New York

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Erie 1 Board of Cooperative Educational Services (the "**Local Education Agency**" or "**LEA**" or "**New York Original LEA**") and PowerSchool Group LLC (the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform 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:

1. Provider agrees to offer the LEA all the same terms and conditions found in the **MA-ME-OH-RI-TN-VT-VA-DPA, Modified Version 1.0** Data Privacy Agreement between the Provider and **Hopkinton Public Schools** (Originating LEA") which is dated **October 19, 2024** ("Originating DPA"). The terms and conditions of the Originating DPA are thus incorporated herein.
2. Provider additionally agrees to the following additional terms outlined in the attached Exhibit "G" for New York, which will control in the event of a conflict between the DPA and the Originating DPA.
3. Provider may, by signing the attached form of "General Offer of Privacy Terms" be bound by the terms of the General Offer of Privacy Terms to any other LEA who signs the acceptance on said Offer. The form is limited by the terms and conditions described therein.
4. **Notices**. All notices or other communication required or permitted to be given pursuant to the Originating DPA may be given for the LEA via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Darron Flagg
Title: Chief Privacy Officer
Address: 150 Parkshore Drive, Folsom, CA 95630
Phone: 877-873-1550
Email: legalnotices@powerschool.com

docs\EDU002\00023\1405794.v1-7/3/25

The designated representative for the LEA for this DPA is:

Michelle Okal-Frink, Director
355 Harlem Road West Seneca, NY 14224
mokal@e1b.org 716-821-7200

PowerSchool Group LLC

By: _____

Date: March 17, 2026

Printed Name: Jon Scrimshaw

Title/Position: Chief Accounting Officer

Erie 1 Board of Cooperative Educational Services

By: James Fregelette

Date: 03/18/2026

Printed Name: Jim Fregelette

Title/Position: Executive Director

docs\EDU002\00023\1405794.v1-7/3/25

Exhibit "G"

New York

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations.

4. Provider represents that their Data Privacy and Security Plan can be found at the URL link listed in Exhibit K and is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a)implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees and subprocessors who have access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply withterms materially consistent with Education Law § 2-d. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR

docs\EDU002\00023\1405794.v1-7/3/25

Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services. LEA acknowledges the importance of privacy and security training. .

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

    Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.

    The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".**

docs\EDU002\00023\1405794.v1-7/3/25

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: The Provider will cooperate reasonably with the LEA or its designee(s) and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable Access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Provider to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

docs\EDU002\00023\1405794.v1-7/3/25

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, then 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; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and
vi. The number of records affected, if known; and
vii. A description of the investigation undertaken so far; and
viii. The name of a point of contact for Provider.
(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
(3) 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 Student 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.
(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals.
(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

(6) Provider and its subprocessors will cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach. If a Breach is attributable to Provider or its Subprocessors, Provider shall be solely responsible for its costs incidental to the required cooperation and/or participation in an investigation.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.

- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to

docs\EDU002\00023\1405794.v1-7/3/25

such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting.
- **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic.
- **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services, then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement with LEA, and shall include LEA if it uses the Services in its own educational or operational program.

docs\EDU002\00023\1405794.v1-7/3/25

Exhibit "J"

LEA Documents

LEA's Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement can be accessed at:

https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13045

docs\EDU002\00023\1405794.v1-7/3/25

Exhibit "K"

Provider Security Policy

Provider's Data Security and Privacy Plan can be accessed at:

PHYSICAL, ADMINISTRATIVE, AND TECHNOLOGICAL SAFEGUARDS

A.1 Data Security. PowerSchool agrees to abide by and maintain adequate data security measures, consistent with industry standards for digital storage of Customer Data, to protect Customer Data from unauthorized disclosure or acquisition by an unauthorized person. The general security obligations of PowerSchool are set forth below. These security measures will include, but are not limited to:

A.1.1 Passwords and Employee Access. PowerSchool will secure usernames, passwords, and any other means of gaining access to the Services or to Customer Data, at a level meeting or exceeding the applicable standards. PowerSchool will only provide access to Customer Data to employees or contractors who require access pursuant to the MSA and this DPA, and only on terms consistent with or exceeding the data security measures required by this DPA between the Parties.

A.1.2 Security Protocols. The Parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. PowerSchool will maintain all data obtained or generated pursuant to the MSA in a secure digital environment.

A.1.3 Employee Training. PowerSchool will provide periodic security training to those employees who operate or have access to the system. Further, PowerSchool will provide Customer with contact information of an employee whom Customer may contact if there are any security concerns or questions.

