

Shelter Island School Board of Education
Monday, June 9, 2025
Executive Session at 5:00 pm
Public Budget Hearing & Regular Meeting at 6:00 pm
Conference Room

Kathleen M. Lynch, President * Katherine Rossi-Snook, Vice President
Margaret Colligan Dawn Hedberg Tracy McCarthy Karina Montalvo Anthony J. Rando

1. Call to Order

2. Executive Session – *It is expected that the Board of Education will enter Executive Session prior to this scheduled public meeting to discuss the employment of particular individuals in the district.*

3. Pledge of Allegiance

4. Shelter Island School Mission Statement – Engage, Explore, Empower

The following statement will be read:

We want our students to cherish our small Island community while applying and expanding their learning about, understanding of, and engagement with the wider world. To do this they must be: ethical and moral individuals; respectful and responsible communicators; creative and analytical thinkers; knowledgeable and literate readers, writers, mathematicians and scientists; participants in and audiences for art, drama, music, athletics, and other artistic, cultural, and social activities; skilled and successful workers and consumers; and committed and active citizens.

5. Public Budget Hearing

5.1 School Budget (Revote) 2025-2026

- a. Brief Budget Overview – Dr. Brian Doelger
- b. Public will have an opportunity to ask questions regarding the School Budget for the 2025-2026 school year.

6. Visitor Questions (Specific to the agenda)

7. Consent Agenda – The Board President requests a motion to approve and/or accept the following agenda items:

7.1 Approval of Minutes

- a. Public Budget Hearing/Regular Meeting of May 12, 2025
- b. Annual District Meeting and Election of May 20, 2025
- c. Executive Session of May 22, 2025
- d. Budget Revote Presentation of May 28, 2025
- e. Budget Revote Adoption Meeting of June 2, 2025

8. Correspondence - None

9. Student Liaison Report

10. Presentations

10.1 Presentations Not Requiring Board Approval

- a. Mr. Daniel Williams & Students - Our Year in Research
- b. May 2025 Employee of the Month – Mary Kanarvogel

11. Personnel - The Board President requests a motion to approve and/or accept the recommendations of the Superintendent on the following Personnel Action: 11.1 – 11.7

11.1 New Hire

- a. BE IT RESOLVED THAT: The Board of Education hereby approves Kathleen Springer, as 1.0 FTE PK-12 Music Teacher, effective September 1, 2025, at \$71,371, Step 1 MA of the 2025-2026 teacher salary scale with a four (4) year probationary period through September 1, 2029, in the tenure area of Music K-12.

BE IT FURTHER RESOLVED THAT: Ms. Springer must receive three (3) annual APPR composite ratings of Effective or Highly Effective, in at least three (3) preceding four (4) years and cannot have an APPR composite rating of Ineffective in the last year of her probationary appointment to be granted or considered for tenure.

11.2 Summer 2025 Extra Duty

- a. Lisa Goody to provide extra duty, as needed, between the period of June 30, 2025 and September 1, 2025, at a rate of \$16.50 per hour.
- b. Deborah Brewer to provide extra duty, as needed, between the period of June 30, 2025 and September 1, 2025, at a rate of \$16.50 per hour.

11.3 Extra Compensation

- a. Walter C. Brigham, III to provide computer support and supervision for the period of time between July 1, 2025 and September 1, 2025, at his daily rate.
- b. Carol Euring to provide training for the new Claims Auditor, for the period of July 1, 2025 through July 31, 2025, not to exceed at a rate of \$75 an hour.
- c. Alyssa Prior to provide guidance counseling services for the period of July 1, 2025 through August 29, 2025, not to exceed 10 days, at her daily rate.

11.4 Abolish Position

- a. BE IT RESOLVED that for purposes of economy, the Board of Education of the Shelter Island Union Free School District has determined to abolish one full-time position within the Elementary Teacher tenure area, effective June 30, 2025; and be it further

RESOLVED that Employee No. 1302, as the least senior Elementary Teacher, is hereby excessed from said position effective June 30, 2025; and be it further

RESOLVED that said excessed Elementary Teacher shall be placed on a preferred eligible list as per Education Law §3013.

11.5 Agreement

- a. Resolved, that the Board of Education of the Shelter Island Union Free School District, hereby approves an amendment to the employment contract of Deborah Vecchio, and authorizes the Board President to sign said agreement.

