Book: Policy Manual
Section: 6000: Students
Title: Data Security and Privacy Policy
Number: 6320-a
Status: Active
Adopted: March 30, 1993
Last Revised: June 3, 2020
Last Reviewed: May 21, 2020

Definitions:

1. Protected Data means personally identifiable data of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d.

Requirements:

1. Publication: This policy shall be published on the District's website and notice of the policy provided to all officers and employees of the District.
2. The District shall provide the data protection as well as the protection of parent and eligible student's rights and rights to challenge the accuracy of such data required by FERPA (20 USC §1232g), IDEA (20 USC §1400 et. seq.) and any implementing regulations.
3. The District hereby adopts the National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF) in accordance with the Commissioner's Regulations.
4. Every contract or other written agreement with a third party contractor under which the third party contractor will receive protected student data or teacher or Principal data shall include a data security and privacy plan that outlines how all State, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with this policy.
5. Nothing contained in this policy or the District's Data Security and Privacy Plan shall be construed as creating a private right of action against the District.
6. Every use and disclosure of personally identifiable information, as defined by FERPA, shall be for the benefit of students and the educational agency. Examples of such benefit are provided in implementing regulations.
7. The District shall not sell or disclose for marketing or commercial purposes any Protected Data, or facilitate its use of disclosure by any other party for any marketing or commercial purpose, or permit another party to do so.
8. The District shall take steps to minimize its collection, process and transmission of Protected Data.
9. Except as required by law or in the case of enrollment data, the District shall not report to NYSED Juvenile Delinquency records, criminal records, medical health records, or student biometric information.
10. All contracts with vendors that have access to Protected Data shall comply with NIST Cybersecurity Framework.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The District, in compliance with Education Law §2-d, provides the following:

DEFINITIONS:

As used in this policy, the following terms are defined:

Student Data means personally identifiable information from the student records of a District student.

Teacher or Principal Data means personally identifiable information from District records 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 §§3012-c and 3012-d.

Third-Party Contractor means any person or entity, other than a District, that receives student data or teacher or Principal data from the District pursuant to a contract or other written agreement for purposes of providing services to the District, including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student or teacher or Principal data from a school district to carry out its responsibilities pursuant to Education Law §211-e and is not a District, and a not-for-profit corporation or other nonprofit organization, other than a District.

1. Neither student data, nor teacher or Principal data will be sold or released for any commercial purpose;

2. Parents have the right to inspect and review the complete contents of their child's education records;

3. Security protocols regarding confidentiality of personally identifiable information are currently in place and the safeguards necessary to protect the confidentiality of student data are maintained at industry standards and best practices. The safeguards include, but are not limited to, encryption, firewalls, and password protection. As required by Education Law §2-d (5), the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or NIST CSF) is adopted as the standard for data security and privacy;

4. New York State maintains a complete list of all student data collected by the State and the data is available for public review at: http://www.p12.nysed.gov/irs/sirs/NYSEDDataElements2018.xlsx, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234;

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the BOCES' Data Protection Officer, at TSTBOCES.org**;**

6. The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect personally identifiable information;

- Following its investigation of a submitted complaint, the District shall provide the parent or eligible student with its findings within a reasonable period but no more than 60 calendar days from receipt of the complaint;

- Where the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District shall provide the parent or eligible student with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint;

- The District will require complaints to be submitted in writing;

- 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, including the Records Retention and Disposition Schedule ED-1;

7. This policy will be regularly updated with 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. The supplemental information must be developed by the District and include the following information:

- 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;

- 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 State and federal laws and regulations (e.g., FERPA; Education Law §2-d);

- 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 whether, when and how the data will be destroyed);

- 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;

- where the student data or teacher or Principal data will be stored, it will be described in such a manner as to protect data security and the security protections taken to ensure that such data will be protected and data security and privacy risks mitigated; and how the data will be protected using encryption while in motion and at rest will be addressed.

8. This policy shall be published on the District's website. This policy shall also be included with every contract the District enters with a third party contractor where the third party contractor receives student data or teacher or Principal data.

DATA PRIVACY RIDER FOR ALL CONTRACTS INVOLVING PROTECTED DATA PURSUANT TO EDUCATION LAW §2-C AND §2-D

District and Vendor agree as follows:

1. Definitions:

(1) Protected Data means personally identifiable information of students from student education records as defined by FERPA, as well as teacher and Principal data regarding annual professional performance reviews made confidential under New York Education Law §3012-c and §3012-d;

(2) Personally Identifiable Information (PII) means the same as defined by the regulations

implementing FERPA (20 USC §1232-g);

2. Confidentiality of all Protected Data shall be maintained in accordance with State and Federal Law and the District's Data Security and Privacy Policy;

3. The Parties agree that the District's Parents' Bill of Rights for Data Privacy and Security are incorporated as part of this agreement, and Vendor shall comply with its terms;

4. Vendor agrees to comply with Education Law §2-d and its implementing regulations;

5. Vendor agrees that any officers or employees of Vendor, and its assignees who have access to Protected Data, have received or will receive training on federal and State law governing confidentiality of such data prior to receiving access;

6. Vendor shall:

(1) limit internal access to education records to those individuals that are determined to have legitimate educational interests;

(2) not use the education records for any other purposes than those explicitly authorized in its contract. Unauthorized use specifically includes, but is not limited to, selling or disclosing personally identifiable information for marketing or commercial purposes or permitting, facilitating, or disclosing such information to a third party for marketing or commercial purposes;

(3) except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information to any other party:

> (i) without the prior written consent of the parent or eligible student; or
>
> (ii) unless required by statute or court order and the party provides notice of the disclosure to the department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(4) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

(5) use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law §111-5;

(6) adopt technology, safeguards and practices that align with NIST Cybersecurity Framework;

(7) impose all the terms of this rider in writing where the Vendor engages a subcontractor or other party to perform any of its contractual obligations which provides access to Protected Data.

Adopted Addendum, 6320-a: July 2, 2014
Complete Revision: April 1, 2020
Revision Date: June 3, 2020