Office of Superintendent of Schools
Board Meeting of January 14, 2015

December 17, 2014

Office of School Board Attorney
Walter J. Harvey, School Board Attorney

SUBJECT: **FINAL READING: PROPOSED ADOPTION OF NEW BOARD POLICY 8351, *ELECTRONIC DATA SECURITY BREACH NOTICE REQUIREMENTS*, AND AMENDED BOARD POLICIES 8332, *BIOMETRIC INFORMATION RESTRICTION AND PRIVACY PROTECTIONS*, AND 2430.01, *SCHOOL VOLUNTEERS***

COMMITTEE: **INNOVATION, EFFICIENCY & GOVERNMENTAL RELATIONS**

LINK TO STRATEGIC FRAMEWORK: **FINANCIAL EFFICIENCY/STABILITY**

At the December 10, 2014, Board meeting, the Board unanimously approved Agenda Item G-1 ("Data Security Breach") to authorize the Superintendent to initiate rulemaking to promulgate new Board policy 8351, *Electronic Data Security Breach Notice Requirements*, and amend Board policies 8332, *Biometric Information Restriction and Privacy Protections*, and 2430.01, *School Volunteers.*

The purpose of the changes is to assist in preventing identity theft that may result from an electronic data security breach that discloses personal information. The effect of the new policy is to incorporate state law into Board policy requiring government agencies to provide notice of an electronic security breach of personal information under certain conditions. In addition, the District must provide information to parents of students who are younger than sixteen (16), disabled or incapacitated, of their legal right under state law to have their child's credit frozen if they are potentially a victim of a breach. Policies 8332 and 2430.01 are proposed to be amended to conform to legislative changes that prohibit the collection of political affiliation, voting history, religious affiliation or biometric information from students, parents and siblings. It is also recommended that Policy 8332 be renamed to *Collection of Personal Information.*

The new policy directs the District to notify potential victims of a breach of electronic data security. It applies only to data stored electronically or digitally on any District computer system or database and provides a definition of personal information, requirements for (1) timing of the notice and interaction with law enforcement investigating the breach, (2) minimum content for the notice, (3) methods of communication of the notice, and (4) other necessary reporting. It also requires that the District annually provide information to all parents of their legal right to request the state to freeze the credit of their child who is sixteen (16) years old or younger, incapacitated or disabled.

G-2

The Notice of Intended Action was published in the *Miami Daily Business Review* on December 15, 2014, in various places for public information and mailed to various organizations representing persons affected by the new and amended policies and to individuals requesting notification. The time to request a hearing or protest the adoption of the new and amended policies has elapsed.

Pursuant to the Administrative Procedures Act, the new and amended policies are presented to The School Board of Miami-Dade County, Florida, for adoption and authorization to file the new and amended policies in the official records of The School Board of Miami-Dade County, Florida.

Attached are the Notice of Intended Action and the proposed new and amended policies. Changes are indicated by underscoring words to be added and ~~striking through~~ words to be deleted.

RECOMMEND: That The School Board of Miami-Dade County, Florida, adopt new Board policy 8351, *Electronic Data Security Breach Notice Requirements*, and amend Board policies 8332, *Biometric Information Restriction and Privacy Protections*, and 2430.01, *School Volunteers* and authorize the Superintendent to file the new and amended policies with The School Board of Miami-Dade County, Florida, to be effective January 14, 2015.

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on December 10, 2014, its intention to promulgate new Board Policy 8351, *Electronic Data Security Breach Notice Requirements*, and amend Board Policies 8332, *Biometric Information Collection Restrictions and Privacy Protections*, and 2430.01, *School Volunteers*, at its meeting of January 14, 2015.

PURPOSE AND EFFECT: The purpose of the changes is to assist in preventing identity theft that may result from an electronic data security breach that discloses personal information. The effect of the new policy is to incorporate state law into Board policy requiring government agencies to provide notice of an electronic security breach of personal information under certain conditions. In addition, the District must provide information to parents of students who are younger than sixteen (16), disabled or incapacitated, of their legal right under state law to have their child's credit frozen if they are potentially a victim of a breach. Policies 8332 and 2430.01 are being amended to conform to legislative changes that prohibit the collection of political affiliation, voting history, religious affiliation or biometric information from students, parents and siblings. In addition, the name of Board Policy 8332 is proposed to be changed to *Collection of Personal Information.*

