NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

co-sponsored by

NEW YORK STATE OF OPPORTUNITY. Office of General Services

How Your Contract Can Meet School & Vendor Responsibilities for Protecting Student Information

SAMPO NIGP CHAPTER

SUNY

Boards of Cooperative Educational Services BOCES of NEW YORK STATE

May 4 & 5, 2022

David Pellow
Labor Relations Specialist
Madison-Oneida BOCES

Amanda Palmer
Assistant Director
Mohawk Regional Information Center

THESE ARE YOUR STUDENTS

Evolution of Legal Requirements

FERPA
FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT

1974

COPPA
CHILDREN'S ONLINE PRIVACY PROTECTION ACT

1998

ED LAW 2-D EFFECTIVE

2014

PART 121 EFFECTIVE

2020

NEW YORK STATE OF OPPORTUNITY. | NY GovBuy

Evolution of Legal Requirements

- **FERPA**
  - Enforced by US DOE
  - Defines student “personally identifiable information” (PII)
  - Defines “educational record”
  - Requires consent before disclosure
    - Exception: “directory information”
    - Exception: “school official with a legitimate educational interest”
  - Written agreements required for certain sharing

Evolution of Legal Requirements

- **COPPA**
  - Enforced by FTC
  - Regulates operators of commercial websites and online services that collect personal information from children under the age of 13
  - Requires operators to obtain verifiable parental consent before collecting a child's personal information
  - Guidance (not statue on regulations) states that schools can provide consent in certain circumstances
  - Vendors typically use master agreement language that obligates educational agencies to collect consents

Evolution of Legal Requrements

- **Ed Law 2-d**
  - "Unauthorized Release of Personally Identifiable Information"
  - 4 key concepts:
    - Personally Identifiable Information
    - Educational Agency
    - Third Party Contractor
    - Disclose

Ed Law 2-d

- Personally Identifiable Information
  - Student PII (student data)
    - FERPA definition
    - But no exceptions for Directory Information
  - Teacher or Principal PII
    - Basically, APPR ratings

Ed Law 2-d

- Educational Agency
  - School districts, BOCES, NYSED
  - NOT higher education
  - If an educational agency shares PII with another educational agency, Education Law 2-D does not apply

Ed Law 2-d

- Third Party Contractor
  - Any entity that is not an educational agency, and
    - Receives student data or teacher or principal data from an educational agency
    - Pursuant to a written agreement
    - For purposes of providing services to such educational agency

NOTE: Accepting online terms of service creates a "written agreement"

Ed Law 2-d

- Third Party Contractor
  - No requirement that the service be paid with money
  - Not limited to digital exchanges of student data
  - Examples:
    - Google
    - iReady
    - Yearbook photographer
    - Physical therapists
    - Occupational therapists
    - SROs
    - School attorneys

Ed Law 2-d

- Disclose
  - Scope
    - “to permit access to” PII
    - “the release, transfer or other communication” of PII
    - “by any means, including oral, written, or electronic”
    - “whether intended or unintended”
  - Rule: an educational agency may not disclose PII in order to receive services unless the agreement to do so includes required contractual protections

Non-Procurement Obligations of Educational Agencies

Parent's Bill of Rights for Data Privacy & Security

- Posted on website
- Must include "supplemental information" about each contract

Data Security and Privacy Policy

- "aligned with" NIST Cybersecurity Framework
- Posted on website

Annual Employee Cybersecurity Training

Complaint Procedures

Incident (Breach) Reporting and Notification

Data Protection Officer

Prohibitions on Commercial Use

- PII maintained by educational agencies shall not be sold or used for marketing purposes

Determination that the benefit to students or the educational agency justifies the risk of information sharing

Ed Law 2-d: Contract Requirements

- Require the confidentiality of the shared student data be maintained in accordance with:
  - State and federal law
  - The educational agency's policy and data security policy
- The vendor's data security and privacy plan that contains the elements set forth in the regulations
  - Including a signed copy of the Parents Bill of Rights for Data Privacy and Security

