CONTRACTING TRENDS FOR EDTECH

FERPA, State Laws & DPAs

JUNE 2021

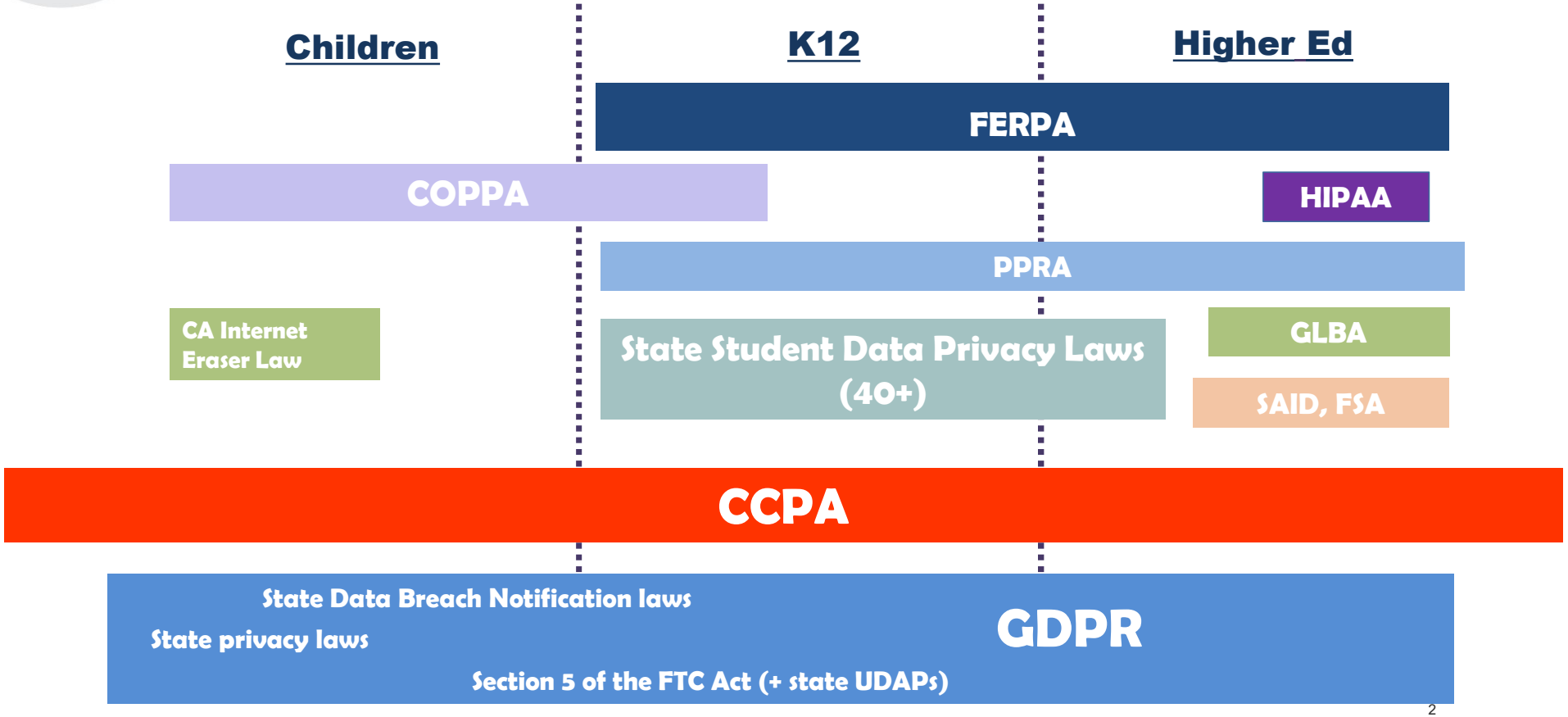
Emily Tabatabai

Partner, Cyber, Privacy & Data Innovation

orrick

EdTech Legal Framework

Operators of child or student-related services face a patchwork of regulation



Compliance is complicated for EdTech

Providers of K12 school services are governed by *a lot* of laws, rules, and regs

