EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Liminex, Inc. dba GoGuardian, (acting on behalf of itself and its affiliates, including Pear Deck, Inc. and Snapwiz Inc. dba Edulastic (collectively, the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement or as authorized by the Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place appropriate internal controls designed to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any personally identifiable information and confidential information in accordance with State or federal student data privacy laws, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of ESBOCES and/or participating school districts 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to use commercially reasonable efforts to comply with the attached ESBOCES Policy 4591, Data Security and Privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall use commercially reasonable methods to destroy, or if requested in writing within thirty (30) days of termination or expiration, return all of ESBOCES' and/or participating school districts' data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, 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;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how 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 educational agency;

6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option and direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);

2. Comply with the applicable data security and privacy policy of ESBOCES attached herein; Education Law § 2-d; and Part 121;

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

LIMINEX, INC. D/B/A GOGUARDIAN, acting on behalf of itself and its affiliates, including Pear Deck, Inc. and Snapwiz Inc. dba Edulastic

BY: Mike Jonas
Mike Jonas, Chief Financial Officer

DATED: March 30, 2022

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

- Contractor will implement applicable state, federal, and local data security and privacy requirements during the term of the Agreement, consistent with ESBOCES's data security and privacy policy.

- Contractor has administrative, operational and technical safeguards designed to protect Protected Data that it receives during the Term, including:

    - Administrative Safeguards: Data breach response plan, change management systems, security and privacy awareness training, employee background checks
    - Operational Safeguards: Office security guards, key cards, office surveillance
    - Technical Safeguards: Access controls to Personally Identifiable Information, encryption in motion between product endpoints via SSL and at rest of Personally Identifiable Information, authentication of desktops and laptops, penetration testing

- Contractor is providing its Supplemental Information for the Bill of Rights below.

- Contractor provides training to employees who access to Protected Data under the Contract on the federal and state laws governing confidentiality of such data in the onboarding process for new employees and on an annual basis for existing employees.
- Contractor will use subcontractors to help operate some of the Products such as a database provider. Contractor will take steps designed to ensure that the subcontractors, or other authorized persons or entities to which Contractor will disclose Protected Data will abide by data security and privacy requirements, including by:
    - Conducting diligence and evaluating the security practices of subcontractors that can access Protected Data
    - Requesting verification of compliance with security and privacy standards aligned with state and federal law
    - Evaluating the contractual safeguards of subcontractors of Protected Data

- Contractor will manage data security and privacy incidents that implicate Protected Data by implementing a data incident response policy, conducting penetration tests to help prevent breaches, and as applicable, by complying with the breach provisions of Education Law 2-d, including the breach notification requirements.

- For information about whether, how and when Protected Data will be transitioned to a successor contractor or deleted and destroyed when the Agreement is terminated or expire, please refer to Contractor's Product Privacy Policy (available at https://www.goguardian.com/product-privacy/)

Supplemental Information:

Supplemental Information for a third party contractor includes:

- 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;

Please see Contractor's Product Privacy Policy (available at https://www.goguardian.com/policies/product-privacy) listing the exclusive purposes for which the Protected Data will be used by Contractor).

- 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; New York Education Law Section 2-d);

Please see Contractor's Data Privacy and Security Plan above and incorporated herein for a description of how Contractor will help ensure that the subcontractors, or other authorized persons or entities to which Contractor will disclose Protected Data

- the duration of the contract, including the contract's expiration date and a description of what will happen to the Protected Data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed);

The duration of the contract between Participant and Contractor is found on the applicable order from. Please see Product Privacy Policy for a description of what will happen to Protected Data, unless otherwise agreed to in writing between Participant and Contractor

- if and how a parent, student, eligible student, teacher or principal may challenge the accuracy of Protected Data that is collected;

Please see Contractor's Product Privacy Policy listing for how a student may challenge the accuracy may challenge the accuracy of Protected Data.

- where the Student Data or Teacher or Principal Data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated; and

    - Protected Data will be stored in industry-leading databases.

- address how the data will be protected using Encryption while in motion and at rest.

    - Protected Data will be protected using encryption in motion between product endpoints via SSL and at rest.

EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at:
http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.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.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

   The exclusive purpose for which Contractor is being provided access to Protected Data is to provide ESBOCES and/or participating school districts with the functionality of Contractor's Offering(s). Protected Data received by Contractor, or any of Contractor's subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purpose.

2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

   Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations (including but not limited to Education Law 2-d), and the Agreement.

   Contractor will take the following steps to ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements:

   - *Conduct diligence and evaluating the security practices of subcontractors that can access Protected Data*
   - *Request verification of compliance with security and privacy standards aligned with state and federal law*
   - *Evaluate the contractual safeguards of subcontractors of Protected Data*

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   The duration of the contract between Participant and Contractor is found on the applicable order form. Please see Product Privacy Policy for a description of what will happen to Protected Data, unless otherwise agreed to in writing between Participant and Contractor.

4. 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; and

Complaints should be directed to: the Associate Superintendent for Curriculum for your district; Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

Protected Data will be stored in industry-leading databases.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose 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 third-party contractor provides a notice of the disclosure to the New York State Education 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;
5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

Eastern Suffolk BOCES
Educational Services That Transform Lives

First Supervisory District of Suffolk County
201 Sunrise Highway
Patchogue, New York 11772

Board Policy

Data Security and Privacy

The Board is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in ESBOCES and when disclosing or releasing it to others, including, but not limited to, third-party contractors. ESBOCES adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align ESBOCES data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d) "Commercial or Marketing Purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f) "Disclose" or "Disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g) "Education Records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

h) "Educational Agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) "Eligible Student" means a student who is eighteen (18) years or older.

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.

k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m) "Parent" means a parent, or person in parental relation to a student.

n) "Personally Identifiable Information" as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c (10).

o) "Release" shall have the same meaning as Disclosure or Disclose.

p) "Student" means any person attending or seeking to enroll in an educational agency.

q) "Student data" means personally identifiable information from the student records of an educational agency.

r) "Teacher or Principal Data" means personally identifiable information from the records of an educational agency 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 Sections 3012-c and 3012-d.

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

t) "Unauthorized Disclosure" or "Unauthorized Release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or

written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, ESBOCES will take steps to minimize its collection, processing, and transmission of Personally Identifiable Information (PII). Additionally, ESBOCES will:

a) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and ESBOCES' data security and privacy policy.

Except as required by law or in the case of educational enrollment data, ESBOCES will not report to NYSED the following student data elements:

a) Juvenile delinquency records;

b) Criminal records;

c) Medical and health records; and

d) Student biometric information.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

ESBOCES will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

Data Protection Officer

ESBOCES has designated, and will maintain, an ESBOCES employee to serve as ESBOCES Data Protection Officer. The Data Protection Officer for ESBOCES is: the Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for ESBOCES.

ESBOCES will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

ESBOCES Data Privacy and Security Standards

ESBOCES will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

a) Describe their current cybersecurity posture;

b) Describe their target state for cybersecurity;

c) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

d) Assess progress toward the target state; and

e) Communicate among internal and external stakeholders about cybersecurity risk.

ESBOCES will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by ESBOCES benefits students and ESBOCES by considering, among other criteria, whether the use and/or disclosure will:

   1. Improve academic achievement;

   2. Empower parents/persons in parental relation and students with information; and/or

   3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

ESBOCES affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents/persons in parental relation or eligible students, where applicable.

Third-Party Contractors

ESBOCES Responsibilities

ESBOCES will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from ESBOCES, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and ESBOCES policy.

In addition, ESBOCES will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by ESBOCES.

The third-party contractor's data privacy and security plan must, at a minimum:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with ESBOCES' data security and privacy policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data 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;

e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify ESBOCES;

g) Describe whether, how, and when data will be returned to ESBOCES, transitioned to a successor contractor, at ESBOCES option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with ESBOCES under which the third-party contractor will receive student data or teacher or principal data from ESBOCES, is required to:

a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b) Comply with ESBOCES' data security and privacy policy and Education Law Section 2-d and its implementing regulations;

c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent/person in parental relation or eligible student:

1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with ESBOCES; or

2. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g) Use encryption to protect PII in its custody while in motion or at rest; and

h) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Cooperative Educational Services through a BOCES

A district may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from a district under all circumstances.

For example, a district may not need its own contract or agreement where:

a) It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and

b) That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to a district's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from a district is received by a third-party contractor pursuant to a CoSer, a district will consult with the BOCES to, among other things:

a) Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern a district's use of a third-party contractor's product or service under a particular CoSer;

b) Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;

c) Ensure appropriate notification is provided to affected parents/persons in parental relation, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from a district pursuant to a BOCES contract; and

d) Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event a district receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from a district pursuant to a BOCES contract.