SUMMARY: The new policy directs the District to notify potential victims of a breach of electronic data security. It applies only to data stored electronically or digitally on any District computer system or database and provides a definition of personal information, requirements for (1) timing of the notice and interaction with law enforcement investigating the breach, (2) minimum content for the notice, (3) methods of communication of the notice, and (4) other necessary reporting. It also requires that the District annually provide information to all parents of their legal right to request the state to freeze the credit of their child who is sixteen (16) years old or younger, incapacitated or disabled. The amendments to Policies 8332 and 2430.01 will prohibit the collection of political affiliation, voting history, religious affiliation or biometric information from students, parents and siblings. In addition, the name of Board Policy 8332 is proposed to be changed to *Collection of Personal Information.*

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: 1001.41 (1), (2), 1001.42 (25), 1001.43 (10), F.S.

LAWS IMPLEMENTED INTERPRETED OR MADE SPECIFIC: 501.0051, 501.171, 1002.222, F.S.,

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF January 14, 2015, which begins at 1:00 p.m., in the School Board Auditorium, 1450 N.E. Second Avenue, Miami, Florida 33132. Persons requesting such a hearing or who wish to provide information regarding the statement of estimated regulatory costs, or to provide a proposal for a lower cost regulatory alternative as provided in Section 120.54(1), F.S., must do so in writing by January 7, 2015, to the Superintendent, Room 912, at the same address.

ANY PERSON WHO DECIDES TO APPEAL THE DECISION made by the School Board of Miami-Dade County, Florida, with respect to this action will need to ensure the preparation of a verbatim record of the proceedings, including the testimony and evidence upon which the appeal is to be based. (Section 286.0105, Florida Statutes)

COPIES OF THE PROPOSED NEW AND AMENDED POLICIES are available at cost to the public for inspection and copying in the Citizen Information Center, Room 158, 1450 N.E. Second Avenue, Miami, Florida 33132.

Originator: Board Member Raquel Regalado
Date: November 24, 2014

NEW POLICY

8351 – ELECTRONIC DATA SECURITY BREACH NOTICE REQUIREMENTS

The School Board shall take reasonable measures to protect and secure data containing personal information in electronic form and shall provide notice of a security breach pursuant to law.

Definitions

"**Breach of Security**" or "**Breach**" means unauthorized access of data in electronic form containing personal information belonging to School Board members, employees, parents and students. Good faith access of personal information by an employee or agent does not constitute a breach of security, provided that the information is used for a proper, District-related purpose and is not subject to further unauthorized use.

"**Data in electronic form**" means any data stored electronically or digitally on any District or third-party agent computer system or other database and includes mass storage devices.

"**Personal Information**" means

(a) An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(1) a social security number;
(2) driver's license or identification card number, passport number, military identification number or other similar number issued on a government document used to verify identity;
(3) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to access an individuals' financial account;
(4) And information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
(5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

(b) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include information about an individual that has been made publicly available by a federal, state or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

"**Superintendent"** means the Superintendent or designated individual or department.

"**Third-Party Agent**" means an entity that has been contracted to maintain, store, or process personal information on behalf of the School Board.

Notice of Security Breach

I. Individuals

A. The School Board directs the Superintendent to provide notice to each individual whose personal information was, or the Superintendent reasonably believes to have been, accessed as a result of a breach. Notice shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the Superintendent to determine the scope of the breach, to identify the individuals affected by the breach, and to restore the reasonable integrity of the data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred.

B. If a federal, state or local law enforcement agency, including the School Police, determines that notice to individuals would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. The law enforcement agency may, by a subsequent written request, revoke the delay as of a specified date or extend the period set forth in the original request.

C. Notice to the affected individuals is not required, if, after an appropriate investigation and consultation with relevant law enforcement agencies, the Superintendent reasonably determines that the breach has not and will not likely result in identity theft or other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least five (5) years.

D. The notice to an affected individual shall be made by written notice to the affected individual's mailing address, or by e-mail sent to the e-mail address of the affected individual.

E. The notice shall include, at a minimum:

(1) the date, estimated date, or estimated date range of the breach;
(2) a description of the personal information that was accessed or reasonably believed to have been accessed;
(3) a contact person and method that the individual can use to inquire about the breach and the personal information maintained about the individual; and
(4) information about the rights of parents or guardians of students who are under sixteen (16) years of age, incapacitated, or disabled, to request that the student's credit be frozen pursuant to Section 501.001, F.S.

