DATA PROTECTION ADDENDUM

This Data Protection Addendum ("Addendum") is attached to and applies to all services provided by Contractor to District, whether by contract, memorandum of understanding or other form of agreement (the "Contract"), which are quotes Q-471877-1 and Q-468656-2 , by and between School District No. 1 in the City and County of Denver and State of Colorado, d/b/a Denver Public Schools ("District") and PowerSchool Group, LLC ("Contractor") (the Addendum and the Contract are collectively referred to hereinafter as "Agreement"). This Addendum supersedes the Contract by adding to, deleting from and modifying the Contract as set forth herein. To the extent any such addition, deletion or modification results in any conflict or inconsistency between the Contract and this Addendum, this Addendum shall govern and the terms of the Contract that conflict with this Addendum or are inconsistent with this Addendum shall be of no force or effect.

In consideration of the mutual covenants, promises, understandings, releases and payments described in the Contract and this Addendum, the parties agree to amend the Contract by adding the following language:

1. Definitions

1.1. "*Biometric Record*," as used in the definition of "Personally Identifiable Information," means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

1.2. "*Contract*" means quotes Q-471877 and Q-468656-2 , and any other form of agreement signed between the District and Contractor.

1.3. "*Designated Representative*" means District or Contractor employees as specified on Schedule 1 to whom all notices required in this Addendum will be sent.

1.4. "*District Data*" means any Personally Identifiable Information, Record, Education Records, as defined herein, and all Personally Identifiable Information included therein or derived therefrom that is not intentionally made generally available by the District on public websites or publications but is made available directly or indirectly by the District to Contractor or that is otherwise collected or generated by Contractor in connection with the performance of the Services, as defined herein.

1.5. "*De-identified Data*" means District Data from which all Personally Identifiable Information, as defined herein, and attributes about such data, have been permanently removed so that no individual identification can be made.

1.6. "*Education Records*" means records, files, documents and other materials that: (a) contain information directly related to a student; and (b) are maintained by the District, or by a party acting for the District such as Contractor.

1.7. "*End User*" means individuals authorized by the District to access and use the Services as defined herein.

1.8. "*Incident*" means a suspected, attempted, or imminent threat of unauthorized access, use, disclosure, breach, modification, disruption or destruction to or of District Data.

1.9. "*Mine District Data*" means the act of searching through, analyzing, accessing, or extracting District Data, metadata, or information not necessary to accomplish the Services or purpose(s) of this Agreement for the benefit of the District.

1.10. "*Personally Identifiable Information*" or "*PII*" means information and metadata that, alone or in combination, is linked or linkable to a specific student so as to 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. Personally Identifiable Information includes, but is not limited to: (a) the student's name; (b) the name of the student's parent or other family members; (c) the address or phone number of the student or student's family; (d) personal identifiers such as the student's state-assigned student identifier, social security number, student number or biometric record; (e) indirect identifiers such as the student's date of birth, place of birth or mother's maiden name; and (f) demographic attributes, such as race, socioeconomic information, and gender.

To the extent it is not already included in the definition hereinabove, PII also includes: (a) "personal information" as defined in the Colorado Open Records Act, C.R.S. 24-72-101 et seq. ("CORA"); (b) Personally Identifiable Information contained in student "education records" as that term is defined in the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; (c) "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) "nonpublic personal information" as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (e) credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; and (f) other financial account numbers, access codes, and state- or federal-identification numbers such as driver's license, passport or visa numbers.

1.11. "*Record*" means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

1.12. "*Securely Destroy*" means to remove District Data from Contractor's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in National Institute of Standards and Technology ("NIST") SP 800-88 r1 (2014) or as amended Guidelines for Media Sanitization so that District Data is permanently irretrievable in Contractor's and its Subcontractors' normal course of business.

1.13. "*Security Breach*" means an event in which District Data is exposed to unauthorized disclosure, access, alteration or use or a system configuration that results in a documented unsecured disclosure, access, alteration or use, in a manner not permitted in this Addendum, which poses a significant risk of financial, reputational or other harm to the affected End User or the District.