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The data security and privacy plan outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the district/BOCES Policy on Data Security and Privacy.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies the administrative, operational and technical safeguards and practices the contractor has in place to protect personally identifiable information.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan demonstrates compliance with the supplemental information requirements.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies how the vendor's officers and employees who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies how the vendor's assignees (subcontractors) who have access to protected data will receive training on the federal and state laws governing confidentiality of the data prior to receiving access.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies if the contractor uses subcontractors and how it will manage any relationships and contracts to ensure personally identifiable information is protected.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies how the contractor will manage data security and privacy incidents, identify breaches and unauthorized disclosures, and promptly notify the agency.

Vendor Data Security and Privacy Plan Requirements

(8NYCRR 121.9)

The plan specifies whether, how and when data will be returned to the agency, transitioned to a successor contractor, or destroyed by the contractor when the contract is terminated.

Vendor Data Security and Privacy Plan Requirements

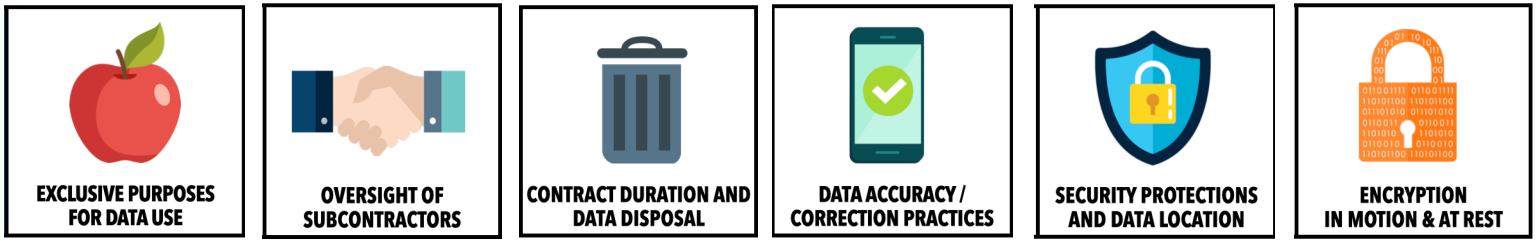
(8NYCRR 121.9)

The plan includes a signed copy of the district/BOCES Parents Bill of Rights for Data Privacy and Security.

Ed Law 2-d: Supplemental Information

(8NYCRR 121.9)

- Must be posted on website with Parents' Bill of Rights for Data Privacy and Security
- Must be "developed" by the educational agency and include:



- These elements should all be addressed in the vendor agreement

Ed Law 2-d: Third Party Contractor Obligations

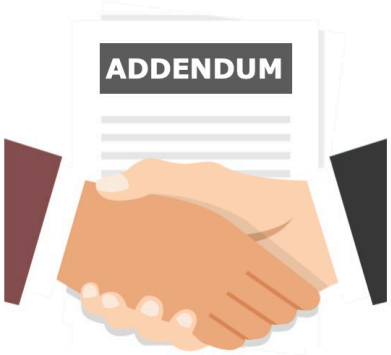
(8NYCRR 121.9)

- Eight (8) elements set forth in Regulation
- Recommended: contract language that recites these eight obligations and makes vendor's failure to comply a breach of contract
- Concern: language giving educational agency a contractual right to audit vendor

Contract Negotiation Challenges

- Other Contract Term Recommendations
  - NYS Law and venue
  - Funding out language (non-appropriation)
  - Warranty language similar to OGS
  - Bilateral indemnification
  - Expiration date of June 30th to match budget year
  - If automatic renewal, limits on price increases and notice of price increases by prior [date] for budgeting purposes

Resources



- RICOne website: https://riconedpss.org
- Sample Ed Law 2-d Addendum

Sample Ed Law 2-d Addendum

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. **Applicability of This Addendum**

The _____ School District ("DISTRICT") and ____ ("Vendor") are parties to a contract dated ____ ("the underlying contract") governing the terms under which DISTRICT accesses, and Vendor provides, [name of product(s) covered by contract] ("Product"). DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. **Definitions**

2.1 "Protected Information", 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 (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.