11.6 Resignation of Personnel

- a. Accept the resignation of Carol Euring, Claims Auditor, effective June 30, 2025.

11.7 Childcare Leave

- a. Approve a contractual childcare leave of absence for Erin Mulrain, Physical Education Teacher, to commence on or about September 2, 2025 through September 12, 2025; with said period credited towards the employee's FMLA leave of absence.

12. Program - The Board President requests a motion to approve or accept the recommendations of the Superintendent on the following Program Actions: 12.1 – 12.5

12.1 CPSE Recommendations for the 2024-2025 School Year

- a. Committee on Preschool Special Education

12.2 CPSE Recommendations for the Summer 2025

- a. Committee on Preschool Special Education

12.3 504/CSE/CPSE Recommendations for the 2025-2026 School Year

- a. 504 Committee
- b. Committee on Special Education
- c. Committee on Preschool Special Education

12.4 Second Reading and Possible Adoption of Policies

- a. Policy 5672 - Info Security Breach and Notification
- b. Policy 5676 - Privacy and Security

12.5 Approve Date of Re-Organizational Meeting

- a. Approve the Re-Organization Meeting date of Monday, July 14, 2025

13. Finance – The Board President requests a motion to approve and/or accept the recommendations of the Superintendent on the following Finance Actions: 13.1 – 13.4

13.1 Financial Reports

- a. Treasurer's Report – April 2025
- b. Extra Class Report – April 2025
- c. Appropriations Status Report
- d. Revenue Status Report
- e. Claim Auditor's Report – April 2025
- f. Payroll Audit Report – April 2025

13.2 Journal Entries

- a. Accept and approve the Journal Entry Reports for the period of May 6, 2025 through June 3, 2025, that in accordance with Board Policy, the Superintendent has approved.

13.3 Donation

- a. Authorize the Shelter Island School District to accept a donation of \$500 from Shelter Island PTSA, for ice cream; and authorize an increase to the budget line of A.2810.400.00.0000 in the same amount.

13.4 Budgetary Modifications

- a. BE IT RESOLVED THAT: The Board of Education of the Shelter Island Union Free School District hereby authorizes a budgetary modification/increase to the following budget lines in the amount, not to exceed:

A1325.160.00.0000 \$44,400.00

to be offset by the Reserve for Employee Benefit Accrued Liability Reserve (EBALR) pursuant to General Municipal Law Section 6-P, effective June 30, 2025.
- b. BE IT RESOLVED THAT: The Board of Education of the Shelter Island Union Free School District hereby authorizes a budgetary modification/increase to the following budget line in the amount, not to exceed:

A9090.802.00.0000 \$32,912.10

to be offset by the Unexpended Budget for the 2024-2025 school year.

14. Business – The Board President requests a motion to approve or accept the recommendations of the Superintendent on the following Business Actions: 14.1 – 14.2

14.1 Contracts

- a. BE IT RESOLVED, that the Board approve the Contract for Cooperative Educational Services between the Shelter Island School District and Eastern Suffolk BOCES in the amount of \$347,340.20, for the 2025-2026 school year in accordance with the terms and conditions set forth in said agreement; and authorize the Board President to execute said agreement.
- b. Approve the agreement between the Board of Education for the Shelter Island Union Free School District and Mattituck-Cutchogue Union Free School District for student services for the 2024-2025 school year; and authorize the Board President to execute said agreement.

14.2 Amend Private School Transportation

- a. Amend the motion May 12, 2025 from:

Approval to transport twenty-eight (28) students to the following private schools for the 2025-2026 school year:

- Ross School – East Hampton, NY (4 students)
- Hayground School – Bridgehampton, NY (7 students)
- Our Lady of the Hamptons - Southampton, NY (11 students)
- Peconic Community School - Cutchogue, NY (6 students)

to:

Approval to transport **thirty-one (31)** students to the following private schools for the 2025-2026 school year:

- Ross School – East Hampton, NY (4 students)
- Hayground School – Bridgehampton, NY (**9 students**)
- Our Lady of the Hamptons - Southampton, NY (11 students)
- Peconic Community School - Cutchogue, NY (**7 students**)

15. Facility – The Board President requests a motion to approve or accept the recommendations of the Superintendent on the following Facility Action: 15.1

15.1 Excessing of Equipment

a. Broken Television, repair cost exceeds replacement cost – Shelter Island Serial #20240047