	COPPA	FERPA	40+ State Student Privacy Laws
	• Online operators • PI broadly defined (incl. image, audio, persistent IDs, IP address, etc.) • Children <13 (K-8)	• EdTech "School Officials" (imposed via contract) • PI from educational records • K12 + Higher Ed students	• EdTech providers or K12 online services • PI or "covered data" (much more broad) • K12 students
Notice	✓ Notice of data practices	✓ Implicit	✓ Specific contract terms
Consent	✓ Can rely on School to provide necessary consent in limited circumstances	☒ No parental consent	☒ No parental consent
Use	✓ *Solely* for use and benefit of school and for no other commercial purpose	✓ *Solely* for educational purpose described in contract, subject to school control	✓ *Solely* to provide service described in agreement on behalf of school
Rights	✓ Right to review or delete PI or withdraw consent	✓ Rights to inspect, review, amend	✓ Generally, yes, subject to school direction
Deletion	✓ Upon request or when no longer needed for school purpose ! $40,000 per violation	✓ Upon request or when no longer needed for school purpose	✓ Upon request or when no longer needed for school purpose ! Strict contracts

Family Education Rights and Privacy Act

What is FERPA?

- Federal law that applies to educational institutions that accept public funds
- Prohibits a school from disclosing **personally identifiable information** from a student's **educational record** to a third party without written **consent** from the parent. There are several exceptions, however.
- Provides parents the right to inspect and correct the information contained in the student record
- Rights transfer to the student when student turns 18 or enters Higher Ed

Enforcement

- FERPA is enforced by the Department of Education. School is responsible for (and liable for) compliance of its vendors and service providers.
- Issue a complaint, cease and desist order, withhold further funding from Dept.
- Seeks voluntary compliance before imposing sanctions

To Be a "School Official"

Schools usually share data with a vendor/provider under the "School Official" exception to FERPA. Under this exception, schools may share PII from the educational record without parent consent as long as the operator:

- Performs a service or function for which the school would otherwise use its own employees (i.e., acts as a outsourced service provider).
- Is under the **direct control** of the school with regard to the collection and use of data.
- Uses data only for authorized purposes and does **not re-disclose** PII from educational record to other parties unless with consent of School or permitted by FERPA.
  - **TIP**: These restrictions (i.e., direct control, authorized use, and prohibition against re-disclosure) should be established in the contract between the school and the provider. Sometimes, these can be established in the online Terms of Service (TOS).

States Rush to Legislate

- Since 2013: 42+ states have passed legislation regulating student data privacy
- California's 2014 Student Online Personal Information Protection Act (SOPIPA) serves as a model for many other state laws
- Laws vary across states. Most apply *directly* to service providers (EdTech vendors)
  - Prohibit certain data use (e.g., behavioral targeting; re-disclosure); some prohibit *any* secondary use of student data
  - Require data deletion
  - Require specific contractual provisions to be included in EdTech vendor contracts
  - Specific security requirements or alignment with security frameworks

California - SOPIPA

Prohibitions

- Cannot target advertising on vendor site or other sites
- Cannot use student data for targeted advertising or marketing
- Cannot create or amass a “profile” on students, except in furtherance of school purposes
- Cannot sell student data
- Cannot disclose student data except in limited circumstances, e.g.:
  - in furtherance of K12 school purpose or to a service provider, under strict contract terms to prohibit re-disclosure, implement security, require deletion
  - to respond to judicial process, to protect safety of users and others, etc.

Requirements

- Reasonable security procedures and practices
- Contractual controls on third parties
- Delete student data at request of school or district

Permissions

- May use student data for certain internal purposes
- May use de-identified data to improve educational products or demonstrate effectiveness
- May share aggregate, de-identified data
- May market educational products to parents (not based on student data)
- May permit students to download, export or maintain their own data

+ Privacy of Pupil Records Provision of California Education Code 49073.1 (aka AB 1584), which requires certain contractual provisions to be included in vendor contracts

Contracts: California Education Code 49073.1 Requirements

1. Statement that pupil records are the property of and under the control of the school.
2. Description of how pupils may retain possession and control of their own pupil-generated content, if applicable, and/or transfer pupil-generated content to a personal account.
3. Prohibition against using any information in the pupil record for any purpose other than those required or specifically permitted by the contract.
4. Description of how parent may review the pupil's records and correct erroneous information.
5. Description of operator's actions to ensure the security and confidentiality of pupil records.
6. Description of notification procedures in the event of unauthorized disclosure of pupil records.
7. Certification that a pupil's records shall not be retained by operator after term of the agreement, unless if pupil wants to maintain an account to store pupil-generated content.
8. Description of how the local educational agency and the third party will jointly ensure compliance with FERPA.
9. Prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

