in accordance with state and federal laws and regulations and School Board policies. When providing access to or passing personal identification information to a vendor or third party agent of the District, the agreements shall include terms and conditions, at a minimal, that:

i. Prevent disclosure of personal identification information by the vendor or third party to other third parties.

ii. Require vendors or third parties to observe federal and state laws and School Board policies for the breach of personal identification information.

iii. Require a specific plan by the third party for the implementation of administrative, technical or physical security strategies to protect personal identification data and information.

iv. Require a plan for the destruction or return of personal identification information upon completion of the third party's contractual obligations.

7. **Storage and Disposal**.

a. All documents or files that contain personal identifiable information must be stored in a physically secure manner. Personal identifiable information shall not be stored on computers or other electronic devices that are not secured against unauthorized access.

b. Documents or other materials that contain personal identifiable information shall not be thrown away through usual trash disposal. They shall be discarded or destroyed only in a manner that protects their confidentiality, such as shredding.

c. Any disposal of documents will comply with state laws and Board policies.

8. **Administrative Procedures.** The Superintendent, or designee, shall be responsible for the coordination of any incident response and shall ensure administrative procedures are implemented to:

a. Ensure prompt internal notification of appropriate persons when a breach is detected, including the use of an incident response team, management and the internal owner of the data;

b. Assess the nature and scope of the incident, and to identify the systems and personal information that has been accessed or misused;

c. Contain, control and correct any security incident;

d. Appropriately notify law enforcement, and public relations personnel;

e. Timely notify individuals affected by a breach of their data; and

f. Address responses to likely inquiries; and

g. Document all responsive actions taken;

h. Regularly review and review the incident response plan; and

i. Provide training to employees on the importance of information protection and immediate reporting of breaches.

STATUTORY AUTHORITY: Fla. Stat. §§ 1001.41, 1001.42
LAWS IMPLEMENTED: Fla. Stat. §§ 817.5681. Fair and Accurate Credit Transaction Act of 2003, *Fair Credit Reporting Act* (15 U.S.C. Sec. 1681 *et seq*.); *Family Educational Rights and Privacy Act* (20 USC § 1232g; 34 CFR Parts 99)

216 HISTORY: __/___2010

Legal Signoff:

The Legal Department has reviewed proposed Policy 2.036 and finds it legally sufficient for adoption by the Board.

_____ _____

Attorney Date

THE SCHOOL DISTRICT OF PALM BEACH COUNTY

Personal Identification Security Breach Report

Date Breach Occurred _____

Date Breach Discovered _____

Reported by _____ **School/Dept.** _____

Provide the number of person(s) affected by the breach:

Employee(s)/Job Applicant(s) _____ Student(s) _____ Volunteer(s) _____ Total Number

Parent(s)/Guardian(s) _____ Vendor(s) _____ Retire(s) _____ ☐

Description of breach (select all that apply):

☐ Stolen information, computer, CD, tape, etc. ☐ Hacking incident ☐ Inadvertent disclosure

☐ Lost computer, CD, tape, etc. ☐ Unauthorized user/person

Other (specify) _____ Attach additional descriptions

Information acquired (select all that apply)

☐ Name ☐ Social Security Number ☐ Driver's License Number ☐ Florida Identification Card Number

☐ Financial Account Number ☐ Credit or Debit Card Number Other (specify) _____

FOR COMPLETION BY PRIVACY OFFICER

A. IF NOTIFICATION

1. Manner of Notification to Affected Person(s) (attach copy)

☐ Written (date) _____ **OR**

☐ Electronic (e-mail - must be done consistent with federal law) (date) _____ **OR**

☐ Substitute (All below must be used if the costs would exceed $250,000, persons to be notified exceed $500,000, or person does not have sufficient contact information) (Attach justification)

☐ Electronic mail or e-mail, if there is an electronic mail or e-mail for the subject person(s) (date sent) _____