16. Items for Consideration

a. Discuss *suggested* 2025-2026 School Board Meeting Dates (to be approved at the July 14, 2025 Re-org meeting)

August 25, 2025	November 10, 2025	February 9, 2026	May 11, 2026
September 15, 2025	December 8, 2025	March 16, 2026	May 19, 2026 (Tues. Budget Vote)
October 14, 2025	January 12, 2026	April 20, 2026	June 8, 2026

17. Old Business - None

18. Director of Athletics, Physical Education, Health, Wellness & Personnel Report

19. Assistant Superintendent Report - None

20. Superintendent Report

21. Board Member Reports

22. Visitor Comments

23. Adjournment

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The District values the protection of private information of individuals in accordance with applicable law and regulations. The District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

- a) "Personal information" means any information concerning a person which, because of name, number, symbol, mark, or other identifier, can be used to identify that person.
- b) "Private information" means either:
 - 1. Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:
 - (a) Social security number;
 - (b) Driver's license number or non-driver identification card number;
 - (c) Account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account;
 - (d) Account number, or credit or debit card number, if circumstances exist where the number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or
 - (e) Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity;
 - 2. A username or email address in combination with a password or security question and answer that would permit access to an online account.

Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- c) "Breach of the security of the system" means unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)**Determining if a Breach Has Occurred**

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the District may consider the following factors, among others:

- a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information;
- b) Indications that the information has been downloaded or copied;
- c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- d) System failures.

Notification Requirements

- a) For any computerized data owned or licensed by the District that includes private information, the District will disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures. Within 90 days of the notice of the breach, the New York State Office of Information Technology Services will deliver a report to the District on the scope of the breach and recommendations to restore and improve the security of the system.
- b) Notice to affected persons under State Technology Law is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the District reasonably determines the exposure will not likely result in the misuse of the information, or financial or emotional harm to the affected persons. This determination must be documented in writing and maintained for at least five years. If the incident affected over 500 New York State residents, the District will provide the written determination to the New York State Attorney General within ten days after the determination.
- c) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under certain laws and regulations, the District is not required to provide additional notice to those affected persons under State Technology Law. However, the District will still provide notice to the New York State Attorney General, the New York State Department of State, the New York State Office of Information Technology Services, and to consumer reporting agencies.

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

- d) For any computerized data maintained by the District that includes private information which the District does not own, the District will notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The required notification will be made after the law enforcement agency determines that the notification does not compromise the investigation.

If the District is required to provide notification of a breach, including breach of information that is not private information, to the United States Secretary of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, it will provide notification to the New York State Attorney General within five business days of notifying the United States Secretary of Health and Human Services.

Methods of Notification

The required notice will be directly provided to the affected persons by one of the following methods:

- a) Written notice;
- b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form and a log of each notification is kept by the District when notifying affected persons in electronic form. However, in no case will the District require a person to consent to accepting the notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;
- c) Telephone notification, provided that a log of each notification is kept by the District when notifying affected persons by phone; or
- d) Substitute notice, if the District demonstrates to the New York State Attorney General that the cost of providing notice would exceed \$250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice will consist of all of the following:
 - 1. Email notice when the District has an email address for the subject persons;
 - 2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and
 - 3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice will include:

- a) Contact information for the notifying District;

(Continued)

Non-Instructional/Business
Operations**SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)**

- b) The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and
- c) A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, accessed or acquired.

In the event that any New York State residents are to be notified, the District will notify the New York State Attorney General, New York State Department of State, and New York State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. This notice will be made without delaying notice to affected New York State residents.

In the event that more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content, and distribution of the notices and approximate number of affected persons. This notice will be made without delaying notice to affected New York State residents.

A list of consumer reporting agencies will be compiled by the New York State Attorney General and furnished upon request to any district required to make a notification in accordance with State Technology Law.

State Technology Law §§ 202 and 208

Adoption Date:

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The Board of Education recognizes its responsibility to enact policies that provide privacy for student, teacher and principal data in accordance with law. This is particularly relevant in the context of the administration of student data which is collected, surveys that collect personal information, the disclosure of personal information for marketing purposes, and in conducting physical exams.