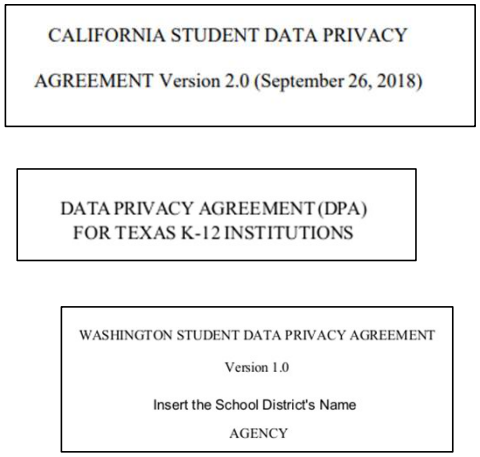
Other States

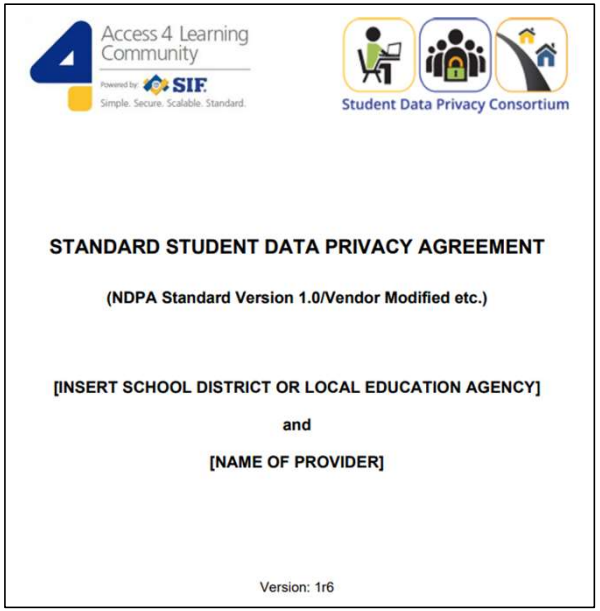
While there are commonalities among state student data privacy laws, there are many unique requirements which vary by state and some states have very unique contracting obligatons. For example:

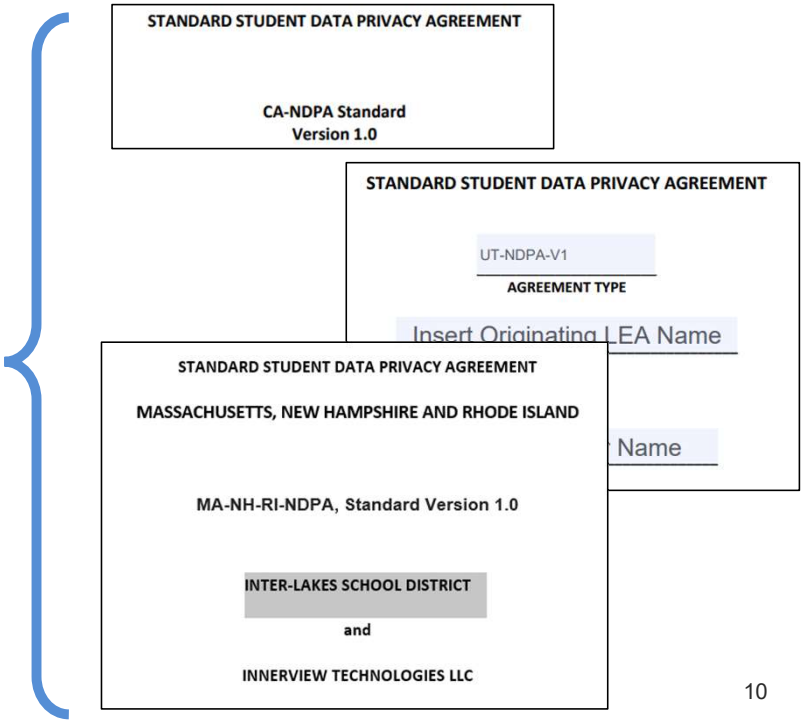
- **New York Ed Law §2d** contracting:
  - Data Protection Agreement (DPA)
  - Vendor Data Security and Privacy Plan (and agree to abide by the District's Data Security and Privacy Plan)
  - Parents Bill of Rights" to be included in all agreements
  - Supplement to the Parent's Bill of Rights
- **Other State law variations**
  - Jurisdictional choice of law provisions
  - Publish list of all subcontractors
  - Employee background checks, confidentiality agreements, training
  - Some DPAs posted publicly
  - Security obligations (e.g., HIPAA Security Rule; encryption at rest, etc.)

