



## **STUDENT DATA PRIVACY AGREEMENT**

**STATE: NEW YORK**

**PROCESSOR:**        **PowerSchool Group, LLC**

**CUSTOMER:**        **Albany-Schoharie-Schenectady-Saratoga BOCES**



This Data Privacy Agreement (“**DPA**”) supplements the agreed to license and service agreement for the PowerSchool Services between the PowerSchool Contracting Entity (“**PowerSchool**”) and Albany-Schoharie-Schenectady-Saratoga BOCES (“**Customer**”) and is made and entered into as of the last signature below, (the “Effective Date”). The terms herein supplement and amend the terms of the PowerSchool’s standard Main Services Agreement or, if there is none, the then-existing applicable agreement between PowerSchool and Customer for the provision of PowerSchool’s services and products, as amended by the Parties from time to time (the “**MSA**”). The term “MSA” includes all exhibits, addenda, statements of work, and quotes that are attached to, referenced in or otherwise associated with the MSA. In the event of a conflict between the MSA and this DPA, the DPA controls. Below are the terms and conditions pursuant to which any Customer Data will be handled by PowerSchool and permitted third parties during the term of the MSA and after its termination. Any capitalized terms not defined herein shall have the meaning given to them in the MSA. PowerSchool and Customer are individually known as a “Party” and collectively referred to as “Parties.”

Attachments:

- A Services Description
- B Parents’ Bill of Rights for Data Privacy and Security

The Processor agrees as follows:

1. Definitions.

“Confidential Information” means (a) Protected Information; (b) any personally identifiable information related to CUSTOMER employees, agents and/or volunteers obtained by or furnished to the Processor; (c) all findings, analysis, data, reports or other information, whether in oral, written, graphic, or machine-readable form, obtained from the CUSTOMER or furnished by the CUSTOMER to the Processor in connection with the Services; and (d) all information marked “confidential” in writing.

Confidential Information excludes any information that both (a) is not Protected Information and (b) is: (i) lawfully in the public domain at the time of receipt or which lawfully comes into the public domain thereafter through no act of the Processor in breach of this Agreement, (ii) demonstrated to have been known to the Processor prior to disclosure by or through the CUSTOMER, (iii) disclosed with the prior written approval of the CUSTOMER, (iv) demonstrated to have been independently developed by the Processor without reference to the Confidential Information, and (v) disclosed to the Processor by a third party under conditions permitting such disclosure, without breach of this Agreement.

“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, or any successor thereto.

“Process” or “Processing” means to perform any act, omission or operation on or with respect to data or information, such as accessing, adapting, altering, blocking, collecting, combining, delivering, deleting, destroying, disclosing, disseminating, erasing, generating, learning of, organizing, recording, releasing, retrieving, reviewing, sharing, storing, transmitting, using or otherwise making data or information available.

“Protected Information,” as it relates to (a) CUSTOMER’s current, future and former students and their families, consists of “personally identifiable information” as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and its implementing regulations, 34 C.F.R. Part 99 (“FERPA;”) and (b) as it relates to certain CUSTOMER employees, consists of “personally identifying information” as that



term is used in New York Education Law 3012-c(10). In the case of either (a) or (b), Protected Information shall consist of any such information Processed by the Processor in the course of providing the Services, whether disclosed or provided by the CUSTOMER or collected, accessed or generated by the Processor in some other manner.

2. Confidentiality. Subject to any security review as required by the CUSTOMER Division of Instructional and Information Technology at its discretion, in furtherance of the use of Processor’s software and/or services on behalf of the CUSTOMER (the “Services,”) the Processor is permitted to Process the CUSTOMER’s Confidential Information as set forth in the Service Description, attached hereto as Attachment A. In accordance with FERPA, the Processor agrees that to the extent that the Services relate to the Processor’s Processing of Protected Information, the Services are (a) for the Processor to perform an institutional service or function for which the CUSTOMER would otherwise use its employees; or (b) in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. The Processor further agrees that it is hereby designated as the authorized representative of the CUSTOMER to the extent that the Services are in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. The Processor agrees to hold the Confidential Information in strict confidence, and not to disclose Confidential Information to or otherwise permit the Processing of Confidential Information by any other parties, nor Process such Confidential Information for the benefit of another or for any use or purpose other than for providing the Services. The confidentiality and data security obligations of the Processor under this Agreement shall survive any termination of this Agreement. The Processor agrees to conduct the Services in a manner that does not permit the personal identification of parents and students by anyone other than Authorized Users with legitimate interests in the Protected Information.

