STILLWATER SCHOOL DISTRICT 834 DATA PRIVACY AGREEMENT

Stillwater School District 834

(ISD 279) AND

PowerSchool Group LLC

August 10, 2022

This Data Privacy Agreement ("DPA") is entered into by and between the Stillwater School District 834 (hereinafter referred to as "LEA") and PowerSchool Group LLC (hereinafter referred to as "Provider") on August 10, 2022. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to the Minnesota Government Data Practices Act ("MGDPA")Minn. Stat. Chapter 13 ; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, MGDPA and other applicable Minnesota State laws, all as may be amended from time to time. In performing services requiring access to private records/data on students, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA.

2. Nature of Services Provided. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

Ecollect: Ecollect digitizes forms to support district initiatives.

Enrollment (fka Registration): 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.

Performance Matters Analytics: Performance Matters Analytics provides more insights into school and district performance to identify, monitor and improve student performance. Dashboards provide access to the data needed by customers related to their schools, district and students.

Performance Matters Assessment: Performance Matters Assessment offers a districtwide assessment product for curriculum teams to build student assessments for use across schools. Performance Matters Assessment delivers easy scoring methods, consistent assessment across schools, and student learning data.

PowerSchool SIS: Our 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.
Schoology LMS: Schoology LMS provides learning management, assessment, and professional development all in one integrated platform.

Unified Insights (aka Hoonuit): 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.

Unified Talent: PowerSchool Unified Talent solution gives schools, districts, and boards the tools to attract, hire, support, develop, and retain talent, including: (i) use research-backed hiring tools to quickly find the right educators and staff; (ii) tailoring professional learning with student achievement insights and performance evaluations to maximize growth and teacher retention; (iii) empowering HR staff with a full suite of flexible tools to streamline and automate everyday processes so they can focus on what matters; and (iv) an ability to scale with the customer's existing systems and processes.

3. Data to Be Provided. The Parties shall indicate the categories of data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. DPA Definitions. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. Data Property of LEA. All LEA data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such LEA data transmitted to the Provider are subject to the provisions of this Agreement in the same manner as the original LEA Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to LEA Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. Separate Account. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

3. Third Party Request. The Provider will report immediately to the District any requests from third parties for information related to this Contract. Unless agreed otherwise, the District will respond to such data requests. If Provider is subject to compelled disclosure to a third party (e.g. lawfully issued subpoena or court order), Provider must provide timely notification to the LEA in advance of such compelled disclosure, unless prohibited.

4. Subprocessors. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect LEA Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. Privacy Compliance. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, MGDPA and all other Minnesota privacy statutes.

2. Annual Notification of Rights. If the LEA has a policy of disclosing education records under FERPA (34 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. Reasonable Precautions. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. Unauthorized Access Notification. LEA shall notify Provider promptly of any known or

suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, MGDPA and all other Minnesota privacy statutes. Provider agrees that any information it creates, collects, receives, stores, uses, or disseminates during the course of its performance, which concerns the personal, financial, or other affairs of the LEA, its Board, officers, employees or students shall be kept private and in conformance with all state and federal laws relating to data privacy, including, without limitation, the MGDPA.

2. Authorized Use. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any LEA Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the LEA Data, without the express written consent of the LEA.

3. Employee Obligation. Provider shall require all employees and agents who have access to LEA Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. No Disclosure. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified LEA Data and not to transfer de-identified LEA Data to any party unless that party agrees in writing not to attempt re-identification. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement, and as allowed under this DPA.

5. Disposition of Data. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all LEA Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any LEA Data; (2) Erasing; or
(3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain LEA Data obtained under the Service Agreement beyond the time period reasonably

needed to complete the disposition. Provider shall provide written notification to LEA when the LEA Data has been disposed. The duty to dispose of LEA Data shall not extend to data that has been de-identified or placed in a separate user account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of LEA Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with any specified portion of the LEA Data within ten (10) calendar days of receipt of said request.

a. Partial Disposal During Term of Service Agreement. Throughout the Term of the Service Agreement, LEA may request partial disposal of LEA Data obtained under the Service Agreement that is no longer needed without cost, up to twice per contract year.

b. Complete Disposal Upon Termination of Service Agreement. Upon Termination of the Service Agreement Provider shall dispose or delete all LEA Data obtained under the Service Agreement. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that data will not be transferred to a separate account.

6. Advertising Prohibition. Provider is prohibited from using or selling LEA Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect LEA Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. Passwords and Employee Access. Provider shall secure employee usernames, passwords, and any other means of gaining access to the Services or to LEA Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to LEA Data to employees or contractors that are performing the Services. Employees with access to LEA Data shall have signed confidentiality agreements. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. Destruction of Data. Provider shall destroy or delete all LEA Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LEA or LEA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain LEA Data beyond the time period reasonably needed to complete the disposition.

c. Security Protocols. Both 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. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purposes of the Service Agreement or data requests by LEA.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. Security Technology. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. Security Coordinator. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the LEA Data received pursuant to the Service Agreement.

g. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect LEA Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and appropriately

remediate identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that LEA Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding seventy-two (72) hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided the number of individuals whose data was potentially subject to the breach and either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.
ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the LEA Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data

breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of LEA Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

f. Unless otherwise directed by the LEA, Provider is required to comply with the disclosure requirements of Minn. Stat. 13.055.

g. In the event of a breach originating from LEA's use of the Service, Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure LEA Data.

ARTICLE VII: MISCELLANEOUS

1. Term. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any LEA Data.

2. Termination. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA if Provider fails to cure within 30 days after written notice by LEA.

3. Effect of Termination Survival. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b). Notwithstanding termination of the Service Agreement and prior to destruction of any data as provided in this agreement, the Provider's obligation to comply with applicable state and federal data privacy laws will continue.

4. Priority of Agreements. This DPA shall govern the treatment of LEA data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. Notice. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the

designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Darron Flagg

Title: Chief Compliance and Privacy Officer

Contact Information:
150 Parkshore Drive
Folsom, CA 95630
legal@powerschool.com

The designated representative for the Provider for this Agreement is:

Name: Omi R

Title: Superintendent

Contact Information:
1895 Greeley St. S.
Stillwater MN 55082

6. Entire Agreement. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in

any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. Governing Law; Venue and Jurisdiction. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. Authority. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of LEA Data and any portion thereof contained therein. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. Waiver. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Osseo Area Schools Data Privacy Agreement as of the last day noted below.

Provider:

BY: _____ Date: August 10, 2022

Printed Name: Eric Shander Title/Position: CFO

Local Education Agency:

BY: _____ Date: 10/7/22

Printed Name: Mike Funk Title/Position: Superintendent

Local Education Agency:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

Note: Electronic signature not permitted.