F. The Superintendent may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $25,000, the number of affected individuals exceeds 500,000, or the School Board does not have an e-mail or mailing address for the affected individuals. The substitute notice must include a conspicuous notice on the School Board website and notice in print and to broadcast media including major media in urban and rural areas where the affected individuals reside.
G. Upon receiving notice of a breach of security of a system maintained by a third-party agent, the Superintendent shall notify all affected individuals according to the procedures in this section.

II. State and Credit Agencies

In addition to providing notice to the affected individuals according to the procedures above:

A. For any breach of security affecting 500 or more individuals in the state, the Superintendent must provide written notice of the breach to the Florida Department of Legal Affairs in accordance with the requirements in Section 501.171, F.S.
B. For any breach of security affecting 1000 or more individuals at a single time, the Superintendent must notify, without reasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution and content of the notices.

Security Freeze on Student Credit

Pursuant to Section 501.0051, F.S., parents or guardians of students who are under 16, incapacitated, or disabled, may have a security freeze placed on the student's credit in the event of a breach of security of personal information. The parent or guardian must submit a request to the consumer reporting agency with proof of authority and identification and pay a fee not to exceed $10 to secure and/or remove the freeze. However, no fee is required if the parent or guardian has documentation showing that the individual has been the victim of identity theft.

Upon request of a parent or guardian of a student under 16 years of age, incapacitated or disabled, who has been the victim of identity theft, the Superintendent shall provide documentation that is within the care, custody or control of the School Board sufficient to invoke the fee waiver under the law. This documentation may be a copy of a valid investigative report, an incident report, or a complaint with a law enforcement agency about the unlawful use of the protected consumer's identifying information by another person.

In addition, the Superintendent shall annually provide parents and guardians of students younger than 16 years of age, disabled, or incapacitated information regarding their rights under this law.

Enforcement

Violations of this policy could result in substantial civil penalties and subject employees to disciplinary action for failure to comply.

The provision of notice and information pursuant to this policy is not an admission that the information breach was caused by the School Board either directly or indirectly. This policy does not create a private cause of action against violators.

F.S. 501.171, 501.0051

~~BIOMETRIC INFORMATION~~ COLLECTION OF PERSONAL INFORMATION ~~RESTRICTIONS AND PRIVACY PROTECTIONS~~

Collection and retention of information on the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student, is prohibited. ~~The use of biometric technologies in the District and schools is prohibited unless it is specifically recommended by the Superintendent and approved by the School Board and determined to be in the best interest of the District or school.~~

Definition

Biometrics information means information collected from the electronic measurement or evaluation of any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty. Examples of biometric information include, but are not limited to, a fingerprint or hand scan, a retina or iris scan, a voice print, or a facial geometry scan. This definition does not include information collected from parents for screening purposes to serve as school volunteers and chaperones pursuant to Policy 2430.01, *School Volunteers*. ~~.is the measurement and analysis of unique physical or behavioral characteristics as a means of verifying personal identity. Biometric information includes, but is not limited to, fingerprints, hand geometry, voice or facial recognition, or iris or retinal scans.~~

~~Collection and Use of Biometric Information~~

~~Biometric information may only be collected and used under the following conditions:~~

~~A. The Superintendent shall determine which schools or departments, if any, may use biometrics based on efficiency and accountability needs, historical success of biometric use in schools and other public agencies, ability to implement the biometric technology system, resource availability and budgetary constraints.~~

~~B. Biometric information shall only be approved for use in identification or fraud prevention.~~

~~C. Written permission to collect or use specific student biometric information shall be annually obtained from the student's parent of record, or the student if eighteen (18) years old or older, before collection or use of any biometric information can take place.~~

~~D. Use of student biometric information shall be discontinued immediately when a student transfers to another school, withdraws from the school or District, graduates, or the parent or student if eighteen (18) or older, requests in writing to discontinue participation. Transfer students and students returning to the District must specifically re-enroll in the program in writing in order for the new school to collect or use biometric information.~~

~~E. Biometric identification information shall be exempt from disclosure under (1) the public records exemption in F.S. 119.07(5)(g)1, and must be destroyed within ninety (90) days after the student is no longer registered in school, or (2) as student records under Board Policy 8330, State and Federal law which must be maintained according to the appropriate records retention law.~~

~~F. An opt-in form adopted by the District will be used to inform parents and manage participation in any District approved biometric program. The Superintendent shall develop a parental consent form that is specific to the type of biometric information being collected and complies with this policy.~~

~~G. If a student is not participating in the program, the District will make available a different form of identification for that child. Failure to provide written consent to participate shall not be the basis for denial of any services otherwise available to the student.~~