3. Authorized Users. The Processor shall only disclose Confidential Information to its employees (hereinafter referred to as “Personnel”), and its nonemployee agents, assignees, consultants or subcontractors (hereinafter collectively referred to as “Non-Employee Processors,” and together with Personnel, “Authorized Users”) who need to Process the Confidential Information in order to carry out the Services and in those instances only to the extent justifiable by that need. The Processor shall ensure that all such Authorized Users comply with the terms of this Agreement. The Processor agrees that upon request by the CUSTOMER, it will provide the CUSTOMER with the names and affiliations of the Non-Employee Processors to whom it proposes to disclose, or has disclosed, Confidential Information. The Processor agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of this Agreement, shall apply to any Non-Employee Processor it engages to Process Confidential Information of the CUSTOMER. The Processor therefore agrees to ensure that each Non-Employee Processor is contractually bound by an agreement that includes confidentiality and data security obligations equivalent to, and no less protective than, those found in this Agreement.

4. Compliance with Law.

- (a) The Processor agrees to hold all Confidential Information it Processes in compliance with all applicable provisions of federal, state and local law, including but not limited to FERPA and New York Education Law §2-d and any applicable regulations promulgated thereunder. The Processor understands that the disclosure of Protected Information to persons or agencies not authorized to receive it is a violation of United States federal law and New York state law, which may result in civil and/or criminal penalties under New York State and Federal laws.
- (b) In the event that disclosure of Confidential Information (including Protected Information) is required of the Processor under the provision of any law, judicial order or

lawfully-issued subpoena, the Processor will (a) promptly notify the CUSTOMER of the obligations to make such disclosure sufficiently in advance of the disclosure, if possible, to allow the CUSTOMER to seek a protective order or to make any notifications required by law, and (b) disclose such Confidential Information only to the extent (i) allowed under a protective order, if any, or (ii) necessary to comply with the law or court order.

5. Mandatory N.Y. Education Law 2-d Requirements.

- (a) CUSTOMER Data Privacy and Security Policies. The Processor agrees that it will comply with the CUSTOMER's data privacy and security policy, and any successor thereto.
- (b) Subject Data Requests. If permitted by law, the Processor agrees to notify the CUSTOMER of any requests it receives from parents, students, principals or teachers ("Subjects") or parties authorized by Subjects, to amend, inspect, obtain copies of, or otherwise access Protected Information in the possession or control of the Processor, in advance of compliance with such requests. The Processor shall defer to the judgment of the CUSTOMER in granting or denying such requests, and in confirming the identity of Subjects and the validity of any authorizations submitted to the Processor. The Processor agrees to assist the CUSTOMER in processing such requests in a timely manner, whether received by the Processor or by the CUSTOMER. The Processor shall amend any Protected Information in accordance with the CUSTOMER's decision and direction.
- (c) Training. The Processor shall ensure that all Authorized Users with access to the Confidential Information are trained in their confidentiality and data security responsibilities under applicable law and understand the privacy and data security obligations of this Agreement.
- (d) Privacy and Security Plan; Additional Data Privacy and Security Protections. The Processor shall neither retain nor incorporate any of the Confidential Information into any database or any medium other than may be required for it to provide the Services. The Processor agrees to maintain appropriate administrative, technical and physical safeguards in accordance with industry standard practices and applicable law to protect the security, confidentiality and integrity of Protected Information in its custody. The Processor agrees to adhere to (a) its data privacy and security plan and the CUSTOMER Information Security Requirements as adjusted with compensating controls as described in Attachment B (together, the "Plan"), attached hereto as Attachment B. The Processor warrants and represents that (i) its technologies, safeguards and practices, as outlined in the Plan, align with the NIST Cybersecurity Framework, and include sufficient (A) data privacy protections, including processes to ensure that personally identifiable information is not included in public reports or other public documents; and (B) data security protections, including data systems monitoring, encryption of data in motion and at rest, an incident response plan, limitations on access to Protected Information, safeguards to ensure Protected Information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of Protected Information when no longer needed; and (ii) its Plan meets all additional requirements of New York Education Law 2-d. The Processor agrees to use encryption technology to protect Protected Information while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5. The Processor acknowledges and agrees to conduct digital and physical periodic risk