A.1.4 Security Technology. PowerSchool will employ industry standard measures to protect data from unauthorized access. The service security measures will include server authentication and data encryption. PowerSchool will host data pursuant to the MSA in an environment using firewall(s) that are updated according to industry standards.

A.1.5 Monitoring. PowerSchool will log and analyze events across critical systems to identify potential threats to confidentiality, integrity, and availability of Customer Data.

A.1.6 Security Coordinator. PowerSchool will provide the name and contact information of PowerSchool's security coordinator for the Customer Data received pursuant to the MSA and this DPA upon written request.

A.1.7 Vendor-Data Subprocessors Bound. PowerSchool will enter into written agreements whereby Vendor-Data Subprocessors agree to secure and protect Customer Data in a manner consistent with the terms of this exhibit and the DPA. PowerSchool will periodically conduct or review compliance monitoring and assessments of Vendor-Data Subprocessors to determine their compliance with this exhibit and DPA.

A.1.8 Periodic Risk Assessment. PowerSchool acknowledges and agrees to conduct digital and physical periodic risk assessments at least annually and take commercially reasonable industry standard steps to remediate identified security and privacy vulnerabilities in a timely manner. PowerSchool shall provide reasonable assistance related to the nature of Processing to Customer in the event that a data protection impact assessment be required by Applicable Law.

A.1.9 Established Security Policies. PowerSchool will follow its established access security policies to support the confidentiality, integrity, and availability of the Customer Data against risks including but not limited to unauthorized access, collection, use, disclosure or disposal, loss, or modification. Such security arrangements will include, without limitation, reasonable physical, administrative, and technical safeguards.

A.1.10 Audits and Compliance Reports. PowerSchool's security compliance is assessed by independent third-party auditors. Upon Customer agreeing to an NOA, PowerSchool shall provide access to information regarding PowerSchool's ISO 27001:2103 certification and SOC II Reports. To the extent that PowerSchool discontinues a third- party audit, PowerSchool will adopt or maintain an equivalent industry-recognized security standard.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

STANDARD STUDENT DATA PRIVACY AGREEMENT

MASSACHUSETTS, MAINE, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA

MA-ME-OH-RI-TN-VT-VA-DPA, Modified Version 1.0

Hopkinton Public Schools

and

PowerSchool Group LLC

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:_Hopkinton Public Schools, located at 89 Hayden Rowe St., Hopkinton, MA 01748 (the "**Local Education Agency**" or "**LEA**") and PowerSchool Group LLC, located at 150 Parkshore Drive, Folsom, CA 95630 (the "**Provider**").

- **WHEREAS**, the Provider is providing educational or digital services to LEA.

- **WHEREAS, the Provider and LEA recognize the need to protect** personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6505 (16 CFR Part 312), application state privacy laws and regulations and

- **WHEREAS**, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   √ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

The designated representative for the Provider for this DPA is:

Name: Darron Flagg Title: Chief Privacy Officer

Address: 150 Parkshore Drive, Folsom, CA 95630

Phone: 877-873-1550 Email: legalnotices@powerschool.com

The designated representative for the LEA for this DPA is:

Ashoke Ghosh, Technology Director
89 Hayden Rowe St., Hopkinton, MA 01748
508-417-9360
aghosh@hopkinton.k12.ma.us

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

Hopkinton Public Schools

By: Ashoke Ghosh Date: 10/19/24

Printed Name: Ashoke Ghosh Title/Position: Director of Technology

PowerSchool Group LLC

By: DocuSigned by: Eric Shander Date: 10/17/2024

Printed Name: Eric Shander Title/Position: CFO

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

3. **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 terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student 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 Student Data transmitted to the Provider, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **PowerSchool Metadata:** Operation of PowerSchool systems create metadata. PowerSchool Metadata (known as "Transaction Data" as mentioned in the PowerSchool global privacy statement) is necessary to monitor the health and security of PowerSchool systems and to provide customer support. Because the definition of FERPA PII is very broad, some PowerSchool created metadata may necessarily contain some FERPA PII. The FERPA PII contained in PowerSchool created metadata is a copy of customer data and not a subtraction from customer data being processed in the PowerSchool application. While the Provider processes metadata differently, the Provider protects metadata similarly to customer data that is processed by the Provider. There are a few notable differences in the treatment of PowerSchool metadata containing FERPA PII than the treatment of customer data. PowerSchool metadata, depending on the storage mechanism, such as a log file, will be overwritten over time. PowerSchool metadata is not saved for returning and is not returned to the customer at the end of the agreement, for clarity. PowerSchool Metadata is permanently deleted over time and not retained for the length of the customer application subscription term. The Provider retains metadata for no longer than fourteen (14) months. PowerSchool proprietary metadata, exclusive of any portion of Student Data, remains the property of PowerSchool

3. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

erroneous information, and procedures for the transfer of student-generated content to a personal

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data 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 Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known 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 federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A, or for any additional Services or a modification to any existing Service as agreed to by the LEA and the Provider.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

confidentiality agreement from each employee or agent with access to Student Data pursuant to the

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider may also use De-Identified Data for any other purposes allowed under applicable laws. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any third party. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** At the LEA's written request (which can be by email), PowerSchool will make available to LEA, as soon as possible following the date hereof and at least once every calendar year thereafter, Provider's ISO/IEC 27001 Statement of Applicability (the "**SOA**"), ISO 27001 certificate issued by the relevant certification body, or equivalent documents relative to an accepted alternative security program and

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

relative to the applicable product or services. The Provider will cooperate reasonably with the LEA and

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

any local, state, or federal agency with oversight authority or jurisdiction in connection delivery of Services to students and/or LEA, and shall provide reasonable access to the LEA's Student Data and all records pertaining to the delivery of Services to the LEA

3. **Data Security**. The Provider agrees to utilize commercially reasonable administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider's cybersecurity program is aligned with the nationally recognized standards selected in **Exhibit "F"**, subject to appropriate exclusions, variations, or exemptions as determined by Provider. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within the most expedient time possible and without unreasonable delay, but no later than five (5) calendar days after the determination of a breach has occurred. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

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, then 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; and
v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) 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 Student 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.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

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

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **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. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service Privacy Policies, or with any other bid/RFP, or writing, the terms of this DPA shall apply and take precedence. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement**. This DPA and the Service Agreement constitute 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.

5. **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.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE APPLICABLE LEA, 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 OF THE APPLICABLE LEA FOR ANY DISPUTE

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

7. **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 In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein.

9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "A"
DESCRIPTION OF SERVICES

The descriptions of the PowerSchool products can be found at:
Microsoft Word - EXHIBIT A - Product Descriptions (powerschool.com)

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "B"
SCHEDULE OF DATA

The data elements for the PowerSchool products can be found at:

Microsoft Word - EXHIBIT B - Total (powerschool.com)

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

PowerSchool Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation PowerSchool Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means the party identified as 'Provider' in the DPA.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data does not include Meta Data that has been stripped of all direct and indirect identifiers. To the extern there is any FERPA PII data within PowerSchool MetaData, such is subject

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

to Article II section 2. Student Data further includes "personally identifiable information (PII)," as defined in 34

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[**Insert Name of District or LEA**] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[**Insert categories of data here**]

_____Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____Disposition shall be by destruction or deletion of data.

_____Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____As soon as commercially practicable.

_____By [**Insert Date**]

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"

Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"

Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
3. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
4. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
5. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
    a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
    b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
    c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes (subject to the clarification below).

For avoidance of doubt, this definition of Student Data does not include De-Identified Data or prohibit the Provider from using De-Identified Data in accordance with the terms of the DPA.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

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

1. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
2. In Article IV, Section 6, replace "Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
3. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
4. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
5. Provider will not access or monitor any of the following:

a. Location-tracking features of a school-issued device;
b. Audio or visual receiving, transmitting or recording features of a school-issued device;
c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"

Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16- 104-1, and R.I.G.L., 11-49.3 et. seq.;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1.
3. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
4. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information:

    i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact:

        1. The credit reporting agencies
        2. Remediation service providers
        3. The attorney general

    ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

    iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"

Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq*., T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq*., T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq*.;

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee.

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
3. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
4. The Provider agrees that it will not collect individual student data on:
    a. Political affiliation;
    b. Religion;
    c. Voting history; and
    d. Firearms ownership

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"
Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

docs\EDU002\00023\1405794.v1-7/3/25

Docusign Envelope ID: 7F8435AE-A47B-445A-AFD4-4A616467579C

EXHIBIT "G"
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are, where applicable, also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

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

1. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
2. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
3. In Article V, Section 4, add: In order to ensure the LEA's ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

docs\EDU002\00023\1405794.v1-7/3/25

Powerschool_Hopkinton_2024_VendorSigned

Final Audit Report 2024-10-19

Created:	2024-10-19
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAABHArUrzRnp3lVl9znCYu8Tl1IGw2YhlW

"Powerschool_Hopkinton_2024_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2024-10-19 - 12:53:40 PM GMT

Document emailed to Ashoke Ghosh (aghosh@hopkinton.k12.ma.us) for signature
2024-10-19 - 12:53:45 PM GMT

Email viewed by Ashoke Ghosh (aghosh@hopkinton.k12.ma.us)
2024-10-19 - 3:04:39 PM GMT

Document e-signed by Ashoke Ghosh (aghosh@hopkinton.k12.ma.us)
Signature Date: 2024-10-19 - 3:05:17 PM GMT - Time Source: server

Agreement completed.
2024-10-19 - 3:05:17 PM GMT

docs\EDU002\00023\1405794.v1-7/3/25

EXHIBIT "A"
DESCRIPTION OF SERVICES

Analytics and Insights: Analytics and 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.