1.14. "*Services*" means any goods or services acquired by the District from the Contractor, or under the contract, including but not limited to computer software, mobile applications (apps), and web-based tools accessed by End Users through the Internet, installed, or run on a computer or electronic device.

1.15. "*Subcontractor*" means Contractor's employees, subcontractors or agents, identified on Schedule 2, as updated by Contractor from time to time in accordance with the requirements of this Addendum, who Contractor has engaged to enable Contractor to perform its obligations under the Contract.

1.16. "*Student Profile*" means a collection of PII data elements relating to a student of the District.

2. Rights and License in and to District Data

District owns all rights, title, and interest in and to District Data, including without limitation, De-identified Data, and any and all now known or hereafter existing intellectual property rights associated therewith, and any derivative works thereof or modifications thereto, although this provision does not amend the intellectual property rights set out in the Contract and does not grant District any rights to Contractor's intellectual property as set out in the Contract. . The District hereby grants to Contractor a limited, nonexclusive license to use District Data solely for the purpose of performing its obligations specified in the Contract. This Agreement does not give Contractor any rights, title, or interest implied or otherwise, to District Data or De-identified Data, except as expressly stated in the Contract.

3. Data Privacy

3.1 Use of District Data. Contractor shall use District Data only for the purpose of performing the Services and fulfilling its duties under the Contract.

3.2 Prohibited Uses of District Data. With the exception of De-identified Data that the District has agreed in writing to allow Contractor to use as specified in Section 3.5, Contractor shall not:

3.2.1 Use, sell, rent, transfer, distribute, alter, mine, or disclose District Data (including metadata) to any third party without the prior written consent of the District, except as required by law;

3.2.2 Use District Data for its own commercial benefit, including but not limited to, advertising or marketing of any kind directed toward children, parents, guardians, or District employees, unless such use is specifically authorized by this Agreement or otherwise authorized in writing by the District;

3.2.3 Use District Data in a manner that is inconsistent with Contractor's privacy policy;

3.2.4 Use District Data to create a Student Profile other than as authorized or required by the Contract to perform the Services; and

3.2.5 Store District Data outside the continental United States unless Contractor has given the District Designated Representative advance written notice of where and how the servers are housed, managed, and secured, and that the security standards required herein can be achieved.

3.3 Qualified FERPA Exception. If Contractor will have access to Education Records, Contractor acknowledges that, for the purposes of this Agreement, pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g and its implementing regulations, 34 C.F.R. Part 99 ("FERPA"), it will be designated as a "school official" with "legitimate educational interests" in the District Education Records and PII disclosed pursuant to the Contract, and Contractor agrees to abide by the FERPA limitations and requirements imposed on school officials. Contractor will use the Education Records only for the purpose of fulfilling its duties under the Contract for District's and its End Users' benefit, and shall not share District Data with or disclose it to any third party except as provided for in the Agreement, as required by law, or if authorized in writing by the District. Contractor warrants and represents that during the five-year period preceding the Effective Date of this Agreement, it has not been found in violation of FERPA by the U.S. Department of Education's Family Policy Compliance Office.

3.4 Subcontractor Use of District Data. To the extent necessary to perform its obligations specified in the Contract, Contractor may disclose District Data to Subcontractors pursuant to a written agreement, specifying the purpose of the disclosure and providing that: (a)

Subcontractor shall not disclose District Data, in whole or in part, to any other party; (b) Subcontractor shall not use any District Data to advertise or market to students or their parents/guardians; (c) Subcontractor shall access, view, collect, generate and use District Data only to the extent necessary to assist Contractor in performing its obligations specified in the Contract; (d) at the conclusion of its/their work under its/their subcontract(s) Subcontractor shall, as directed by the District through Contractor, Securely Destroy all District Data in its/their possession, custody or control, or return such District Data to the District, at the election of the District; and (e) Subcontractor shall utilize appropriate administrative, physical and technical safeguards in accordance with industry standards and best practices to secure District Data from unauthorized disclosure, access and use. Contractor shall ensure that its employees and Subcontractors who have potential access to District Data have undergone appropriate background screening, to the District's satisfaction, and possess all needed qualifications to comply with the terms of this Addendum. Contractor shall also ensure that its Subcontractors comply with the insurance requirements specified in Section 12 of this Addendum.

