

EXHIBIT G

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 **PowerSchool Group LLC** (the "Contractor" or "PowerSchool") 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" or "Customer") 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. 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 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 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 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 comply with ESBOCES' policy(ies) on data security and privacy. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full **reasonable** 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, **upon written request**, shall 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 **of the Regulations of the Commissioner of Education**;
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 **International Standards Organization, Information technology - Security techniques Information security management systems (ISO 27000 series) which are compatible with** the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of Education Law § 2-d; and Part 121 **of the Regulations of the Commissioner of Education**;
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.

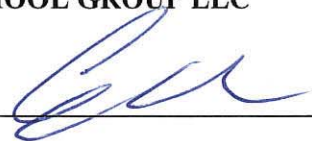
In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

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.

POWERSCHOOL GROUP LLC

BY: _____



DATED: _____



DATA PRIVACY AND SECURITY PLAN

DEFINITIONS

“Customer Data” means all data, files, documents and records uploaded to a PowerSchool Subscription Service or transmitted to PowerSchool under this Agreement by or on behalf of Customer. Customer Data is the property of Customer.

“Documentation” means all written user information, whether in electronic, printed, or other format, delivered or made available to Customer by PowerSchool with respect to PowerSchool Product(s), now or in the future, including instructions, manuals, training materials, and other publications that contain, describe, explain, or otherwise relate to PowerSchool Product(s).

“PowerSchool Product(s)” means any Subscription Service(s) or Services provided to Customer or described on a Quote.

“Quote” means PowerSchool’s standard order form that (i) specifies the PowerSchool Product(s) and other Services provided to Customer; (ii) references the applicable agreement; and (iii) is signed or incorporated to a signed agreement by authorized representatives of both Parties.

“SaaS” means the acronym for the phrase “software as a service.”

“Subscription Service(s)” means all PowerSchool SaaS software applications (including Embedded Applications), any subsequent versions of the same and all related Documentation provided to Customer pursuant to this Agreement, now or in the future; provided, however, that Subscription Services does not include any Third-Party Software and do not apply to perpetual licensed-versions of the PowerSchool software applications. Subscription Service(s) are offered via subscription licenses where services are hosted either by or on behalf of PowerSchool; or in servers on the Customer’s premises as identified on the applicable Quote.

1. **Data Security.** PowerSchool agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices for digital storage of sensitive personal data, to protect Customer Data from unauthorized disclosure or acquisition by an unauthorized person. The general security obligations of PowerSchool are set forth below. These security measures will include, but are not limited to:
 - 1.1. **Passwords and Employee Access.** PowerSchool will secure usernames, passwords, and any other means of gaining access to the Services or to Customer Data, at a level meeting or exceeding the applicable standards. PowerSchool will only provide access to Customer Data to employees or contractors who require access pursuant to the Agreement, and only on terms consistent or exceeding the data security measures required by this Agreement between the Parties.
 - 1.2. **Security Protocols.** The Parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. PowerSchool will maintain all data obtained or generated pursuant to this Agreement in a secure digital environment and will not copy, reproduce, or transmit data obtained pursuant to this Agreement, except as necessary to fulfill the purpose of data requests by Customer.
 - 1.3. **Employee Training.** PowerSchool will provide periodic security training to those of its employees who operate or have access to the system. Further, PowerSchool will provide Customer with contact information of an employee whom Customer may contact if there are any security concerns or questions.

- 1.4. Security Technology. PowerSchool will employ industry standard measures to protect data from unauthorized access. The service security measures will include server authentication and data encryption. PowerSchool will host data pursuant to this Agreement in an environment using a firewall that is updated according to industry standards.
- 1.5. Security Coordinator. PowerSchool will provide the name and contact information of PowerSchool's security coordinator for the Customer Data received pursuant to this Agreement upon written request.
- 1.6. Sub-processors Bound. PowerSchool will enter into written agreements whereby sub-processors agree to secure and protect Customer Data in a manner consistent with the terms of this **Section 1**. PowerSchool will periodically conduct or review compliance monitoring and assessments of sub-processors to determine their compliance with this **Section 1**. For the purposes of this Agreement, the term "sub-processor" means a party other than Customer or PowerSchool, whom PowerSchool uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to Customer Data.
- 1.7. Periodic Risk Assessment. PowerSchool further acknowledges and agrees to conduct digital and physical periodic risk assessments at least annually and remediate any identified security and privacy vulnerabilities in a timely manner.
- 1.8. PowerSchool will follow its established access security policies to support the physical security of the Customer Data against such risks as unauthorized access, collection, use, disclosure or disposal, loss or modification. Such security arrangements will include, without limitation, reasonable technical, physical, and administrative safeguards.

**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;

- a. *PowerSchool's functionality is the management of the school's data including student, teacher and principle PII. The program is utilized by the school to enhance functionality, efficiency and also for the benefit of the students and parents.*
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;
 - a. *PowerSchool will enter into written agreements whereby sub-processors and sub-contractors agree to secure and protect Customer. PowerSchool requires all subcontractors to execute agreements that include strong data protection requirements, and strictly requires that they not use any student information for purposes other than providing services to PowerSchool. Subcontractors are also subject to audit rights in favor of PowerSchool to ensure ongoing compliance.*
3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
 - a. *Upon written request and in accordance with the applicable terms in Sections 2.2 or 2.3 of the Standard PowerSchool MSA, PowerSchool will dispose or delete all Customer Data within a commercially reasonable time period when it is no longer needed for the purpose for which it was obtained. Customer must inform PowerSchool when Customer Data is no longer needed. Disposition will include (1) the shredding of any hard copies of any Customer Data; (2) erasing; or (3) otherwise modifying the personal information in those records to make the information unreadable or indecipherable by human or digital means. Nothing in this Agreement authorizes PowerSchool to maintain Customer Data beyond the time period reasonably needed to complete the disposition. Upon request by Customer, PowerSchool will provide written notification to Customer when all Customer Data have been disposed. Upon receipt of a request from Customer, PowerSchool will provide Customer return of Customer Data, within ten (10) calendar days of receipt of said request, as commercially reasonable. Customer acknowledges there may be a reasonable service fee attached to such data return service where more than two (2) such service request is submitted by the Customer during the term. PowerSchool will promptly provide a copy of the Customer Data in PowerSchool's possession at termination or expiration of the Agreement and will certify in writing delivery to Customer.*
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
 - a. *Complaints should be directed to: the Associate Superintendent for Curriculum ~~you're~~ 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.
 - a. *Data is stored on third party cloud system only with the United States. Data is encrypted at rest and in transit. Only authorized CloudOps team members have access to the data on need to know basis. Access to data is controlled by access control mechanisms. PowerSchool will employ industry standard measures to protect data from unauthorized access. The service security measures will include server authentication and data encryption. PowerSchool will host data pursuant to this Agreement in an environment using a firewall that is updated according to industry standards.*

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.