State Standard DPAs

- Many states and/or Districts have developed standard DPAs for EdTech vendors
- Ostensibly designed to comply with state student data privacy law requirements, most DPAs *are far more restrictive* than underlying law.
- Student Data Privacy Consortium (SDPC), https://sdpc.a4l.org/
  - State Alliance Agreements (25 states)
  - National Standard Agreement



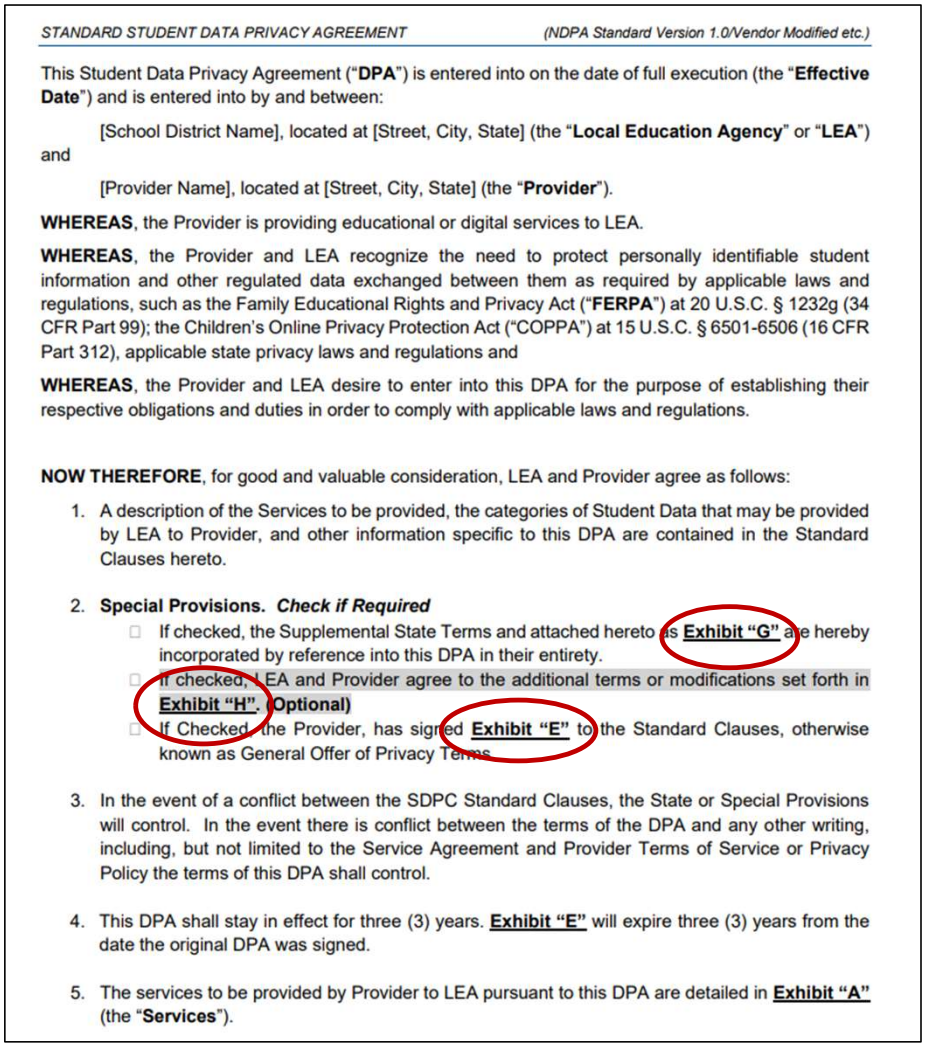




National Standard DPA

National Standard DPA

- **Exhibit E – General Offer of Privacy Terms**
- **Exhibit F – Data Security Requirements**
- **Exhibit G – Supplemental State Terms**
- **Exhibit H – Provider modifications**



