INFORMATION AND DATA PRIVACY, SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened State's concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur that result in the unauthorized disclosure (or acquisition by an unauthorized person of) an individual's private information. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Protection Officer is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, the target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate the Director of Technology and Learning Systems as the district's Data Protection Officer to be responsible for the implementation of the policies and procedures required in Section 2D of Education Law and its accompanying regulations, and to serve as the point of contact for data security and privacy district. The Board may change this designation by adoption of a resolution making a new designation at the annual reorganizational meeting or any other meeting.

To this end, the Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel and the Data Protection Officer, to establish regulations which address:

- the identification and/or definition of the types of private information that is to be kept secure, which for purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

- the protections of "personally identifiable information" of student and teachers/principal under Section 2-d of New York Education Law and Part 121 of the New York Commissioner of Education;

- the protections of "private information" under Section 208 of New York State Technology Law and the New York SHIELD Act;

- the procedures to prevent any possible breaches of security that may result in the unauthorized release of private information; and

- the procedures to notify persons affected by ~~the security~~ breaches or unauthorized access of protected information as required by law.

I. Student and Teacher/Principal "Personally Identifiable Information" under Section 2-d of New York Education Law

A. General Provisions

Personally Identifiable Information (PII) as applied to student data is as defined in Family Educational Rights and Privacy Act, which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Sections 3012-c and 3012-d of New York Education Law, except where required to be disclosed under state law and regulations.

The Data Protection Officer will see that every use and disclosure of personally identifiable information (PII) by the district benefits students and the district (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). However, PII will not be included in public reports or other documents.

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed and its retention period has expired.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in Policy 5500, Student Records, and its accompanying regulation 5500-R.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security, which is published on the district's website at https://www.somersschools.org/ and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors, who will receive from the district student and/or teacher or principal data protected by Section 2-d of New York Education Law, will require that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
   a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
   b. unless required by statute or court order and the third-party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party

contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors, who will receive from the district student and/or teacher or principal data protected by Section 2-d of New York Education Law, include the third-party contractor's data security and privacy plan that is acceptable to the district. At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of the Regulations of the New York Commissioner of Education;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;
7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

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 or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation, or cause further disclosure of PII by disclosing an unfixed security vulnerability, 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.

The Superintendent, in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

II. "Private Information" under State Technology Law §208

"Private information" is defined in Section 208 of the State Technology Law, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Additionally, pursuant to Section 203-d of New York Labor Law, the district will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, and driver's license number. In addition, the district will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed; be printed on any ID badge; card or time card; be placed in files with unrestricted access; or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of private or personal identifying information maintained by the district shall be promptly reported to the Superintendent and the Board of Education.

Ref: State Technology Law §208
Labor Law §203-d
Education Law §2-d
8 NYCRR Part 121

Cross-ref: 1120, District Records
5500, Student Records

Adoption date: April 29, 2008
Revised: November 18, 2014
Reviewed: October 29, 2019
Revised: June 16, 2020