



POLICY 2.036

5-C I recommend that the Board approve development of 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.]

Development

CONSENT ITEM

- 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:
 - Social security number.
 - Driver’s license number or Florida Identification Card Number.
 - 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
2
3 1. **Purpose.** The School Board regards security and confidentiality of personal
4 data and information to be of utmost importance. Palm Beach County School
5 District (District) increasingly provides for the maintenance of personal information
6 of students, parents/guardians, employees or retirees, job applicants, vendors and
7 volunteers in an electronic format, as well as other formats. Thus, the School
8 Board desires to provide for any potential risk of a breach in the District's electronic
9 system security and the possible disclosure of personal information regardless of
10 its format. This policy addresses the manner in which the District will respond to an
11 unauthorized access and acquisition of computerized data that compromises the
12 security and confidentiality of unencrypted personal information. This policy is
13 consistent with Fla. Stat. § 817.5681 and federal laws.
- 14 2. **Definitions.** For the purposes of this policy, the following definitions shall apply:
- 15 a. Breach of the system's security means unauthorized or unlawful acquisition of
16 computerized data that materially compromises the security, confidentiality or
17 integrity of personal information maintained by the District as part of the
18 database of personal information. Good faith acquisition of personal
19 information by an employee or agent of the District for a legitimate business
20 purpose or the purpose of the District is not a breach of the security of the
21 system if the personal information is not used for a purpose other than the
22 lawful purpose of the District and is not subject to further unauthorized
23 disclosure.
- 24 b. Person/Individual means a student or former student, a parent or guardian, job
25 applicant, employee or retiree, vendor or volunteer of the District, firms,
26 associations, joint ventures, partnerships, estates, trusts, business trusts,
27 syndicates, fiduciaries, corporations, and all other groups or combinations, on
28 which the District maintains personal information.
- 29 c. Personal identifiable information includes an individual's first name, first initial
30 and last name, or any middle and last name, in combination with and linked to
31 any one or more of the following, when not encrypted or redacted:
- 32 i. Social security number.
- 33 ii. Driver's license number or Florida Identification Card Number.
- 34 iii. Financial account number, credit or debit card number, in combination with
35 any required security code, access code or password that would permit

36 access to an individual's financial account.

37 Personal identifiable information does not include publicly available information that
38 is lawfully made available to the general public from federal, state or local
39 government records or widely distributed media.

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

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

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

57 a. Time of Notice. The District shall provide notification, as provided in section
58 5 herein, not more than forty-five (45) days after a determination of any
59 computerized system security breach to any state resident whose unencrypted
60 and unredacted personal information was or is reasonably believed to have
61 been accessed or acquired by unauthorized persons, in compliance with Fla.
62 Stat. §817.5681, as now or hereafter amended. This policy also applies to
63 information maintained on behalf of the District by a third party or vendor.

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

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

- 74 d. Reporting of Breach. An employee shall immediately report a breach of
75 personal information as provided in this policy to the responsible person(s), as
76 privacy officers, identified in section 4 for the personal identifiable information
77 and a breach of personal identifiable information. The responsible person, as
78 privacy officers, shall immediately inform the Chief Information Officer, as
79 Security Officer for the District of the breach. In such reporting, the employee
80 and privacy officer shall complete the [Personal Identification Security Breach](#)
81 Reporting Form, PBSD Form 2344, attached and incorporated hereto.
- 82 e. Security Officer. The Security Officer shall review, and implement if necessary,
83 administrative, technical and physical safeguards to ensure the confidentiality,
84 integrity and availability of the personal identifiable information that is
85 maintained in electronic form by the District, and implement any necessary
86 steps or security measures to protect the electronic personal identifiable
87 information against any reasonably anticipated threats or hazards,
88 unauthorized uses or disclosures, during storage, processing or transmission.
89 The Security Officer may designate local security officers to work with the
90 necessary privacy officials and work units as necessary to facilitate the
91 implementation of procedures and security measures.
- 92 f. Employee Confidentiality Agreement. All current and future employees
93 must preserve the security and confidentiality of the personal identification
94 information he or she has access to and uses in the performance of District
95 duties and job responsibilities. Future and current District employees shall
96 sign and be bound by the [Employee Confidentiality Agreement for Handling of](#)
97 Personal Identification Information, PBSD Form 2345, attached and
98 incorporated hereto.
- 99 g. Failure to Report Breach. An employee who fails to report a breach or to
100 comply with this Board policy will be subject to disciplinary action, up to and
101 including dismissal, and may also be subject to criminal prosecution. A
102 consultant or another person who fails to report a breach related to the
103 performance of his/her duties with the School District may be barred from work
104 for the District and may also be subject to criminal prosecution.
- 105 4. **Designated Privacy Officials.** The following employees shall be responsible for
106 personal identifiable information, serving as privacy officers, for any related security
107 breaches in their respective areas of responsibility. The work units shall be
108 responsible for controlling access to, and security of, the personal identification
109 information.
- 110 a. Employee personnel information - Chief of Human Resources or designee.
- 111 b. Information on students - Chief Academic Officer or designee.
- 112 c. Free or reduced lunch program – Director of Food Services, or designee.