STANDARD STUDENT DATA PRIVACY AGREEMENT *(NDPA Standard Version 1.0/Vendor Modified etc.)*

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

[School District Name], located at [Street, City, State] (the "**Local Education Agency**" or "**LEA**") and

[Provider Name], located at [Street, City, State] (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***
   - ☐ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   - ☐ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. **(Optional)**
   - ☐ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

NDPA + State Exhibits

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.
*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G" - Supplemental SDPC (Student Data Privacy Consortium) State Terms for Illinois
Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit G,** Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between _____ (the "Local Education Agency" or "LEA") and _____ (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

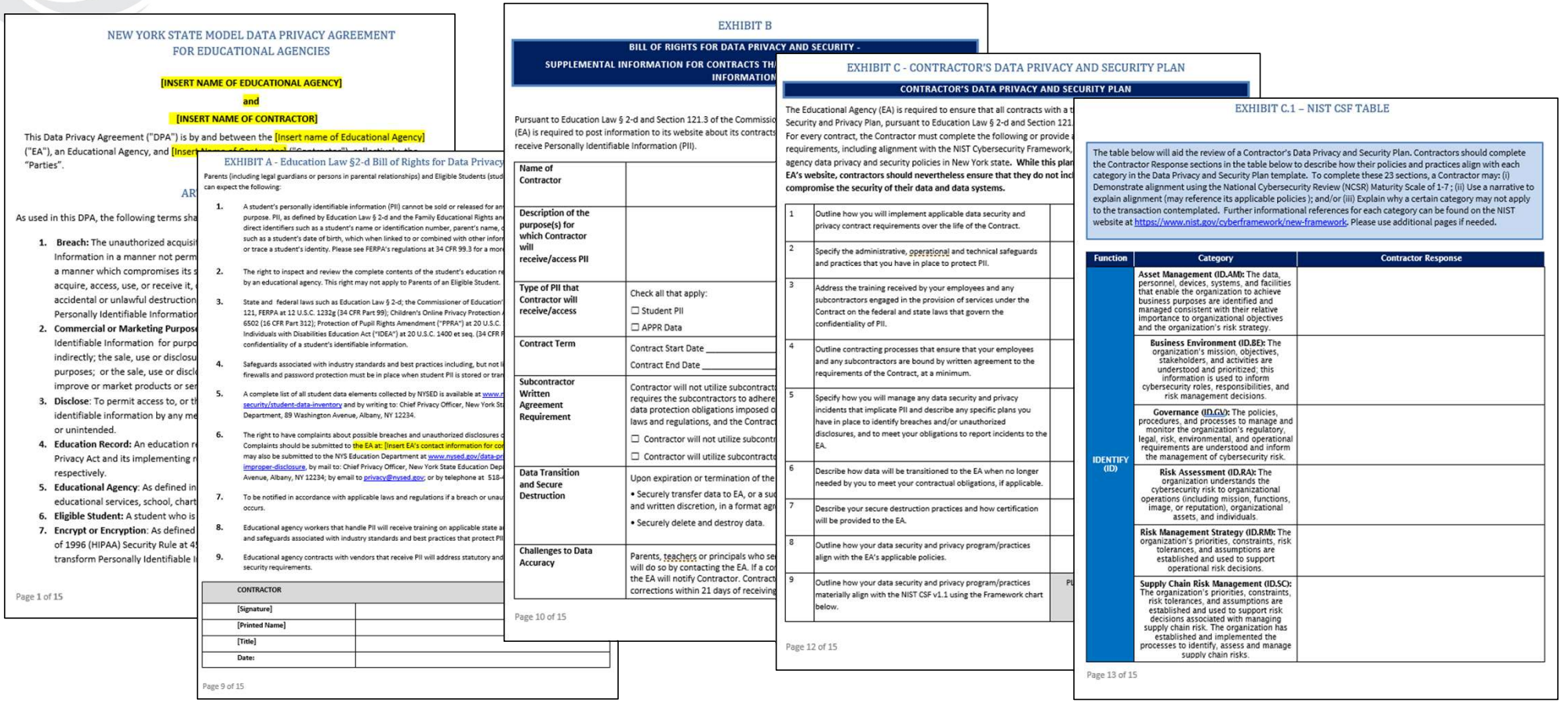
1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C,** Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

NYS Educational Law §2d Requirements



NEW YORK STATE MODEL DATA PRIVACY AGREEMENT
FOR EDUCATIONAL AGENCIES

[INSERT NAME OF EDUCATIONAL AGENCY]
and
[INSERT NAME OF CONTRACTOR]

This Data Privacy Agreement ("DPA") is by and between the [Insert name of Educational Agency] ("EA"), an Educational Agency, and [Insert Name of Contractor] ("Contractor"), collectively, the "Parties".

