Office of Superintendent of Schools
Board Meeting of October 16, 2024

October 2, 2024

Office of the General Counsel
Walter J. Harvey, General Counsel

SUBJECT: **FINAL READING: PROPOSED AMENDMENTS TO SCHOOL BOARD POLICY 8351, *ELECTRONIC DATA SECURITY BREACH NOTICE REQUIREMENTS***

COMMITTEE: **ACADEMICS, INNOVATION, EVALUATION & TECHNOLOGY**

LINK TO STRATEGIC PLAN: **SAFE, HEALTHY, & SUPPORTIVE LEARNING ENVIRONMENTS**

Consistent with the Board's responsibility to periodically review and update its policies to conform to legislative changes, authorization is requested to amend Policy 8351, *Electronic Data Security Breach Notice Requirements*. This policy is proposed for amendment in response to 2023 Florida Senate Bill 262 ("S.B. 262"), which, as of July 1, 2024, revised the definition of "personal information" to include biometric data and geolocation.

In accordance with SB 262, Policy 8351 would be revised to require the Superintendent to take reasonable measures to protect any biometric data or geolocation information in the District's possession and to notify individuals or their legal representatives if such information is accessed through an electronic security breach. The policy would also be revised to incorporate legislative changes surrounding credit freezes in the event of a security breach.

The Notice of Intended Action was published in the Miami Herald on September 16, 2024, and posted in various places for public information and mailed to various organizations representing persons affected by the adopted and amended Board policies and individuals requesting notification. The time to request a hearing or protest the adoption and amendment of these policies has elapsed.

The policy amendments were drafted in collaboration with, and reviewed by the Superintendent, Cabinet, and District staff. The Notice of Intended Action and policy with strikethroughs and underlines are attached.

RECOMMENDED: That The School Board of Miami-Dade County, Florida, amend School Board Policy 8351, *Electronic Data Security Breach Notice Requirement,* and authorize the Superintendent to file the policy with The School Board of Miami-Dade County, Florida, to be effective October 16, 2024.

G-3

NOTICE OF INTENDED ACTION

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA, announced on September 11, 2024, its intention to amend Policy 8351, *Electronic Data Security Breach Notice Requirements*, at its meeting of October 16, 2024.

PURPOSE AND EFFECT: Policy 8351, *Electronic Data Security Breach Notice Requirements*, is proposed for amendment in response to 2023 Florida Senate Bill 262 ("S.B. 262").

SUMMARY: Policy 8351, *Electronic Data Security Breach Notice Requirements*, is proposed for amendment pursuant to S.B. 262 to require the Superintendent to take reasonable measures to protect any biometric data and geolocation information in the District's possession and to notify individuals or their representatives if such information is accessed through a security breach. The policy would also be revised to incorporate legislative changes surrounding credit freezes in the event of a security breach.

SPECIFIC LEGAL AUTHORITY UNDER WHICH RULEMAKING IS AUTHORIZED: Fla. Stat. ss. 1001.41 (1), (2), (5); 1001.43(10).

LAWS IMPLEMENTED INTERPRETED OR MADE SPECIFIC: Fla. Stat. ss. 501.0051, 501.171.

IF REQUESTED, A HEARING WILL BE HELD DURING SCHOOL BOARD MEETING OF October 16, 2024, 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 October 8, 2024, 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 AMENDED POLICY 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.

Book	Policy Manual
Section	October 16, 2024 - Final Reading
Title	**ELECTRONIC DATA SECURITY BREACH NOTICE REQUIREMENTS**
Code	8351
Status	Final Reading

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.

I. **Definitions**

A. **"Biometric data"** means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs; video or audio recordings or data generated from video or audio recordings; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (HIPPA).

~~A.~~ **""Breach of security"""** or **""breach"""** means unauthorized access of data in electronic form containing personal information belonging to Board members, employees, parents and students. Good faith access ~~of~~ to 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.

B.

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

C.

D. ~~"~~"**Personal information**"~~"~~ means:

~~A.~~1. A~~a~~n 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:

~~a.~~ a social security number;

a.

~~1.~~b. 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;

~~2.~~c. 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;

~~3.~~d. information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; ~~or~~

e. an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; ~~.~~

f. an individual's biometric data; or

~~4.~~g. any information regarding an individual's geolocation.

~~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.

3. ~~The~~ This 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.~~

E. ~~"~~"**Third-party agent**~~"~~" means an entity that has been contracted to maintain, store, or process personal information on behalf of the Board.

II. Notice of Security Breach

A. Notice to Individuals

~~1.~~ The 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 thirty (30) days after the determination of a breach or reason to believe a breach occurred.

1.

~~2.~~ 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.

2.

~~B.~~3. 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~~This determination must be documented in writing~~ and maintained for at least five (5) years~~, submitted to the Florida Department of Legal Affairs within thirty (30) days, an maintained for at least five (5) years.~~.~~

~~1.~~ 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.

4.

~~C.~~5. ~~The n~~Notices to affected individuals shall include, at a minimum:

~~a.~~ the date, estimated date, or estimated date range of the breach;

a.

~~b.~~ a description of the personal information that was accessed or reasonably believed to have been accessed;

b.

~~c.~~ a contact person and method that the individual can use to inquire about the breach and the personal information maintained about the individual; and

c.

~~2.~~d. 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 F.S. 501.0051.

~~3.~~ 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 $250,000, the number of affected individuals exceeds ~~$~~500,000, or the Board does not have an e-mail or mailing address for the affected individuals. The substitute notice must include a conspicuous notice on the Board website and notice in print and to broadcast media including major media in urban and rural areas where the affected individuals reside.

6.

~~D.~~7. 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.

B. Notice to State and Credit Agencies

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

~~1.~~ 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 F.S. 501.171(3).

1.

~~A.~~2. For any breach of security affecting 1,000 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. 1681a(p), of the timing, distribution and content of the notices.

III. Security Freeze on Student Credit

~~A.~~ Pursuant to F.S. 501.0051, parents or guardians of students who are under sixteen (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~~.

A.

~~B.~~ Upon request of a parent or guardian of a student under sixteen (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 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.

B.

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

IV. Enforcement

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

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

Legal References:
F.S. 501.0051
F.S. 501.171
F.S. 501.702
~~, 501.0051~~

Adoption Date: 01.14.2015