- 113 d. Purchasing proposals and related contracts - Director of Purchasing.
- 114 e. Computer system authentication, authorization, access, usage, profile, cookie,
115 or other such files or in telecommunications or network records – Chief
116 Information Officer or designee.
- 117 f. For the administration of federal and state income taxes – Chief Financial
118 Officer or designee.
- 119 g. Information in grant proposals - Chief Academic Officer or designee.
- 120 h. Financial account numbers, debit and credit cards - Treasurer.
- 121 i. Retirees, health or workers' compensation information – Director of Risk and
122 Benefits Management
- 123 j. Volunteer information - Director of Public Affairs.

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

128 **5. Notice and Notification Methods.**

- 129 a. The District, through the responsible person identified in section 4 herein as
130 the privacy officer, shall provide notice to any affected student or former
131 student, parent/guardian, job applicant, employee or retiree, vendor or
132 volunteer by at least one (1) of the following methods:
 - 133 i. Written notice to last known home address for the individual.
 - 134 ii. E-mail notice, if a prior business relationship exists and the District has a valid
135 e-mail address for the individual and the individual has agreed to accept
136 communications electronically.
 - 137 iii. Substitute notice, if the District determines that the cost of notice exceeds
138 \$250,000, the affected individuals exceed 500,000 people, or the District does
139 not have sufficient contact information. Substitute notice shall consist of a
140 written notice as above; an electronic or e-mail notice when the District has
141 an electronic mail or email for the subject persons; conspicuous posting of the
142 notice on the District's web site; and notification to major statewide media.
 - 143 iv. If the District provides notification to more than 1,000 persons at one (1) time,
144 the District shall also notify all consumer reporting agencies that compile and
145 maintain files on consumers on a nationwide basis of the timing, distribution

- 146 and number of notices, without unreasonable delay.
- 147 b. The notice shall be clear and conspicuous and shall include the following
148 information:
- 149 i. A description of the incident in general terms;
- 150 ii. A description of the type of personal information that was the subject of the
151 security breach;
- 152 iii. A description of what the District has done to protect the individuals'
153 information from the security breach;
- 154 iv. A telephone number or other contact information so that recipients of the
155 notice can call for further information and assistance; and
- 156 v. A reminder to the recipient to review account statements or monitor credit
157 reports and to immediately report any suspicious activity or incidents of
158 suspected theft to law enforcement and consumer reporting bureaus.
- 159 6. **District Vendors or Third Parties with Access to Personal Information.** Any
160 District vendor maintaining computerized data that includes personal information
161 on behalf of the District shall disclose to the District any breach of security of its
162 system as soon as practicable, but not later than three (3) days following the
163 determination, if personal information was, or is reasonably believed to have been,
164 acquired by an unauthorized person. The notice to the District shall be to the
165 Superintendent and to the responsible work unit, and the notice shall include the
166 information as provided in section 5b of this policy. The vendor shall be
167 responsible for any costs associated with the providing of notice related to a breach
168 of security of its system.
- 169 a. When agreements are established with vendors or third parties, those
170 agreements shall include satisfactory assurances that the contracting third
171 party will appropriately safeguard personal identification information in
172 accordance with state and federal laws and regulations and School Board
173 policies. When providing access to or passing personal identification
174 information to a vendor or third party agent of the District, the agreements
175 shall include terms and conditions, at a minimal, that:
- 176 i. Prevent disclosure of personal identification information by the vendor or third
177 party to other third parties.
- 178 ii. Require vendors or third parties to observe federal and state laws and School
179 Board policies for the breach of personal identification information.
- 180 iii. Require a specific plan by the third party for the implementation of

181 administrative, technical or physical security strategies to protect personal
182 identification data and information.

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

185 7. **Storage and Disposal.**

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

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

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

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

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

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

203 c. Contain, control and correct any security incident;

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

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

206 f. Address responses to likely inquiries; and

207 g. Document all responsive actions taken;

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

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

211 STATUTORY AUTHORITY: Fla. Stat. §§ 1001.41, 1001.42

212 LAWS IMPLEMENTED: Fla. Stat. §§ 817.5681. Fair and Accurate Credit Transaction
213 Act of 2003, *Fair Credit Reporting Act* (15 U.S.C. Sec. 1681 *et seq.*); *Family Educational*
214 *Rights and Privacy Act* (20 USC § 1232g; 34 CFR Parts 99)
215 HISTORY: __/____2010

Legal Signoff:

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

Attorney

Date