3.5 Use of De-identified Data. Contractor may use De-identified Data for purposes of research, the improvement of Contractor's products and services, and/or the development of new products and services. In no event shall Contractor or Subcontractors re-identify or attempt to re-identify any De-identified Data or use De-identified Data in combination with other data elements or De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

3.6 Privacy Policy Changes. Prior to making a material change to Contractor's privacy policies, Contractor shall send District's Designated Representative written notice, which includes a clear explanation of the proposed changes. This will be a publicly posted notice available to all of Contractor's customers.

4. Data Security

4.1 Security Safeguards. Contractor shall store and process District Data in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than those outlined in SANS Top 20 Security Controls, as amended, to secure such data from unauthorized access, disclosure, alteration, and use. Contractor shall ensure that all such safeguards, including the manner in which District Data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with all applicable federal and state data protection and privacy laws, regulations and directives, including without limitation C.R.S. § 22-16-101 *et seq.*, as well as the terms and conditions of this Addendum. Without limiting the foregoing, and unless expressly agreed to the contrary in writing, Contractor warrants that all electronic District Data will be encrypted in transmission and at rest in accordance with NIST Special Publication 800-57, as amended.

4.2 Risk Assessments. Contractor shall conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

4.3 Audit Trails. Contractor shall take reasonable measures, including audit trails, to protect District Data against deterioration or degradation of data quality and authenticity, and to ensure data is deidentified in accordance with this Addendum.

4.4 Verification of Safeguards. Upon District's written request, Contractor shall provide or make available to the District for review, one or more of the following, verifying Contractor's administrative, physical and technical safeguards are in compliance with industry standards and best practices: (1) certification from Contractor indicating that an independent vulnerability or risk assessment of the Contractor's data security program has occurred; (2) district data has been deidentified by Contractor as set forth in the definition of Deidentified Data in section 1.3 of this Addendum.

4.5 Background Checks. The Contractor and every person, including any subcontractor or agent of the Contractor, who provides direct services to students, or who has access to student data, shall be required to have a criminal background check that meets the requirements of § 22-32-109.7, C.R.S. and other District requirements. Conducting a Colorado Bureau of Investigation criminal history check or a Name Check investigation for any person providing services under this Contract does not meet District requirements. The costs associated with the background checks are solely the Contractor's responsibility. Thereafter, any personnel, subcontractor, volunteer or agent hired or added during the term of this Contract shall satisfy the requirements set forth in this Section before performing services on Contractor's behalf. The Contractor shall make the background check results available for any individual who has direct contact with students upon request of the District in compliance with the provisions of § 24-72-305.3, C.R.S. The District also reserves the right to conduct its own criminal background check of every person who has direct access to students before Services begin.

4.5.1 Notwithstanding the criminal background check requirement as set forth above, Contractor hereby certifies that no employee, subcontractor, volunteer or agent of the Contractor performing the Services has been convicted in Colorado or in any other State of a criminal offense involving: (i) the abuse, abduction, sexual molestation, physical or sexual assault on, or rape of a minor; or (ii) any crime involving exploitation of minors, including but not limited to, child pornography offenses or any crime of violence. Contractor understands that allowing any employee, subcontractor, volunteer or agent of the Contractor performing the Services who has been arrested or convicted of the aforementioned crimes to: (i) provide direct services to students, (ii) access student data, or (iii) enter onto District property, constitutes a material breach of this Contract and may result in the immediate termination of this Contract and referral to law enforcement for possible criminal charges, or additional civil sanctions pursuant to federal and state law. Misdemeanor conviction(s) may not necessarily result in the immediate

termination of this Contract. Misdemeanor convictions are evaluated on a case-by-case basis, considering the nature and gravity of the offense, time elapsed since the offense, conviction, or time served, and the nature of the Services.

5. Security Incident and Security Breach

5.1 Security Incident Evaluation. In the event of an Incident, Contractor shall follow industry best practices to fully investigate and resolve the Incident, and take steps to prevent developments that may result in the Incident becoming a Security Breach at Contractor's expense in accordance with applicable privacy laws.