assessments and to appropriately remediate any identified security and privacy vulnerabilities in a timely manner. The CUSTOMER reserves the right to request information from the Processor regarding its security practices and compliance with the Plan, prior to authorizing any exchange of Confidential Information. The Processor's security compliance is assessed by independent third-party auditors as described in the following industry standards. Upon CUSTOMER agreeing to an NDA, Processor shall provide access to Processor's Information Security Management System Policy, relevant annual penetration test reports, and ISO 27001:2103and SOCII Reports. To the extent that Processor discontinues a third-party audit, Processor will adopt or maintain equivalent industry-recognized security standard procedures and policies. The CUSTOMER may audit the Processor's Processing of the Confidential Information for data privacy and data security purposes. For clarity, such "audit" means an annual security and privacy questionnaire followed by a reasonable number of interview sessions with applicable CUSTOMER staff; a CUSTOMER review of Processor's security and privacy related policies and procedures; and, in coordination with Processor's Information Security department, an annual scheduled penetration test of identified systems not impacting any other customers.

- (e) Parent Bill of Rights. The Processor agrees to comply with the CUSTOMER Parents' Bill of Rights for Data Privacy and Security, attached hereto as Attachment B. The Processor shall complete the Supplemental Information section of Attachment C and append it to this Agreement. The Processor shall notify the CUSTOMER on a yearly basis, by January 31 of each year that this Agreement remains in effect, of any change to its responses to Attachment C. The Processor acknowledges and agrees that the CUSTOMER shall make the Processor's Supplemental Information public, including but not limited to posting it on the CUSTOMER's website. The Processor acknowledges that this Agreement, including the attachments hereto, may be made available to the public.
  
- (f) Reportable Data Events. The Processor shall promptly notify, without unreasonable delay the CUSTOMER at Phone number and email address ) of (i)any unauthorized release or unauthorized Processing of Confidential Information, whether by the Processor, its Authorized Users or any other party that shall have gained access to the affected Confidential Information; or (ii)any other breach of contractual obligations relating to data privacy and security under this Agreement or any other applicable Agreement("Reportable Data Event"). In no event shall such notification occur more than forty-eight (48) hours after confirmation of an event described in clause (i)of the previous sentence, or more than seven (7) calendar days after confirmation of an event described in clause (ii) of the previous sentence. Moreover, to the extent(a) New York Education Law 2-d or any other law or regulation requires parties affected by the Reportable Data Event to be notified, and (b)the Reportable Data Event is not attributable to the acts or omissions of the CUSTOMER, the Processor shall be responsible, at its own cost and expense, to notify in writing all persons affected by the Reportable Data Event, or shall compensate the CUSTOMER for the full cost of any notifications that the CUSTOMER instead makes. The Processor and CUSTOMER will collaborate to support such notification. The Processor agrees to assist and collaborate with the CUSTOMER in ensuring that required notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: (a) a brief description of the Reportable Data Event, the dates of the incident and the date of discovery, if known; (b) a description of the types of Confidential Information affected; (c)an estimate of the number of records affected;(d) a brief description of the investigation or plan to investigate; and (e) contact information for

representatives who can assist parents or adult students that have additional questions. Processor follows its established incident response plan which ensures the CUSTOMER receives updates from knowledgeable Processor employees of the Reportable Data Event. If requested, Processor shall provide the CUSTOMER with access to Processor's Authorized Users or other employees with knowledge of the Reportable Data Event. The Processor shall reasonably cooperate with and assist the CUSTOMER in investigating the Reportable Data Event or in effectuating notifications, including reasonable disclosure of any relevant access information, records or other material necessary for such purposes or required to comply with applicable law.

- (g) No Sale or Commercial Use. The Processor agrees that it will not (i) sell Protected Information; (ii) use, disclose or otherwise Process Confidential Information for purposes of receiving remuneration, whether directly or indirectly; or (iii) use, disclose or otherwise Process Confidential Information for marketing, commercial or advertising purposes (or facilitate its Processing by any other party for such purposes), or to develop, improve or market products or services to students, or permit another party to do so.

