8635

(X) Required
( ) Local
( ) Notice

Data Privacy and Security Policy

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Data Privacy Officer is responsible for ensuring the districts systems follow NIST CSF and adopt technologies, safeguards and practices that align with it. This will include an assessment of the districts current cybersecurity state, its target future cybersecurity state, opportunities for improvement, progress toward the target state and communication about cyber security risk.

The Board will designate a Data Privacy Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy in the district.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Privacy Officer (where applicable) to establish regulations that address:

- the protections of personally identifiable information (PII) of student and teacher/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of private information under State Technology Law §208 and the NY SHIELD Act; and § General Business 899-bb; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal Personally Identifiable Information under Education Law §2-d

A. General Provisions

PII as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500), 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 Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Privacy Officer will ensure that every use and disclosure of PII by the district benefits students and the district (e.g., improves academic achievement, empowers parents and students with information, and/or advances 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.

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 and regulation 5500, Student Records.

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 Parents Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the districts website at www.dfsd.org/Page/1121 and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and regulation 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 districts 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/guardian 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 while in motion or at rest; 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 contractors 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 breachs discovery.

C. Third-Party Contractors Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractors data security and privacy plan. This plan must be accepted by 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 Commissioners Regulation regarding the contractual supplement to the Bill of Rights;

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 PII is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate PII 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 districts 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 districts information storage or computerized data that compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Privacy Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Privacy Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the States 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 Privacy 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 State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, that 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.

Any breach of the districts information storage or computerized data that compromises the security, confidentiality, or integrity of private information maintained by the district must be promptly reported to the Superintendent and the Board of Education.

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

- 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

Pursuant to Labor Law §203-d, the district will not communicate employee personal identifying information to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parents surname prior to marriage; and
6. drivers license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

IV. SHIELD Act Security Requirements under General Business Law § 899-bb

The District shall maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information regarding persons as defined in General Business Business Law § 899-aa, including but not limited to the disposal of such data as describer in General Business Law § 899-bb(2).

Cross-ref: 1120, District Records
5500, Student Records
8630, Computer Resources and Data Management

Ref: State Technology Law §§201-208
Labor Law §203-d
Education Law §2-d
8 NYCRR Part 121

Adoption date: May 26, 2020