5.2 Response. Immediately upon confirmation of a Security Breach, or a complaint of a Security Breach, Contractor shall notify the District Designated Representative in writing as set forth herein, fully investigate the Security Breach, cooperate fully with the District's investigation of and response to the Security Breach, and use best efforts to prevent any further Security Breach at Contractor's expense in accordance with applicable privacy laws. Except as otherwise required by law, Contractor shall not provide notice of the Security Breach directly to individuals whose Personally Identifiable Information was involved, to regulatory agencies, or to other entities, without first providing written notice to the District's Designated Representative.

5.3 Security Breach Report. If the District reasonably determines that Contractor has committed a Security Breach, then the District may request Contractor to submit, within seven (7) calendar days from discovery of such breach, a written report, and any supporting documentation, identifying (i) the nature of the Security Breach, (ii) the steps Contractor has executed to investigate the Security Breach, (iii) what District Data or PII was used or disclosed, (iv) who or what was the cause of the Security Breach, (v) what Contractor has done or shall do to remediate any deleterious effect of the Security Breach, and (vi) what corrective action Contractor has taken or shall take to prevent a future Incident or Security Breach. The District reserves the right to require Contractor to amend its remediation plans.

6. Response to Legal Orders, Demands or Requests for Data

6.1 Received by Contractor. Except as otherwise expressly prohibited by law, Contractor shall immediately notify the District of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking District Data; consult with the District regarding its response; cooperate with the District's reasonable requests in connection with efforts by the District to intervene and quash or modify the legal order, demand or request; and, upon the District's request, provide the District with a copy of its response.

6.2 Received by District. If the District receives a subpoena, warrant, or other legal order, demand or request seeking District Data maintained by Contractor, including but not limited to, a request pursuant to the CORA, the District will promptly notify Contractor and, within two (2) business days, excluding national holidays, Contractor shall supply the District with copies of the District Data for the District to respond.

6.3 Parent Request. If a parent, legal guardian or student contacts the District with a request to review or correct District Data or PII, pursuant to FERPA or the Student Data Transparency and Security Act, C.R.S. § 22-16-101 *et seq*. (the "Act"), the District will promptly notify Contractor's Designated Representative and Contractor shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District, within ten calendar (10) days after receipt of District's notice. Conversely, if a parent, legal guardian or student contacts the Contractor with a request to review or correct District Data or PII, within ten calendar (10) days after receipt of such notice, Contractor shall promptly notify the District and shall use reasonable and good faith efforts to assist the District in fulfilling such requests, as directed by the District.

6.4 Access to District Data. District shall have the right to access and retrieve any or all District Data stored by or in possession of Contractor upon written notice to Contractor's Designated Representative. Contractor shall make the District Data available to the District within seven (7) calendar days from the date of request.

7. Compliance with Applicable Law

7.1. Children's Online Privacy and Protection Act. If Contractor collects personal information (as defined in the Children's Online Privacy and Protection Act of 1998, 5 U.S.C. 6501 to 6505, and its implementing regulations ("COPPA")) from children under thirteen (13) years of age in performing the Services, Contractor warrants, represents, and covenants that such collection is and shall be for the use and benefit of the District and for no other commercial purpose. Contractor has provided District with written notice of its collection, use, and disclosure practices.

7.2 Compliance with Laws. Contractor warrants that it will abide by all applicable laws, ordinances, rules, regulations, and orders of all governmental agencies or authorities having jurisdiction over the Services including but not limited to: (a) COPPA; (b) FERPA; (c) the Health Insurance Portability and Accountability Act, 45 C.F.R. Part 160.103; (d) the Health Information Technology for Economic and Clinical Health Act, (e) Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 U.S.C. 6809; (f) Payment Card Industry Data Security

Standards; (g) Protection of Pupil Rights Amendment, 20 U.S.C. 1232h, 34 C.F.R. Part 98; and (h) Americans with Disabilities Act, and Federal Export Administration Regulations.