6. Right to Termination. The CUSTOMER shall have the right at its sole discretion to terminate the Processor's access to the CUSTOMER's Confidential Information upon fifteen (15) days written notice to the Processor. The CUSTOMER shall have the right at its sole discretion to terminate the Processor's access to the CUSTOMER's Confidential Information immediately upon the Processor's breach of any confidentiality obligations herein. No claim for damages will be made or allowed to the Processor because of said termination.

7. Confidential Information Retention, Transfer and Destruction. Upon the earliest of any of the following (i) whenever requested by the CUSTOMER, (ii) whenever the Processor no longer needs the Confidential Information to provide the Services to the CUSTOMER, (iii) whenever a CUSTOMER school or office ceases use of a product or service of the Processor, with respect to the Confidential Information Processed for the school or office with respect to that product or service, or (iv) no later than upon termination of this Agreement, the Processor shall promptly. (a) with respect to physical copies of Confidential Information, surrender, or if surrender is not practicable, securely delete or otherwise destroy Confidential Information and (b) with respect to digital and electronic Confidential Information, securely delete or otherwise destroy Confidential Information remaining in the possession of the Processor and its Authorized Users, including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data. The Processor shall ensure that no copies, summaries, or extracts of Confidential Information are retained on any storage medium whatsoever by the Processor or its Authorized Users. The Processor shall certify, in writing, that Confidential Information has been surrendered or destroyed in accordance with this Agreement via the "Certificate of Records Disposal" form attached to this Agreement as Attachment D. Any and all measures related to the extraction, deletion, transmission, destruction or disposition of Confidential Information will be accomplished utilizing an appropriate method of confidential destruction, including shredding, burning or certified/witnessed destruction of physical materials or verified erasure of magnetic media using approved methods of electronic file destruction. The Processor agrees not to attempt to re-identify, or have others attempt to re-identify, Subjects from any data remaining after such deletion, destruction or disposition. If student-, parent- or employee-generated content is stored or maintained by the Processor, Processor shall, at the request of the CUSTOMER, and if severable, provide opportunity to CUSTOMER to download Confidential Information upon termination of this Agreement.

8. CUSTOMER Property. All reports and work product containing Confidential Information (a) created or collected by the Processor, or (b) disclosed or transmitted to the Processor,





pursuant to this Agreement, shall remain the exclusive property of the CUSTOMER. All rights, including the intellectual property rights in and to the Confidential

Information Processed pursuant to this Agreement shall remain the exclusive property of the CUSTOMER. Any reports or work product may not contain any Confidential Information, unless required by the CUSTOMER or if necessary to carry out the Services.

9. Other Agreements. The Processor agrees that to the extent that any confidentiality or data security terms or conditions regarding the Services found in another agreement binding CUSTOMER employees, subcontractors, parents or students (together, “CUSTOMER Users,”) including but not limited to any end-user license agreement, “clickwrap,” “click-through,” “click and accept,” “web-wrap,” or other form of agreement requiring the individual user to accept terms in order to use or benefit from the Services, conflict with the terms found in this Agreement, the terms and conditions which afford more protection to CUSTOMER Users shall apply. Any subsequent agreements between the Processor and the CUSTOMER with respect to the provision of the Services shall include confidentiality and data security obligations on the part of the Processor at least as strict as set forth in this Agreement. In the event a subsequent agreement fails to contain confidentiality and data security provisions with obligations at least as strict as this Agreement, the confidentiality provisions of this Agreement shall be deemed inserted therein, and shall continue to bind the Processor, unless such subsequent agreement specifically references this Agreement by name and disclaims its obligations in writing.