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

- a) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
- b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.
- c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.
- d) "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.
- e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
- f) "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
- g) "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

- h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).
- i) "Eligible student" means a student who is eighteen years or older.
- j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).
- k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.
- l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.
- m) "Parent" means a parent, legal guardian, or person in parental relation to a student.
- n) "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).
- o) "Release" has the same meaning as disclosure or disclose.
- p) "Student" means any person attending or seeking to enroll in an educational agency.
- q) "Student data" means personally identifiable information from the student records of an educational agency.
- r) "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.
- s) "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not-for-profit corporation or other

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

nonprofit organization, other than an educational agency.

- t) "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the District will take steps to minimize its collection, processing, and transmission of PII. Additionally, the District will:

- a) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.
- b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

Except as required by law or in the case of educational enrollment data, the District will not report to NYSED the following student data elements:

- a) Juvenile delinquency records;
- b) Criminal records;
- c) Medical and health records; and
- d) Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the District.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

The Chief Privacy Officer has the power, among others, to:

- a) Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and
- b) Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the District to perform a privacy impact and security risk assessment.

Data Protection Officer

The District has designated a District employee to serve as the District's Data Protection Officer. The Data Protection Officer for the District is: Mr. Walter Brigham.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities. Additionally, some aspects of this role may be outsourced to a provider such as a BOCES, to the extent available.

District Data Privacy and Security Standards

The District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

- a) Describe their current cybersecurity posture;
- b) Describe their target state for cybersecurity;
- c) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- d) Assess progress toward the target state; and
- e) Communicate among internal and external stakeholders about cybersecurity risk.

The District will protect the privacy of PII by:

- a) Ensuring that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

1. Improve academic achievement;
 2. Empower parents and students with information; and/or
 3. Advance efficient and effective school operations.
- b) Not including PII in public reports or other public documents.

The District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

The District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

Third-Party Contractors**District Responsibilities**

In addition, the District will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the District.

The third-party contractor's data privacy and security plan must, at a minimum:

- a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with District policy;
- b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;
- c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);
- d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;
- e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;
- f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

- g) Describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and
- h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the District under which the third-party contractor will receive student data or teacher or principal data from the District, is required to:

- a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;
- b) Comply with District policy and Education Law Section 2-d and its implementing regulations;
- c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);
- d) Not use the PII for any purpose not explicitly authorized in its contract;
- e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:
 - 1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the District; or
 - 2. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;
- f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;
- g) Use encryption to protect PII in its custody while in motion or at rest; and
- h) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)Cooperative Educational Services through a BOCES

The District may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from the District under all circumstances.

For example, the District may not need its own contract or agreement where:

- a) It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and
- b) That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the District's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from the District is received by a third-party contractor pursuant to a CoSer, the District will consult with the BOCES to, among other things:

- a) Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the District's use of a third-party contractor's product or service under a particular CoSer;
- b) Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;
- c) Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from the District pursuant to a BOCES contract; and
- d) Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the District receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the District pursuant to a BOCES contract.

Click-Wrap Agreements

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

District staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Privacy Officer or designee.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The Bill of Rights will contain all required elements including supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District. The supplemental information must be developed by the District and include the following information:

- a) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- b) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- c) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- d) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- e) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- f) Address how the data will be protected using encryption while in motion and at rest.

The District will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the District under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the District in a manner prescribed by the District.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

The District will ensure that only authorized individuals are able to inspect and review student data. To that end, the District will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the District and not to a third-party contractor. The District may require that requests to inspect and review education records be made in writing.

The District will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the District through its annual FERPA notice. A notice separate from the District's annual FERPA notice is not required.

The District will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The District may provide the records to a parent or eligible student electronically, if the parent consents. The District must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the District about breaches or unauthorized releases of student data and/or teacher or principal data:

- a) All complaints must be submitted to the District's Data Protection Officer in writing.
- b) Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.
- c) Following the investigation of a submitted complaint, the District will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the District.
- d) If the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other District staff.

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies.

Reporting a Breach or Unauthorized Release

The District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, District policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than 30 days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

**SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND
PRINCIPAL DATA (Cont'd.)**

- a) Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years;
- b) Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years;
- c) Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or
- d) Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was in advertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

The District will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the District or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the District will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;
- b) A description of the types of PII affected;
- c) An estimate of the number of records affected;

**SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND
PRINCIPAL DATA (Cont'd.)**

- d) A brief description of the District's investigation or plan to investigate; and
- e) Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the District for the full cost of this notification.

Annual Data Privacy and Security Training

The District will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

Notification of Policy

The District will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121

Adoption Date: 01/11/2021
Revised: