

(iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as “directory information” (described below). The attached FERPA Model Notification of Rights more fully describes the exceptions to the consent requirement under FERPA).

4. Where a school or school district has a policy of releasing “directory information” from student records, the parent has a right to refuse to let the school or school district designate any all of such information as directory information. Directory information, as defined in federal regulations, includes: the student’s name, address, telephone number, email address, photograph, date and place of birth, major field of study, grade level, enrollment status, dates of attendance, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received and the most recent educational agency or institution attended. Where disclosure without consent is otherwise authorized under FERPA, however, a parent’s refusal to permit disclosure of directory information does not prevent disclosure pursuant to such separate authorization.
5. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the School to comply with the requirements of FERPA.

B. What are parents’ rights under the Personal Privacy Protection Law (PPPL), Article 6-A of the Public Officers Law relating to records held by State agencies?

The PPPL (Public Officers Law §§91-99) applies to all records of State agencies and is not specific to student records or to parents. It does not apply to school districts or other local educational agencies. It imposes duties on State agencies to have procedures in place to protect from disclosure of “personal information,” defined as information which because of a name, number, symbol, mark or other identifier, can be used to identify a “data subject” (in this case the student or the student’s parent). Like FERPA, the PPPL confers a right on the data subject (student or the student’s parent) to access to State agency records relating to them and requires State agencies to have procedures for correction or amendment of records.

A more detailed description of the PPPL is available from the Committee on Open Government of the New York Department of State. Guidance on what you should know about the PPPL can be accessed at <http://www.dos.ny.gov/coog/shldno1.html>. The Committee on Open Government’s address is Committee on Open Government, Department of State, One Commerce Plaza, 99 Washington Avenue, suite 650, Albany, NY 12231, their email address is coog@dos.ny.gov, and their telephone number is (518) 474-2518.

C. Parents’ Rights Under Education Law §2-d relating to Unauthorized Release of Personally Identifiable Information

1. What “educational agencies” are included in the requirements of Education Law §2-d?

- The New York State Education Department (“NYSED”);
- Each public-school district;
- Each Board of Cooperative Educational Services or BOCES; and

- All schools that are:
 - a public elementary or secondary school;
 - a universal pre-kindergarten program authorized pursuant to Education Law §3602-e;
 - an approved provider of preschool special education services;
 - any other publicly funded pre-kindergarten program;
 - a school serving children in a special act school district as defined in Education Law 4001; or
 - certain schools for the education of students with disabilities - an approved private school, a state-supported school subject to the provisions of Education Law Article 85, or a state-operated school subject to Education Law Article 87 or 88.

2. What kind of student data is subject to the confidentiality and security requirements of Education Law §2-d?

The law applies to personally identifiable information contained in student records of an educational agency listed above. The term “student” refers to any person attending or seeking to enroll in an educational agency, and the term “personally identifiable information” (“PII”) uses the definition provided in FERPA. Under FERPA, personally identifiable information or PII includes, but is not limited to:

- (a) The student’s name;
- (b) The name of the student’s parent or other family members;
- (c) The address of the student or student’s family;
- (d) A personal identifier, such as the student’s social security number, student number, or biometric record;
- (e) Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name¹;
- (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

3. What kind of student data is *not* subject to the confidentiality and security requirements of Education Law §2-d?

The confidentiality and privacy provisions of Education Law §2-d and FERPA extend only to PII, and not to student data that is not personally identifiable. Therefore, de-identified data (e.g., data regarding students that uses random identifiers), aggregated data (e.g., data reported at the school district level) or anonymized data that could not be used to identify a particular student is not considered to be PII and is not within the purview of Education Law §2-d or within the scope of this Parents’ Bill of Rights.

4. What are my rights under Education Law § 2-d as a parent regarding my student’s PII?

¹ Please note that NYSED does not collect certain information defined in FERPA, such as students’ social security numbers, biometric records, mother’s maiden name (unless used as the mother’s legal name).

Education Law §2-d ensures that, in addition to all of the protections and rights of parents under the federal FERPA law, certain rights will also be provided under the Education Law. These rights include, but are not limited to, the following elements:

- (A) A student's PII cannot be sold or released by the educational agency for any commercial or marketing purposes.
 - PII may be used for purposes of a contract that provides payment to a vendor for providing services to an educational agency as permitted by law.
 - However, sale of PII to a third party solely for commercial purposes or receipt of payment by an educational agency, or disclosure of PII that is not related to a service being provided to the educational agency, is strictly prohibited.

- (B) Parents have the right to inspect and review the complete contents of their child's education record including any student data stored or maintained by an educational agency.
 - This right of inspection is consistent with the requirements of FERPA. In addition to the right of inspection of the educational record, Education Law §2-d provides a specific right for parents to inspect or receive copies of any data in the student's educational record.
 - NYSED will develop policies for annual notification by educational agencies to parents regarding the right to request student data. Such policies will specify a reasonable time for the educational agency to comply with such requests.
 - The policies will also require security measures when providing student data to parents, to ensure that only authorized individuals receive such data. A parent may be asked for information or verifications reasonably necessary to ensure that he or she is in fact the student's parent and is authorized to receive such information pursuant to law.

- (C) State and federal laws protect the confidentiality of PII, 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.

Education Law §2-d also specifically provides certain limitations on the collection of data by educational agencies, including, but not limited to:

- (A) A mandate that, except as otherwise specifically authorized by law, NYSED shall only collect PII relating to an educational purpose;

- (B) NYSED may only require districts to submit PII, including data on disability status and student suspensions, where such release is required by law or otherwise authorized under FERPA and/or the New York State Personal Privacy Law; and

- (C) Except as required by law or in the case of educational enrollment data, school districts shall not report to NYSED student data regarding juvenile delinquency records, criminal records, medical and health records or student biometric information.

- (D) Parents may access the NYSED Student Data Elements List, a complete list of all student data elements collected by NYSED, at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, or may obtain a copy of this list by writing to the Office of Information & Reporting Services,

New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

- (E) Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. The complaint process is under development and will be established through regulations to be proposed by NYSED's Chief Privacy Officer, who has not yet been appointed.
- Specifically, the Commissioner of Education, after consultation with the Chief Privacy Officer, will promulgate regulations establishing procedures for the submission of complaints from parents, classroom teachers or building principals, or other staff of an educational agency, making allegations of improper disclosure of student data and/or teacher or principal APPR data by a third-party contractor or its officers, employees or assignees.
 - When appointed, the Chief Privacy Officer of NYSED will also provide a procedure within NYSED whereby parents, students, teachers, superintendents, school board members, principals, and other persons or entities may request information pertaining to student data or teacher or principal APPR data in a timely and efficient manner.

5. Must additional elements be included in the Parents' Bill of Rights.?

Yes. For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third-party contractor shall include the following supplemental information:

- (A) the exclusive purposes for which the student data, or teacher or principal data, will be used;
- (B) 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;
- (C) when the agreement with the third-party contractor expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- (D) 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
- (E) 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.
 - a. In addition, the Chief Privacy Officer, with input from parents and other education and expert stakeholders, is required to develop additional elements of the Parents' Bill of Rights to be prescribed in Regulations of the Commissioner.

6. What protections are required to be in place if an educational agency contracts with a third-party contractor to provide services, and the contract requires the disclosure of PII to the third-party contractor?

Education Law §2-d provides very specific protections for contracts with “third party contractors”, defined as 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 such educational agency. The term “third party contractor” also includes an educational partnership organization that receives student and/or teacher or principal APPR data from a school district to carry out its responsibilities pursuant to Education Law §211-e, and a not-for-profit corporation or other non-profit organization, which are not themselves covered by the definition of an “educational agency.”

Services of a third-party contractor covered under Education Law §2-d include, 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.

When an educational agency enters into a contract with a third-party contractor, under which the third-party contractor will receive student data, the contract or agreement must include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. However, the standards for an educational agency's policy on data security and privacy must be prescribed in Regulations of the Commissioner that have not yet been promulgated. A signed copy of the Parents' Bill of Rights must be included, as well as a requirement that any officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Each third-party contractor that enters into a contract or other written agreement with an educational agency under which the third-party contractor will receive student data or teacher or principal data shall:

- limit internal access to education records to those individuals that are determined to have legitimate educational interests
- not use the education records for any other purposes than those explicitly authorized in its contract;
- except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any PII to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the party provides a notice of the disclosure to NYSED, district 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;
- maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody; and
- use encryption technology to protect data while in motion or in its custody from unauthorized disclosure.

7. What steps can and must be taken in the event of a breach of confidentiality or security?

Upon receipt of a complaint or other information indicating that a third-party contractor may have improperly disclosed student data, or teacher or principal APPR data, NYSED's Chief Privacy Officer is authorized to investigate, visit, examine and inspect the third-party contractor's facilities

and records and obtain documentation from, or require the testimony of, any party relating to the alleged improper disclosure of student data or teacher or principal APPR data.

Where there is a breach and unauthorized release of PII by a by a third party contractor or its assignees (e.g., a subcontractor): (i) the third party contractor must notify the educational agency of the breach in the most expedient way possible and without unreasonable delay; (ii) the educational agency must notify the parent in the most expedient way possible and without unreasonable delay; and (iii) the third party contractor may be subject to certain penalties including, but not limited to, a monetary fine; mandatory training regarding federal and state law governing the confidentiality of student data, or teacher or principal APPR data; and preclusion from accessing any student data, or teacher or principal APPR data, from an educational agency for a fixed period up to five years.

8. Data Security and Privacy Standards

Upon appointment, NYSED's Chief Privacy Officer will be required to develop, with input from experts, standards for educational agency data security and privacy policies. The Commissioner will then promulgate regulations implementing these data security and privacy standards.

9. No Private Right of Action

Please note that Education Law §2-d explicitly states that it does not create a private right of action against NYSED or any other educational agency, such as a school, school district or BOCES.

APPENDIX S-1
Attachment to Parents' Bill of Rights
For Contracts Involving Disclosure of Certain Personally Identifiable Information

Education Law §2-d, added by Ch. 56 of the Laws of 2014, requires that a Parents' Bill of Rights be attached to every contract with a third-party contractor (as defined in the law) which involves the disclosure of personally identifiable information (PII) derived from student education records ("Student Data"), or certain teacher/principal information regarding annual professional performance evaluations that is confidential pursuant to Education Law §30212-c ("APPR Data"). Each such Contract must include this completed Attachment to provide specific information about the use of such data by the Contractor.

1. Specify whether this Contract involves disclosure to the Contractor of Student Data, APPR Data, or both.

- Disclosure of Student Data
 Disclosure of APPR Data

2. Describe the exclusive purposes for which the Student Data or APPR Data will be used in the performance of this contract.

Student Data may be utilized for the purposes of evaluating district needs, progress over time, and achievement of goals. "

3. Identify any subcontractors or other persons/entities with whom the Contractor will share the Student Data or APPR in the performance of this Contract and describe how the Contractor will ensure that such persons/entities will abide by the data protection and security requirements of the Contract.

Subcontractors or other entities with whom the Contractor will share data:

Bidder should specifically list in this section any/all subcontractors that will/may receive data.

Currently, no Eastern Suffolk BOCES Consultants hired to carry out L.I. RBERN contract deliverables require access to Student or APPR data.

In the event that this circumstance changes, contractors/subcontractors will be required to sign and submit the attached "ESBOCES Education Law 2-d Rider" as well as a Data Privacy & Security Plan to affirm compliance with the law. The Rider clarifies the requirements for contractors to have "Data Security and Privacy Plan" in place and includes a copy of ESBOCES Parents' Bill of Rights for Data Security and Privacy. Any data that may be provided will be paper copies (unless unavoidable) and restricted to use in the Eastern Suffolk BOCES' L.I. RBERN office. Please see number 6 below for a description of security measures in place to address this possibility.

In the event the Contractor engages a Subcontractor or otherwise shares Student Data or APPR Data with any other entity, Contractor acknowledges and agrees that before any such data is shared with a Contractor or another entity, such party must agree in writing to be bound by the confidentiality and data protection provisions set forth in this Contract including, but not limited to, the "Data Security and Privacy Plan" set forth in Appendix R. Upon termination of the agreement between the Contractor and a Subcontractor or other entity, Contractor acknowledges and agrees that it is responsible for ensuring that all Student Data or APPR Data shared by the Contractor must be returned to Contractor

or otherwise destroyed as provided in Paragraph 4 of the “Data Security and Privacy Plan” set forth in Appendix R.