10. Other Terms.

- (a) As a supplement to the existing injunctive relief provisions in the underlying subscription/services agreement, the Processor agree that money damages would be an insufficient remedy for breach or threatened breach of this Agreement. Accordingly, in addition to all other remedies that DOE may have, DOE shall be entitled to enforce the data-security provisions of this Agreement by seeking specific performance or other equitable relief as a remedy for any breach that is not cured after 24-hours’ notice.
- (b) Nothing in this Agreement obligates either party to consummate a transaction, to enter into any agreement or negotiations with respect thereto, or to take any other action not expressly agreed to herein.
- (c) The Processor shall defend, indemnify and hold harmless the CUSTOMER from any and all claims brought by third parties to the extent arising from, or in connection with, any negligent acts or omissions of the Processor and the Processor’s Authorized Users or any other representatives for whom the Processor is legally responsible for, in connection with the performance of this Agreement.
- (d) No failure or delay (in whole or in part) on the part of either party hereto to exercise any right or remedy hereunder shall impair any such right or remedy, operate as a waiver thereof, or affect any right or remedy hereunder. All rights and remedies hereunder are cumulative and are not exclusive of any other rights or remedies provided hereunder or by law or equity. To the extent any provision of this Agreement is held to be unenforceable or invalid, the remainder of the Agreement shall remain in full force and effect, and the Agreement shall be interpreted to give effect to such provision to the maximum extent permitted by law.
- (e) This Agreement shall be governed by and construed in accordance with the law of the State of New York. The Federal or State Courts of New York, New York will have exclusive jurisdiction to adjudicate any dispute arising under or in connection with this Agreement. This Agreement constitutes the entire Agreement with respect to the subject matter hereof; it supersedes any other Processor terms and conditions, all prior agreements or understandings of the parties, oral or written, relating to the subject matter of this



Agreement and shall not be modified or amended except in writing signed by the Processor and the CUSTOMER. The Processor may not assign or transfer, without the prior written consent of the CUSTOMER, this Agreement. This Agreement shall inure to the benefit of the respective parties, their legal representatives, successors, and permitted assigns. This Agreement is effective upon execution of the Processor.






IN WITNESS WHEREOF, the Parties' authorized signatories have duly executed this Agreement on the date set forth below, effective as of the Effective Date.


**PROCESSOR**

**CUSTOMER**

POWERSCHOOL GROUP LLC, a Delaware limited liability company

Albany-Schoharie-Schenectady-Saratoga BOCES

By: 

By: 

Name: Eric Shander

Name: Kelly Rose Yaeger, Esq.

Title: Chief Financial Officer

Title: Data Protection Officer

Date: February 16, 2024

Date: 2/20/2024

SIGNATURE PAGE FOR THE STUDENT DATA PRIVACY AGREEMENT (NEW YORK) BETWEEN POWERSCHOOL AND ALBANY-SCHOHARIE-SCHENECTADY-SARATOGA BOCES

## **Attachment A: Services Description**

**Naviance CCLR:** Naviance is a college and career readiness platform that Naviance helps students explore goal setting, career interests, academic planning, and college preparation, while operating as the system of records for schools and districts. (former product name: PowerSchool Unified Classroom Naviance CCLR)

**Enrollment:** Enrollment is an enterprise enrollment product that facilitates student acquisition and registration business process through data collection from parents, administrative workflows, data integration with various SIS's, and lotteries, streamlining related business processes. Registration is a multitenant cloud-based web application. (former product name: PowerSchool Unified Operations Enrollment)

**Enrollment Express:** Enrollment Express is a student enrollment management system inside PowerSchool SIS. (former product name: PowerSchool Unified Operations Enrollment Express)

**Performance Matters:** Performance Matters and its Advanced Reporting feature brings multiple data measures into one location to help school districts identify, monitor, and improve student performance. Dashboards provide access to state and national test scores, third-party diagnostic results, and district-based common formative assessments to give you the data needed to inform decisions for your schools, district, and students. (former product: PowerSchool Unified Classroom Performance Matters Advanced Reporting)

**Performance Matters:** Performance and its Matters Assessment offers a school-wide assessment management system for curriculum teams to build student assessments for use across grade levels, content areas, and schools. Various assessment delivery methods are available including online testing, scanning, and observational scoring tools. The data is available within minutes to view how students performed on standards, each item, and overall making data-driven decisions about instructional needs quick and easy for teachers. (former product: PowerSchool Unified Classroom Performance Matters Assessment)

**PowerSchool SIS:** Our PowerSchool SIS solution provides deep functionality across PowerSchool solutions empowering schools to configure the administrative and instructional tools for their unique needs, from managing classroom data and assignments to family engagement, student enrollment and registration, student analytics, and special education. (former product name: Unified Classroom PowerSchool SIS)

**Employee Records:** Digitizing processes with Employee Records simplifies onboarding. Online checklists, digital storage, centralized tracking, automated alerts, and information forwarding combine to create a more positive experience. Say goodbye to the calls, emails, and tedious verifications that hamper traditional, paper-based onboarding processes. (former product name: PowerSchool Unified Talent Employee Records)

**Schoology Learning:** Schoology Learning Management System (LMS) provides learning management, assessment, and professional development all in one integrated platform. Be prepared for inevitable changes and challenges with a more flexible and reliable approach to teaching and learning while providing consistent access to learning resources across your whole district. (former product name: PowerSchool Unified Classroom Schoology Learning)



**Curriculum and Instruction:** Provide centralized access to shared curriculum so teachers can collaborate in real-time and connect curriculum directly to their lesson plans. Streamline horizontal and vertical standards alignment with our integrated digital curriculum mapping and lesson planning solution. (former product name: PowerSchool Unified Classroom Curriculum and Instruction)

**Special Programs:** Special Programs gives special education staff the support they need to simplify case management, collaborate with general education staff, save time, and meet compliance requirements with confidence. This allows special education staff the ability to provide high-quality instruction, services, and appropriate modifications and accommodations for students with disabilities. (former product name: PowerSchool Unified Classroom Special Programs)

**Behavior Support:** Support the whole child with the only evidence-based (ESSA Level II) behavior solution proven to reduce suspensions and referrals and increase school positivity. Educators can collect and analyze real-time data to further positive behavior support and interventions (PBIS) and social and emotional learning (SEL). (former product name: PowerSchool Unified Classroom Behavior Support)

**Communication:** Improve communication between school and home by engaging in two-way conversations that create partnerships between educators and families. Improve equity of access by reducing technology gaps and language barriers with two-way translated text messaging, multimedia messaging, and more. (former product name: PowerSchool Unified Operations Communication; Unified Home Communication, Kinvo Connect)

**Attendance Intervention:** Perform research-based attendance interventions that use best-practice, data-driven family engagement tools that are proven to address the root causes and improve attendance and engagement. Track and view actionable attendance data and strengthen and simplify school-home connections by communicating in real-time via two-way translated text notifications, multimedia messages, visual postcards, and more. (former product name: PowerSchool Unified Operations Attendance Intervention Suite; and Kinvo Attend)

**Student Readiness Analytics, Risk Analysis and MTSS:** Unified Insights provides a comprehensive analytics platform with actionable insights across key aspects of school and district operations and allows district staff to extract student data, create notifications, gain access with mobile devices, and distribute reports throughout the entire district. (former product name: Unified Insights)

**Perform:** K-12 teacher evaluation software that Improves teacher support and retains effective educators. Manage and conduct teacher evaluations and observations online or in person. (former product name: PowerSchool Unified Talent Perform)

**Professional Learning:** Provides professional learning for teachers that supports career growth with easier professional development management and 24/7 accessibility. (former product name: PowerSchool Unified Talent Professional Learning)

**SmartFind Express:** K-12 substitute teacher management software that automates callouts and streamlines online substitute management to quickly fill teacher and staff absences. (former product name: PowerSchool Unified Talent SmartFind Express)

**Applicant Tracking:** Helps schools and districts hire the teachers and staff they need faster and easier. (former product name: PowerSchool Unified Talent Applicant Tracking)

## ATTACHMENT B

### PARENTS' BILL OF RIGHTS FOR STUDENT

#### DATA PRIVACY AND SECURITY

Capital Region BOCES, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. 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;
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov/data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, (518) 464-5139, [DPO@neric.org](mailto:DPO@neric.org), Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov/data-privacy-security> by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to [privacy@nysed.gov](mailto:privacy@nysed.gov) or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, (518)-464-5139, [DPO@neric.org](mailto:DPO@neric.org), 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on BOCES' website <https://www.capitalregionboces.org/>.