~~H. Biometric information shall not be sold, leased or traded to any other entity, including government agencies.~~

~~**Collection of Student Information by Vendors and Other Third Parties**~~

~~Vendors are prohibited from collecting biometric information unless recommended by the Superintendent and approved by the Board pursuant to a written agreement that requires the vendor to specifically comply, at a minimum, with all of the criteria and standards in this policy.~~

~~**Privacy Standards**~~

~~All District officials, employees and vendors shall keep biometric information confidential at all times and may only disclose it with approval of the Superintendent pursuant to Board policy and law. The Superintendent shall develop processes and procedures to protect biometric information and ensure that it is only used in accordance with this policy. These standards, requirements and~~

~~responsibilities apply to all persons with access to District biometric information and shall include, but are not limited to, the following:~~

~~A. All biometric information must be kept secure and confidential.~~

~~B. Biometric information must be maintained in a secure environment with access restricted to a minimum of specifically authorized employees who need access to perform their daily responsibilities.~~

~~C. Biometric information must be protected against fraud, unauthorized use or other compromise.~~

~~D. Disclosure of biometric information is prohibited unless approved by the Superintendent pursuant to law and this policy.~~

~~**Training and Compliance**~~

~~The Superintendent shall provide training on the collection and use of biometric information to any employee that will have access to such information. An employee's failure to comply with this policy or the administrative procedures may result in discipline up to and including termination. Any violation by a vendor will be considered a breach of contract and could subject the vendor to debarment pursuant to Board Policy 6320.04.~~

F.S. ~~119.071(5)(g)~~1002.222, F.S.

Adopted 1/15/14

SCHOOL VOLUNTEERS

Providing opportunities for students to participate in appropriate co-curricular and extra-curricular activities enhances their education. Community members who have special knowledge and skills that add to the District's program are an excellent resource for these activities. Principals are authorized to contact local businesses and government agencies to recruit mentors. Employees of the District are also encouraged to volunteer.

Activities recommended by or involving community volunteers in an instructional role should be aligned with District philosophy and assist students to accomplish the District's learning goals. The following policies and guidelines are designed to provide for student and staff safety and an environment that maximizes community and parent resources.

A. Notwithstanding the restrictions in Policy 8332, *Collection of Personal Information*, regarding collection of information from parents, Aall volunteers must successfully complete the registration and background check process in administrative policies annually approved by the Superintendent. If significant changes occur in the background check process, the School Board will be notified by the Superintendent. Volunteers must report any criminal proceedings, including those which may occur after a background check, to school authorities immediately. The District's Employment Standard applies to all volunteers.

B. Once approved, all volunteers must sign in and out at a designated location in the school before proceeding to their volunteer site.

C. All volunteers must have identification and wear an identifying badge whenever volunteering.

1. Volunteers shall serve as positive role models. A school volunteer must always:

a. use appropriate language;

b. discuss age-appropriate topics;

c. refrain from inappropriately touching students;

d. refrain from disciplining students (behaviors needing discipline must be referred to the appropriate teacher or staff member);

e. Refrain from giving students gifts, rewards, or food items of any kind without the teacher's permission.

2. Volunteers shall not bring preschoolers or children not registered in the school.

3. Volunteers may not be left alone to supervise students. The visual and auditory presence of a District employee must be maintained at all times.

4. Volunteers must keep confidential any information about a student or any school-related incident. If there is a safety concern or an emergency issue, it must immediately be communicated to someone in authority.

5. Volunteers should notify the front office if an illness or emergency prohibits them from attending a scheduled volunteer shift. Volunteers should be prompt and dependable.

6. Volunteers should be dressed appropriately at all times.

7. Volunteers, under the supervision of the school volunteer liaison, should maintain a sign in sheet for volunteer activities and service. If service is provided after school or in the evenings, the beginning-ending time frame of the activity should be written. This record sheet should be submitted to the School Volunteer Liaison during the next visit to the worksite.

8. Certain volunteer activities require training and are subject to a fingerprint level 2 background check. Please refer to the District's web site for specific policies and procedures.

9. Volunteers and staff members must comply with Board policies regarding ethical conduct and student welfare.

10. Each school principal or work site supervisor may set additional procedures with respect to volunteer involvement. A volunteer's service may be terminated at any time, either at the discretion of the Principal, work site administrator, or the volunteer.

F.S. 1012.01(5)
F.A.C. 6A-1.0502