7.3 Americans with Disabilities Act. To the extent the District is required to provide accommodations in compliance with the Americans with Disability Act ("ADA"), Contractor will make best efforts to assist the District in providing its services to end users pursuant to this Agreement, and will assistance the District in a manner that its system and services will, upon request, provide District with access to applicable Voluntary Product Accessibility Templates (VPATs) to show how the products at issue provide accessibloity in accordance with the ADA, Section 504 of the Rehabilitation Act of 1973, and the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA guidelines; provided, however, Contractor will have no obligations with respect to such compliance as it relates to any portion of the system and services provided or developed by the District including District content.

8. Term and Termination

8.1 This Addendum takes effect immediately as of the Effective Date, and remains in full force and effect until the successful completion of the services, unless earlier terminated under Sections 8.3 or 12.3.

8.2 Subject to Sections 8.3 and 12.3, this Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Contract between the Parties or successful completion of the Services. Alternatively, upon re-execution of the Contract by the authorized persons of District and Contractor, this Addendum shall also be revived and be of full force and effect.

8.3 Termination by the District.

8.3.1 The District may immediately terminate the Contract in accordance with District policies if, at any time, the District determines in its sole discretion, that Contractor has breached any of the requirements of this Addendum.

9. Data Transfer Upon Termination or Expiration

9.1 Destruction or Return of District Data. With the exception of De-identified Data that District has specifically agreed in writing to allow Contractor to use after termination or expiration of this Agreement, or District Data for which Contractor has specifically obtained consent from the parent, legal guardian or student to keep, no later than (30) calendar days after termination or expiration of this Agreement, Contractor shall certify in writing that all District

Data and PII that Contractor collected, generated or inferred pursuant to the Contract ("Contract Data"), is securely returned or Securely Destroyed, pursuant to Schedule 4 attached hereto.

9.2 Transfer and Destruction of District Data. If the District elects to have all District Data or Contract Data that is in Contractor's possession or in the possession of Contractor's Subcontractors transferred to a third party designated by the District, such transfer shall occur within a reasonable period of time but no later than thirty (30) calendar days after expiration or termination of this Agreement, and without significant interruption in service or access to such District Data. Contractor shall work closely with such third party transferee to ensure that such transfer/migration uses facilities and methods compatible with the relevant systems of the District or its transferee, and to the extent technologically feasible, that the District will have reasonable access to District Data during the transition. District will pay all costs associated with such transfer, unless such transfer is as the result of termination of this Agreement following Contractor's breach of the terms of this Agreement. Upon successful transfer of District Data, as confirmed in writing by the District's Designated Representative, Contractor shall Securely Destroy all District Data in accordance with Section 9.1.

9.3 Response to Specific Data Destruction or Return Requests. After receiving a written request from the District, Contractor shall Securely Destroy or return any specific District Data or Contract Data that is in its possession or in the possession of its Subcontractors within five (5) business days, excluding national holidays, after receiving a written request from the District.

10. (deleted)

11. Insurance

11.1 Coverage. As required by Schedule 6.

12. Miscellaneous

12.1 No Contractor End User Agreements. For accounts associated with District's account, Contractor shall not require End Users to sign or complete any end user license agreements (EULA) or acceptable use policy (AUP) agreements or understandings, whether electronic, verbal, or in writing. In the event that an EULA or AUP is completed by a District End User, this Addendum shall supersede the Contractor's agreement.

12.2 Public Inspection of Agreement. Contractor acknowledges and agrees that this Agreement and all documents Contractor provides District as required herein, are public records for purposes of the CORA and shall at all times be subject to public inspection. The parties understand that in the event of a request for disclosure of such information, the District will

notify Contractor to give Contractor the opportunity to redact its proprietary or confidential material. In the event of the filing of a lawsuit to compel disclosure, the District will tender Contractor's material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure or waive the same.

12.3 Survival. The Contractor's obligations under Sections 3, 4, 5, 6, 9, and 10, and any other obligations or restrictions that expressly or by their nature are to continue after termination, shall survive termination of this Agreement for any reason until all District Data has been returned or Securely Destroyed.