## Parents Bill of Rights for Data Privacy and Security—Supplemental Information

### I. Explanation and Instructions

Pursuant to New York Education Law §2-d and 8 N.Y.C.R.R 121.3, Albany-Schoharie-Schenectady-Saratoga BOCES is required to supplement its Parents Bill of Rights for Data Privacy and Security with additional information concerning a written agreement (“Agreement”) under which an outside entity (“Entity”) will receive personally identifiable information from education records of students (“PII”; see full definition below). In accordance with these provisions, it is necessary for you to provide a complete and accurate response to each item below. If an item is not applicable to your agreement with Albany-Schoharie-Schenectady-Saratoga BOCES, explain why. Your responses will be posted are subject to review and approval by the Albany-Schoharie-Schenectady-Saratoga BOCES, and will be posted to the Albany-Schoharie-Schenectady-Saratoga BOCES website.

Please note that New York Education Law 2-d defines PII as follows:

1. With respect to student data, personally identifiable information from the DOE’s education records, including but not limited to the following:
  - a. The student's name;
  - b. The name of the student's parent or other family members;
  - c. The physical or electronic address, device number (including telephone and mobile phone numbers, geolocation information and IP addresses) and other contact information of the student or student's family;
  - d. A personal identifier, such as the student's social security number, student number, or biometric record (including but not limited to fingerprints, facial images, iris scans and handwriting);
  - e. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
  - 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—including combinations of demographic, performance and school information that could lead to the student being identified); and
  - 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.
2. With respect to teacher or principal data, any annual professional performance review (APPR) data disclosed by the DOE to the Entity on an identifiable basis.

Please note that “education records” include records directly related to a student and maintained by **or on behalf of** the DOE. Accordingly, to the extent the Entity is providing a service or function on behalf of the DOE, education records, and the PII found in it, includes information that the Entity may collect directly from parents or students.

With respect to any explanation the Entity provides below in response to the questionnaire:



- Albany-Schoharie-Schenectady-Saratoga BOCES reserves the right to review and reject them, or request further explanation. Note that certain options below match federal and state legal requirements, and deviations will need to be reviewed and considered on a case-by-case basis.
- Phrase your responses so that public posting of it will not jeopardize the security of PII or your data protection processes.
- Do not refer back to your written agreement with the Albany-Schoharie-Schenectady-Saratoga BOCES, or use defined terms found elsewhere in the agreement or in other documents. Your explanations must stand on their own, since they will be posted publicly.
- Ensure that it is clear and uses plain English, because the audience for it consists of Albany-Schoharie-Schenectady-Saratoga BOCES parents, staff, students and other interested members of the public.

## II. Questionnaire

### 1. Name of Entity

**PowerSchool Group LLC**

### 2. Type of Entity

- Commercial Enterprise
- Research Institution or Evaluator
- Community Based Organization or Not-for-Profit
- Government Agency
- Other (You must explain below)

Click or tap here to enter text.

### 3. Contract / Agreement Term

Contract Start Date: \_\_\_\_\_

Contract End Date: \_\_\_\_\_

### 4. Description of the exclusive purpose(s) for which Entity will receive/access PII

Describe briefly the project/evaluation/research you are conducting or participating in, and/or the commercial product or service you are providing. Describe the purposes for which you are receiving or accessing PII.

### 5. Type of PII that the Entity will receive/access

Check all that apply:

Student PII

APPR PII (Identifiable Teacher or Principal Annual Professional Performance Review Data)

Entity will not receive or access PII (do not choose this response if Entity's services or products permit users to store PII on a platform that the Entity or its subcontractors host)

Other (You must explain below)

[Click or tap here to enter text.](#)

## 6. Subcontractor Written Agreement Requirement

In accordance with New York Education Law 2-d, the Entity may not share PII with subcontractors without a written agreement that requires each of its subcontractors to adhere to, at a minimum, materially similar—and no less protective—data protection obligations imposed on the Entity by the Agreement with the Albany-Schoharie-Schenectady-Saratoga BOCES and by applicable state and federal laws and regulations.

Check one option only:

The Entity will not share PII with subcontractors, outside persons, or third party entities.

The Entity will utilize subcontractors or third party entities and agrees not share PII unless similar data protection obligations contained herein are imposed on each subcontractor or third party, in compliance with applicable New York State and federal law and using industry standard best practices for data privacy and security.