2.2 "Vendor" means [name of vendor identified above].

2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.

2.4 DISTRICT" means the _____ School District.

Sample Ed Law 2-d Addendum

2.5 “Parent” means a parent, legal guardian, or person in parental relation to a Student.
2.6 “Student” means any person attending or seeking to enroll in an educational agency.
2.7 “Eligible Student” means a student eighteen years or older.
2.8 “Assignee” and “Subcontractor” shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
2.9 “This Contract” means the underlying contract as modified by this Addendum.

3. **Vendor Status**

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. **Confidentiality of Protected Information**

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the DISTRICT Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

Sample Ed Law 2-d Addendum

5. **Vendor Employee Training**

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. **No Use of Protected Information for Commercial or Marketing Purposes**

Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. **Ownership and Location of Protected Information**

7.1 Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2 DISTRICT shall have access to the DISTRICT's Protected Information at all times through the term of this Contract. DISTRICT shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

Sample Ed Law 2-d Addendum

7.3 Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by DISTRICT or it authorized users, or performing any other data analytics other than those required to provide the Product to DISTRICT. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to DISTRICT upon request.

7.4 All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. **Purpose for Sharing Protected Information**

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.

9. **Downstream Protections**

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an “Assignee” of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

Sample Ed Law 2-d Addendum

10. **Protected Information and Contract Termination**

10.1 The expiration date of this Contract is defined by the underlying contract.

10.2 Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT.

10.3 Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4 Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5 To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify deidentified data and not to transfer de-identified data to any party.

10.6 Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. **Data Subject Request to Amend Protected Information**

11.1 In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

Sample Ed Law 2-d Addendum

11.2 Vendor will cooperate with DISTRICT in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. **Vendor Data Security and Privacy Plan**

12.1 Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2 Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;
b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;
c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy (Attachment B);
d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;
e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

Sample Ed Law 2-d Addendum

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and

i. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. **Additional Vendor Responsibilities**

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor’s obligations under this Contract or to the DISTRICT unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

Sample Ed Law 2-d Addendum

13.5 Vendor will 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 U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of 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; and

13.7 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

Sample Ed Law 2-d Addendum

Signatures

For _____ School District

For *[Vendor Name]*

_____

President of the Board of Education

Date:

_____

Date:

Attachment A – Parents' Bill of Rights for Data Security and Privacy

_____ School District

Parents' Bill of Rights for Data Privacy and Security

[INSERT Parents' Bill of Rights for Data Privacy and Security]

For _____ School District

For *[Vendor Name]*

_____

Superintendent

Date:

_____

Date:

Sample Ed Law 2-d Addendum

Supplemental Information About this Contract
[INSERT Supplemental Information. View an example on Page 9.]

Attachment B – District Policy

Attachment C – Vendor's Data Security and Privacy Plan

The DISTRICT Parents Bill of Rights for Data Privacy and Security, a signed copy of which is included as Attachment A to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

[INSERT Links or Text, as provided by the Vendor]

Additional Considerations

NYSED Chief Privacy Officer

Louise Decandia

New York State Education Department
89 Washington Avenue, EB 152
Albany, NY 12234

Phone: 518-474-0937

Email: Privacy@nysed.gov

NYS Office of the State Comptroller

Recent areas of focus:

- Employee Cybersecurity Training
- Review of Internet Usage
- Management of User Accounts

David Pellow
dpellow@moboces.org

Amanda Palmer
apalmer@moric.org

@NYS_OGS @NewYorkStateOGS #2022NYGovBuy

NEW YORK STATE OF OPPORTUNITY. | NY GovBuy