As used in this DPA, the following terms sha

1. **Breach:** The unauthorized acquisit Information in a manner not perm a manner which compromises its s acquire, access, use, or receive it, accidental or unlawful destruction Personally Identifiable Informatior
2. **Commercial or Marketing Purpos** Identifiable Information for purpo indirectly; the sale, use or disclosu purposes; or the sale, use or discl improve or market products or ser
3. **Disclose**: To permit access to, or th identifiable information by any me or unintended.
4. **Education Record:** An education r Privacy Act and its implementing r respectively.
5. **Educational Agency**: As defined in educational services, school, chart
6. **Eligible Student:** A student who is
7. **Encrypt or Encryption**: As defined of 1996 (HIPAA) Security Rule at 4 transform Personally Identifiable I

Page 1 of 15

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy

Parents (including legal guardians or persons in parental relationships) and Eligible Students (stud can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for an purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights an direct identifiers such as a student's name or identification number, parent's name, such as a student's date of birth, which when linked to or combined with other infor or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a mor
2. The right to inspect and review the complete contents of the student's education re by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education' 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection A 6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR P confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not li firewalls and password protection must be in place when student PII is stored or tran
5. A complete list of all student data elements collected by NYSED is available at www.n security/student-data-inventory and by writing to: Chief Privacy Officer, New York St Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures d Complaints should be submitted to the EA at: [Insert EA's contact information for co may also be submitted to the NYS Education Department at www.nysed.gov/data-pr improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Dep Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-
7. To be notified in accordance with applicable laws and regulations if a breach or unau occurs.
8. Educational agency workers that handle PII will receive training on applicable state a and safeguards associated with industry standards and best practices that protect PII
9. Educational agency contracts with vendors that receive PII will address statutory and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	
[Title]	
Date:	

Page 9 of 15

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS TH
INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissio (EA) is required to post information to its website about its contracts receive Personally Identifiable Information (PII).

Name of Contractor	
Description of the purpose(s) for which Contractor will receive/access PII	
Type of PII that Contractor will receive/access	Check all that apply: ☐ Student PII ☐ APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontract requires the subcontractors to adhere data protection obligations imposed o laws and regulations, and the Contrac ☐ Contractor will not utilize subcontr ☐ Contractor will utilize subcontracto
Data Transition and Secure Destruction	Upon expiration or termination of the • Securely transfer data to EA, or a su and written discretion, in a format agr • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who se will do so by contacting the EA. If a co the EA will notify Contractor. Contract corrections within 21 days of receiving

Page 10 of 15

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a t Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121. For every contract, the Contractor must complete the following or provide requirements, including alignment with the NIST Cybersecurity Framework, agency data privacy and security policies in New York state. **While this plan EA's website, contractors should nevertheless ensure that they do not inc compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PL

Page 12 of 15

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	

Page 13 of 15

Source: NYSED.gov Model Forms and Policies http://www.nysed.gov/data-privacy-security/model-forms-and-policies

FERPA Resources

- FERPA Regulations, https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferparegs.pdf
- Final Regulations, with comments, published by Department of Education, http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- Protecting Student Privacy (US Dept. of Education) https://studentprivacy.ed.gov/
- Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices, https://studentprivacy.ed.gov/training/protecting-student-privacy-while-using-online-educational-services
- Responsibilities of Third Party Service Providers Under FERPA, https://studentprivacy.ed.gov/resources/responsibilities-third-party-service-providers-under-ferpa
- Model Terms of Service, https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-model-terms-service

General Resources

- Student Privacy Compass (formerly FERPA/Sherpa) https://studentprivacycompass.org/
- TEC Student Data Privacy Alliance (MA, NH and RI) https://tec-coop.org/data-privacy/resources/
- Illinois SBOE Resources for Student Data Privacy https://www.isbe.net/Pages/Privacy-Policy-Resources-and-Links.aspx
- RIC One NY 2d Guidance and Policies https://riconedpss.org/resources