12.4 Choice of Law. Any claim, controversy or dispute arising under or related to this Addendum shall be construed pursuant to the substantive, not conflicts, laws of the State of Colorado. Each of the Parties submits to the exclusive jurisdiction of any state court sitting in or federal court with jurisdiction over Denver County, Colorado, in any action or proceeding arising out of or relating to this Agreement and agrees that all claims in respect of the action or proceeding may be heard and determined in any such court. Each Party also agrees not to bring any action or proceeding arising out of or relating to this Addendum in any other court. Each of the Parties waives any defense of inconvenient forum to the maintenance of any action or proceeding so brought and waives any bond, surety or other security that might be required of any other Party with respect to any such action or proceeding.

12.5 Immunities. The District retains all of its rights, privileges and immunities under the Colorado Governmental Immunity Act, C.R.S. § 24-10-101 *et seq*.

12.6 No Assignment. Contractor shall not assign or subcontract any of its rights or obligations hereunder without the express written consent of District. Any assignment in violation of this section shall be void. Notwithstanding the foregoing, nothing prohibits Contractor from assigning this agreement pursuant to a merger or sale of essentially all of Contractor's assets.

12.7 No Third Party Beneficiaries. Nothing in this Agreement shall be construed to give any rights or benefits to anyone other than District.

12.8 Schedules. The following schedules are attached hereto, or shall be attached hereto, and are specifically made a part hereof by this reference:

Schedule 1 – Designated Representatives
Schedule 2 – Subcontractors
Schedule 3 – Written Consent to Maintain De-identified Data
Schedule 4 – Certification of Destruction\Return of District Data
Schedule 5 – Data Elements

Schedule 6 – Insurance

12.9 Counterparts. This Addendum may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument.

12.10 Effectiveness; Date. This Addendum will become effective when all parties have signed it. The date of this Addendum will be the date this Addendum is signed by the last party to sign it (as indicated by the date associated with the party's signature).

12.11 Electronic Signatures and Electronic Records. The Contractor consents to the use of electronic signatures by the District. This Addendum, and any other documents requiring a signature under this Addendum, may be signed electronically by the District in the manner specified by the District. The parties agree not to deny the legal effect or enforceability of this Addendum solely because it is in electronic form or because an electronic record was used in its formation. The parties agree not to object to the admissibility of the Addendum in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Each party is signing this agreement on the date stated opposite that party's signature.

SCHOOL DISTRICT NO. 1 IN THE CITY AND COUNTY OF DENVER AND STATE OF COLORADO, D/B/A DENVER PUBLIC SCHOOLS

Date: Mar 10, 2021

By: Staci Crum (Mar 10, 2021 13:36 MST)

Staci Crum/DeeDee Case
Manager, Strategic Sourcing

POWERSCHOOL GROUP, LLC

Date: 3/10/2021

By: DocuSigned by: Phil Radmilovic 170B9E005E66422...

Philip Radmilovic
VP and Controller

Date: _____

By: _____

APPROVED AS TO FORM:

By: _____

Office of the General Counsel

OPTION 1

SCHEDULE 1
Designated Representatives

NOTICE REQUIRED	DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Security Breach:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
FERPA Records Requests:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org** **Records Requests: https://denverco.scriborder.com/**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
CORA Requests:	**Stacy Wheeler** **CORA Officer** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: cora@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
Updates to Privacy Policy / Transparency Requirements:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
Updates to Subcontractor Schedule:	**Jennifer Collins** **Chief Privacy Officer, Deputy General Counsel** **By U.S. Mail: 1860 Lincoln St** **Denver, CO 80203** **By E-mail: legal_contracts@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
Data Retrieval:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____
Destruction of Data:	**Robert Losinski** **Manager, Info Security** **By U.S. Mail: 780 Grant St** **Denver, CO 80203** **By E-mail: infosec@dpsk12.org**	**[TITLE]** **By U.S. Mail:** _____ _____ **By E-mail:** _____

OPTION 2

SCHEDULE 1
Designated Representatives

DISTRICT REPRESENTATIVE	CONTRACTOR REPRESENTATIVE
Name: **Jennifer Collins** **Title:** **Chief Privacy Officer, Deputy General Counsel** **Address:** **1860 Lincoln St** **Denver, CO 80203** **Phone:** **720-423-2211** **E-mail:** **legal_contracts@dpsk12.org**	**Name:General Counsel** **Title:** **Address: 150 Parkshore Dr, Folsom, CA 95630** **Phone:** **E-mail: legal@powerschool.com**

SCHEDULE 2
Subcontractors

Contractor shall update this information as necessary to maintain accuracy and shall send revised attachments, exhibits or schedules to the District's Authorized Representative.