Other (You must explain below)

[Click or tap here to enter text.](#)

## 7. Data Transition and Secure Destruction

Upon expiration or termination of the Agreement, the Entity shall (check all that apply):

Securely transfer PII to Albany-Schoharie-Schenectady-Saratoga BOCES, or a successor contractor at the Albany-Schoharie-Schenectady-Saratoga BOCES's option and written discretion, in a format agreed to by the parties

Securely delete and/or destroy PII

Other (You must explain below)

[Click or tap here to enter text.](#)

## 8. Challenges to Data Accuracy

In accordance with N.Y. Education Law 2-d, parents, students, eligible students, teachers, or principals may seek copies of their PII, or seek to challenge the accuracy of PII in the custody or control of the Entity. Typically, they can do so by contacting the Albany-Schoharie-Schenectady-Saratoga BOCES using the email address or mailing address below. If a correction to PII is deemed necessary, the Entity agrees to facilitate such corrections within 21 days of receiving the Albany-Schoharie-Schenectady-Saratoga BOCES's written request. The Entity must forward the request to the Albany-Schoharie-Schenectady-Saratoga BOCES as soon as practicable in order for the DOE to authenticate the identity of the student or parent, and to advise the Entity on how to process the request.

All requests for copies of PII or requests to challenge the accuracy of PII should be directed to the following email address: [dpo@neric.org](mailto:dpo@neric.org).

Please select one option only:

- The Entity agrees to the procedure outlined above
- Other (You must explain below)

[Click or tap here to enter text.](#)

## 9. Security and Storage Protections

Describe where PII will be stored or hosted (check all that apply)

- Using a cloud or infrastructure owned tool hosted by a subcontractor
- Using an Entity-owned and/or internally hosted-solution
- No PII will be stored or hosted by Entity
- Other (you must explain below):

[Click or tap here to enter text.](#)

**10. Describe the administrative, technical and/or physical safeguards to ensure PII will be protected and how the Entity will mitigate data privacy and security risks. (Please do so in a manner that ensures that disclosure of the description on Albany-Schoharie-Schenectady-Saratoga BOCES's website will not compromise the security of the data or the Entity's security practices and protocols):**

### **Data Security and Privacy Plan**

Processor agrees that it will protect the security, confidentiality, and integrity of the Customer Data it receives from Customers in accordance with customer's Parents' Bill of Rights for Data Privacy and Security.

Additional elements of Processor's Data Security and Privacy Plan are as follows:

- (a) To implement all state, federal, and local data security and privacy requirements, including those contained within this Data Security and Privacy Plan (“DSPP”), consistent with customer’s data security and privacy policy, Processor will: Review its data security and privacy policy and practices to ensure they are in conformance with all applicable federal, state, and local laws and the terms of this DSPP. In the event Processor’s policy and practices are not in conformance, Processor will implement commercially reasonable efforts to ensure such compliance.
- (b) As required by the NIST Cybersecurity Framework, to protect the security, confidentiality and integrity of the Customer Data that it receives under the MSA, Processor will have the following reasonable physical, administrative, and technical safeguards and practices in place throughout the term of the Agreement:
- Data Security:*
- Processor ensures that both data-at-rest and data-in-transit (motion) is encrypted, and data leak protections are implemented.
- Information Protection Processes and Procedures:*
- Processor performs data destructions according to the terms set in contracts and agreements. Processor also possesses a vulnerability management plan that will be developed and implemented.
- Protective Technology:*
- To ensure that network communications are protected, log/audit records are ascertained, implemented, documented, and reviewed according to Processor/District policy.
- Identity Management, Authentication and Access Control:*
- Processor manages remote access through credentials and identities that are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users.
- (c) If Processor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MSA, Processor will require such subcontractors, assignees, or other authorized agents to execute written agreements requiring those parties to protect the confidentiality and security of Protected Data under applicable privacy laws.

## 11. Encryption

Pursuant to New York Education Law 2-d, PII must be encrypted while in motion and while at rest. By checking the box below, Entity agrees that PII will be encrypted using industry standard data encryption technology while Protected Information is in motion and at rest.

Entity agrees that PII will be encrypted in motion and at rest using industry-standard data encryption technology.

Other (you must explain below):

Click or tap here to enter text.