4. Specify the expiration date of the Contract and explain what will happen to the Student Data or APPR Data in the Contractor’s possession, or the possession of any person/entity described in response to Paragraph 3, upon the expiration or earlier termination of the Contract.

Contract expiration date: **June 30, 2025**

Contractor agrees to return the Student Data or APPR Data to NYSED consistent with the protocols set forth in Paragraph 4 of the “Data Security and Privacy Plan” set forth in Appendix R.

Contractor agrees to securely destroy the Student Data or APPR Data consistent with the protocols set forth in Paragraph 4 of the “Data Security and Privacy Plan” set forth in Appendix R.

5. State whether the Contractor will be collecting any data from or pertaining to students derived from the student’s education record or pertaining to teachers or principals’ annual professional performance evaluation pursuant to the Contract, and explain if and how a parent, student, eligible student (student eighteen years or older), teacher or principal may challenge the accuracy of the Student Data or APPR data that is collected.

Student Data

APPR Data

Any challenges to the accuracy of any of the Student Data or APPR Data shared pursuant to this Contract should be addressed to the school, educational agency or entity which produced, generated or otherwise created such data.

6. Describe where the Student Data or APPR Data will be stored (in a manner that does not jeopardize data security), and the security protections taken to ensure that the data will be protected, including whether such data will be encrypted.

Bidder should detail in this section where data will be stored, what security measures will be in place, and whether electronic data is encrypted in motion and/or at rest.

ESBOCES' L.I. RBERN staff does not have digital access to Student or Staff APPR data.

Any paper copies of student or APPR data provided to Eastern Suffolk BOCES' L.I. RBERN staff will be stored in locked filed cabinets in a secure area away from the public and will not be allowed to be removed from the office. When the data is no longer needed, the copies will either be returned to the owner in person or securely destroyed with a cross-cut shredder.

If digital copies of data are provided by NYSED or a school district, they will be stored on ESBOCES secure internal servers only accessible to individuals employed by the agency and accessible with a unique user name and password.

Should it be necessary for NYSED or a school district to transmit Student or APPR data to ESBOCES staff, ESBOCES provides access to a secure "web courier" service to securely transfer encrypted data, only accessible with username and password and only viewable by the intended recipient.

Eastern Suffolk BOCES will provide annual training on security procedures and compliance with Ed Law 2-d, Children's Internet Protection Act (CIPA), Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA), as applicable.



**Education Law
§2-d Rider**

Board of Cooperative Educational Services
First Supervisory District of Suffolk County
201 Sunrise Highway
Patchogue, New York 11772
(631) 289-2200

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 signs 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 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 contract between ESBOCES and Contractor 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. 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 sufficient internal controls to ensure that ESBOCES and/or Participants' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or Federal law, 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 a Participant. 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 its Participants as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of ESBOCES and/or its Participants 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.

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 comply with ESBOCES policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or its Participants 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 return all ESBOCES and/or its Participants' data, 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 ESBOCES and/or its Participant's Protected Data shall maintain a Data Security and Privacy Plan that includes the following elements:

1. a provision incorporating the requirements of ESBOCES Parents' Bill of Rights for data security and privacy, to the extent that any of the provisions in the Bill of Rights applies to Contractor's possession and use of Protected Data pursuant to this Agreement;
2. an outline of how all State, Federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the Contractor's policy on data security and privacy;
3. an outline of the measures taken by Contractor to secure Protected Data and to limit access to such data to authorized staff;
4. an outline of how Contractor will use "best practices" and industry standards with respect to data storage, privacy, and protection, including, but not limited to, encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff; and
5. an outline of how Contractor will ensure that any subcontractors, persons, or entities with which Contractor will share Protected Data, if any, will abide by the requirements of Contractor's policy on data security and privacy, and the contractual obligations with respect to Protected Data set forth herein.

9. provide a signed copy of this Parents' Bill of Rights to ESBOCES, thereby acknowledging that they are aware of and agree to abide by this Parents' Bill of Rights.

This Parents' 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.

Contractor hereby acknowledges that it is aware of and agrees to abide by the terms of this Parents' Bill of Rights. A copy of this signed document must be made a part of Contractor's Data Security and Privacy Plan.

SIGNATURE: _____

DATE: _____

TITLE: _____