What third party vendors does Contractor do business with that may have access to student personally identifiable data, and what is the purpose of these third party vendors (please fill complete the table below with this information)?

Name of Subcontractor	Primary Contact Person	Subcontractor's Address	Subcontractor's Phone/email	Purpose of re-disclosure to Subcontractor
Zendesk		450 Park Ave S, New York, NY 10016		Zendesk is the support service our Support Team uses to provide private customer support communication to our users. Our support system is available for users of all ages to submit requests or questions to our team, though non-Enterprise users who 'fail' an age gating question ('Year of Birth') receive only a one-time, automated response, and their information is not retained. Also, the Year of Birth is not retained. Requests can be submitted using a webform via support.schoology.com, by calling a private number with access code that is unique to Enterprise administrators or staff, or by live chatting via a link that is only accessible to Enterprise administrators or staff. Zendesk does not share user information with any other third parties.
Transfluent		440 N. Wolfe Rd. Sunnyvale, California UNITED STATES		Transfluent is the translation service our Support Team uses to

				provide foreign language customer support. When a ticket comes in, Support will submit the copy of the ticket to Transfluent - which is an application integrated into Zendesk. That copy is translated by a remote translator, then returned via the Transfluent app.
Pendo		150 Fayetteville St #1400, Raleigh, NC 27601		Pendo is an analytics service used to help analyze your use of our App and to improve it. We use the information we get from Pendo only to improve our App and our Services. Pendo does not share your information with any other third parties.
Flurry		110 5th Street, Suite 200 San Francisco, CA 94103 United States		Flurry is an analytics service used to help analyze your use of our Mobile Apps. We use the information we get from Flurry only to improve the experience of our Mobile Apps. Flurry do not share your information with any other third parties.
Crashlytics		One Kendall Square B3201 Cambridge, MA 02139 United States		Crashlytics is a platform for our Mobile Team to use to help analyze the performance of mobile apps. We use the information we get from Crashlytics only to improve the experience of using our mobile apps. Crashlytics does not share your information with any other third parties.
Learnosity		333W W 39th St #1003, New York, NY 10018		Learnosity is an assessment authoring, test delivery, and assessment scoring service that is used within Schoology to deliver the Assessment and Managed Assessment test experience.

SendGrid		1855 California St #500 Denver, CO 80202		SendGrid is an email delivery service that is used to send email notifications and push notifications for actions generating within Schoology to notify users of activity
Telestream		21351 Ridgetop Cir # 120, Sterling, VA 20166		Telestream is an audio/video transcoding service that is used to convert uploaded audio/videos files into an HTML5 friendly format so that uploaded media can be viewed on any device.
Sumo Logic		175 Varick St, New York, NY 10014		Sumo Logic is a cloud-based log management service that allows us to query and analyze our log data.
Amazon Web Services		410 Terry Ave. North, Seattle, WA, 98109-5210		Amazon Web Services is a cloud services platform that providers the core infrastructure for supporting Schoology's platform.
New Relic		188 Spear Street, Suite 1200, San Francisco, California 94105		New Relic is an internal monitoring platform that allows Schoology's development team to monitor the overall health and performance of our application.

SCHEDULE 3
Written Consent to Maintain De-identified Data

The District hereby gives its consent for Contractor to retain and use for the stated purpose and period, De-identified Data elements as set forth below:

Description of De-identified Data Elements	Purpose for Retention and Use	Period of Use

I\We, Phil Radmilovic, as [title] VP Controller and the authorized representative(s) of the Contractor do hereby certify that no attempt will be made to re-identify De-identified Data.