☐ Conspicuous posting of notification on School District's web page (date posted) _____

☐ Notification to statewide media (date notifitied) _____

2. Notification of Consumer Reporting Agencies (if more than 1,000 persons affected at a single time (date) _____

- Equifax (800) 525-6285 www.equifax.com
- Experian (800) 397-3742 www.experian.com
- TransUnion (800) 680-7289 www.transunion.com

B. IF THERE IS NONOTIFICATION(Check, if applicable)

☐ An investigation or consultation has occurred with relevant federal, state and local law enforcement agencies; and it has been determined that the breach has not and will not likely result in harm to the subject individuals. (Attach the required documentation in writing. Please retain this completed form, attachments and documentation for at least 5 years).

C. IF DELAY IN NOTIFICATION (Check applicable reason)

☐ Due to law enforcement request OR ☐ Need District to determine scope of breach/restore integrity of data system.

_____ _____

Signature of Privacy Officer *Date*

THE SCHOOL DISTRICT OF PALM BEACH COUNTY

Employee Confidentiality Agreement for Personal Identification and Protected Health Information

Print or Type

Employee ID # _____ School/Department _____

Employee First Name _____ MI _____ Last Name _____

I, above named employee, have accepted a position or currently hold a position with the Palm Beach County School District. As a condition of my employment or continued employment with the School District, I understand and agree with the following provisions governing the confidentiality of personal identification information and protected health information (confidential information), to which I am bound as an employee:

1. I will only access, use, or disclose confidential information, during the course of my employment or after my employment ends, as required and permitted in the performing of duties and responsibilities for which I have been hired with the School District. I understand that this obligation extends to any confidential information that I may acquire during the course of my employment or association with the School District, whether in oral, written or electronic form and regardless of the manner in which access was obtained. I understand confidential includes:

    a. Personal identification information which means an individual's first name, first initial and last name, or any middle and last name, in combination with and linked to any one or more of the following, when not encrypted or redacted: social security number; driver's license number or Florida Identification Card Number; or financial account number, 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.

    b. Protected Health Information which means information collected from an employee, retiree or student that is created or received by the School District, in electronic media or any other form or medium, that relates to the past, present or future physical or mental health or condition of an employee, retiree or student in the provision of health care to the employee, retiree or student and that identifies the employee, retiree or student individually or which reasonably can be used to identify the employee, retiree or student. Protected health information does not include individually identifiable health information in education records covered by the Family Education Rights and Privacy Act (FERPA).

2. I agree to safeguard all confidential information I access in the course of my employment and to keep it confidential as required by law and in accordance with School Board Policies 2.035 (Breach of Personal Identification Information) and 2.036 (Protected Health Information).
3. I understand unauthorized use or disclosure of confidential information will result in disciplinary action, up to and including the termination of my employment or association with the Palm Beach County School District, and the imposition of possible civil or criminal actions.
4. If I become aware that a breach of confidential information has occurred due to my own or others' acts or omissions, I agree to immediately report the breach of confidential information to the Privacy Officer/Data Owner in my work area (or my department head, if my work unit does not have a Privacy Officer/Data Owner), as required by School Board Policies 2.035 and 2.036. I understand that should I fail to report a breach or to comply with this agreement or Board Policies, I will be subject to disciplinary action, up to and including termination of my employment. In addition, I understand that the District reserves the right to take further action, including referral to the appropriate internal or law enforcement authorities for investigation, adjudication or prosecution, or the pursuit of civil remedies.
5. Upon termination of my employment or as requested by my supervisor, I will return any and all material containing confidential information to my supervisor or designee.
6. I understand that this obligation will survive the termination of my employment or end of my association with the Palm Beach County School District regardless of the reason for such termination.

By signing and dating this Agreement in the spaces below, I certify that I have read and understood this Agreement in its entirety, and that I agree to be bound by its terms during my employment and after I leave my position with the School District.

_____ _____

Signature of Employee *Date*