Click-Wrap Agreements

Periodically, ESBOCES staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

ESBOCES staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from ESBOCES unless they have received prior approval from ESBOCES Data Privacy Officer or designee.

ESBOCES will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

ESBOCES will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, ESBOCES will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from ESBOCES.

The Bill of Rights will contain all required elements including supplemental information for each contract ESBOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from ESBOCES or a district. The supplemental information must be developed by ESBOCES and include the following information:

a) 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;

b) 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 laws and regulations (e.g., FERPA; Education Law Section 2-d);

c) 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 ESBOCES or a district, and/or whether, when, and how the data will be destroyed);

d) If and how a parent/person in parental relation, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

e) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

f) Address how the data will be protected using encryption while in motion and at rest.

ESBOCES will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from ESBOCES. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of ESBOCES data and/or technology infrastructure.

Right of Parents/Persons in Parental Relation and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of ESBOCES under FERPA, parents/persons in parental relation and eligible students have the right to inspect and review a student's education record by making a request directly to ESBOCES in a manner prescribed by ESBOCES.

ESBOCES will ensure that only authorized individuals are able to inspect and review student data. To that end, ESBOCES will take steps to verify the identity of parents/persons in parental relation or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent/person in parental relation or eligible student for access to a student's education records must be directed to ESBOCES and not to a third-party contractor. ESBOCES may require that requests to inspect and review education records be made in writing.

ESBOCES will notify parents/persons in parental relation annually of their right to request to inspect and review their child's education record including any student data stored or maintained by ESBOCES through its annual FERPA notice. A notice separate from ESBOCES annual FERPA notice is not required.

ESBOCES will comply with a request for access to records within a reasonable period, but not more than forty five (45) calendar days after receipt of a request.

ESBOCES may provide the records to a parent/person in parental relation or eligible student electronically, if the parent/person in parental relation consents. ESBOCES must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent/person in parental relation or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

ESBOCES will inform parents/persons in parental relation, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible

breaches of student data to the Chief Privacy Officer at NYSED. In addition, ESBOCES has established the following procedures for parents/persons in parental relation, eligible students, teachers, principals, and other ESBOCES staff to file complaints with ESBOCES about breaches or unauthorized releases of student data and/or teacher or principal data:

a) All complaints must be submitted to ESBOCES Data Protection Officer in writing without unreasonable delay, but no more than ten (10) calendar days after such discovery.

b) Upon receipt of a complaint, ESBOCES will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) Following the investigation of a submitted complaint, ESBOCES will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than sixty (60) calendar days from the receipt of the complaint by ESBOCES.

d) If ESBOCES requires additional time, or where the response may compromise security or impede a law enforcement investigation, ESBOCES will provide the individual who filed the complaint with a written explanation that includes the approximate date when ESBOCES anticipates that it will respond to the complaint.

These procedures will be disseminated to parents/persons in parental relation, eligible students, teachers, principals, and other ESBOCES staff.

ESBOCES 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.

Reporting a Breach or Unauthorized Release

ESBOCES will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within ESBOCES to the Chief Privacy Officer without unreasonable delay, but no more than ten (10) calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with ESBOCES will be required to promptly notify ESBOCES of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, ESBOCES policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, ESBOCES will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten (10) calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation,

the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with ESBOCES and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, ESBOCES policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than thirty (30) days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

a) Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five (5) years;

b) Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five (5) years;

c) Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five (5) years; and/or

d) Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed, at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

ESBOCES will notify affected parents/persons in parental relation, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than sixty (60) calendar days after the discovery of a breach or unauthorized release of PII by ESBOCES or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, ESBOCES will notify parents/persons in parental relation, eligible students, teachers, and/or principals within seven (7) calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

b) A description of the types of PII affected;

c) An estimate of the number of records affected;

d) A brief description of ESBOCES investigation or plan to investigate; and

e) Contact information for representatives who can assist parents/persons in parental relation or eligible students that have additional questions.

Notification will be directly provided to the affected parent/person in parental relation, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse ESBOCES for the full cost of this notification.

Annual Data Privacy and Security Training

ESBOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. ESBOCES may deliver this training using online training tools. Additionally, this training may be included as part of the training that ESBOCES already offers to its workforce.

Notification of Policy

ESBOCES will publish this policy on its website and provide notice of the policy to all its officers and staff.

References:

- NYS Education Law § 2-d
- 8 NYCRR Part 121

First Adopted: 9/23/2020
Adopted as revised: 3/18/2021