Contractor Name: PowerSchool Group LLC

Contractor Representative Name: Phil Radmilovic

Title: VP Controller

Signature: DocuSigned by: Phil Radmilovic 170B9E005E66422... Date: 3/10/2021

SCHEDULE 4
Certification of Destruction\Return of District Data

I\We, _____[NAME(S)]_____, as the authorized representative(s) of the Contractor do hereby acknowledge and certify under penalty of perjury that [initial next to both subparts of the applicable Part A or Part B]:

Part A - Destruction:

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was destroyed on _____, 20___ by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was destroyed as set forth below:

Name of Subcontractor	*Date of Deletion*	*Destruction Method*

Part B - Return: [If this option is elected by the District, then Contractor shall also complete Part A.]

_____ the District Data and PII provided to Contractor by the District as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District, on _____, 20___ to _____, by means of [describe destruction methods]: _____.

_____ the District Data and PII provided to Contractor's Subcontractors as part of the Data Protection Addendum in accordance with federal and state law was returned or transferred to the District's Authorized Representative or other person or entity designated by the District as set forth below:

Name of Subcontractor	*Date of Return*	*Return / Transfer Method*

Contractor Name: _____

Contractor Representative Name: _____

Title: _____

Signature: _____ Date: _____

SCHEDULE 5
Data Elements

(Mandatory to be completed if Service Provider is a School Service Contract Provider under CRS 22-16-101 et seq.)

1. **Service Provider collects, generates or uses pursuant to the Agreement the following data elements of District Data or PII**:

First name, last name, school, district, email address, role, course information, student responses and grades

2. **Service Provider collects and uses the District Data for the following educational purposes**:

Schoology Learning is designed to help schools and districts improve student performance while enabling equity and access for every student, at home, at school, or anywhere in between. Schoology Learning provides your entire district one integrated platform for sharing curriculum resources, data, insights, and more. Districts can support connections between the classroom and the home with native communication capabilities and online spaces for everyone, including students, teachers, PLCs, and others. Teachers can create courses, assignments, and other educational materials for their students.

3. **Service Provider's policies regarding retention and disposal of District Data are as follows**:

At the end of a customer's usage of the Schoology platform, the customer may request that Schoology make their data unavailable. At this point Schoology will disable access to the customer's data by configuring the software to disallow access. In cases where the customer wants additional changes to be put in place, Schoology will work with customers to determine the best course of action to achieve their goal. Typically, this means "scrubbing" the customer's data to obfuscate all data for their users. In the rare case where this isn't satisfactory, Schoology will engage with the customer to define a scope of data to be overwritten and a Statement of Work may have to be created to cover any custom work.

4. **Service Provider uses, shares or discloses the District Data in the following manner:**

See schedule 2 for list of subcontractors

5. **Has Service Provider's agreement has ever been terminated by another school district for failure to comply with the same or substantially similar security obligations as those set forth in this Agreement**?
   ☐ Yes ☐ x No. No
   If yes, describe:

PowerSchoolDPA

Final Audit Report 2021-03-10

Created:	2021-03-10
By:	Staci Crum (staci_crum@dpsk12.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAKCUpKSJncXgM1khVtAtwebx3MHOoh3Ck

"PowerSchoolDPA" History

Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)
2021-03-10 - 8:20:33 PM GMT- IP address: 164.92.9.21

Document created by Staci Crum (staci_crum@dpsk12.org)
2021-03-10 - 8:27:21 PM GMT- IP address: 164.92.9.21

Document emailed to Staci Crum (staci_crum@dpsk12.net) for signature
2021-03-10 - 8:27:58 PM GMT

Email viewed by Staci Crum (staci_crum@dpsk12.net)
2021-03-10 - 8:35:39 PM GMT- IP address: 164.92.9.21

Document e-signed by Staci Crum (staci_crum@dpsk12.net)
Signature Date: 2021-03-10 - 8:36:10 PM GMT - Time Source: server- IP address: 164.92.9.21

Agreement completed.
2021-03-10 - 8:36:10 PM GMT