Attendance Intervention: PowerSchool's Attendance Intervention product allows districts to use best-practice, data-driven family engagement tools proven to improve school attendance and reduce truancy and chronic absenteeism through strengthening partnership with students and their families. Attendance Intervention provides the ability to perform data-driven, automated attendance interventions, easier access to all families through two-way, translated, text-based communications, and a data-driven approach and research-backed family engagement strategies to drive impact.

Behavior Support: PowerSchool Behavior Support's behavior management solutions help educators more effectively manage social and emotional learning (SEL) and multi-tiered systems of support (MTSS) to help improve student well-being, school culture, and achieve more equitable outcomes. Users do this by collecting student behavior data to coordinate positive reward systems, restorative practices, and other interventions.

BusinessPlus: BusinessPlus helps business managers, CFOs, and HR staff manage complex business processes, employees, and workflows, and provides district staff the ability to manage budget, make important allocation decisions, run payroll, and manage employees, vendors, and other third parties in one integrated solution. BusinessPlus is used by larger districts (25K+ enrollment) with extremely complex and highly configurable and customizable workflows and other business functions.

Communicate: Communicate is the trust platform for managing parent and community engagement. Communicate is a multi-channel, mass notification platform that allows schools and districts to quickly and easily communicate with their school community.

Connected Intelligence: Connected Intelligence is a data as a service (DaaS) platform to help K-12 districts securely centralize their data for insights, analytics, and data-informed decision-making.

Curriculum & Instruction is a curriculum mapping and teacher lesson planning solution. Districts create and centralize their curriculum plan, supported by pacing guides. Build and share a curriculum framework that is cohesive and provides improved vertical alignment between instruction and national and state standards.

ContentNav is a learning object repository that centralizes instructional resources from publishers and districts. The platform allows for the creation and ingestion of content, tagged to metadata and standards, that facilitate global search. ContentNav integrates into the Schoology Learning platform, providing educators access to a complete library of school- or district-approved, standards-aligned instructional content, all in one location.

docs\EDU002\00023\1405794.v1-7/3/25

CustomApp: CustomApp is a platform that allows districts to create customized and branded school district iOS and Android mobile apps. CustomApp solutions are integrated with notifications, website content, social media, and other content to provide their parents and community with a comprehensive mobile experience.

Ecollect: Ecollect allows districts to create, edit and share online K-12 forms to support their initiatives. The product is a plugin within PowerSchool SIS, so any user (regardless of persona) that uses the product would have had to go through the PowerSchool SIS account creation/activation process.

eFinancePlus: eFinancePlus helps business managers and HR staff manage complex business processes and workflows making it easier to process departmental tasks across various functions. eFinancePlus lets district staff manage budget, make allocation decisions, run payroll, and manage employees, vendors, and other third parties in one integration solution.

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 SISs, and lotteries, streamlining related business processes. Registration is a multitenant cloud-based web application.

Enrollment Express: Enrollment Express is a student enrollment management system inside PowerSchool SIS.

eSchoolPlus: eSchoolPlus SIS solution provides functionality across PowerSchool solutions empowering users 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.

Headed2: By connecting Headed2's college, career, military, and life readiness platform to PowerSchool's industry,-leading suite of solutions, students of all ages will benefit from intuitive planning tools designed to help them explore options as they research and prepare for future success.

Naviance: 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.

Naviance for Elementary: Naviance for Elementary is a career and life exploration platform for elementary students focused on early pathway equity. It provides built-in CCLR lessons, career exploration content, and a gamified experience for career awareness.

Perform Enterprise: An assessment creation and delivery platform where users can create assessment content such as items, observational measures and assessments. Users can find instructional opportunities through sophisticated data analysis of assessment results, aggregated standards result, imported student attendance, discipline and grades data, and third-party assessment results.

Permission Click: Permission Click provides schools with a platform to deploy online forms for parents, teachers, staff, coaches, and district administration. It offers custom forms with a drag-and-drop

docs\EDU002\00023\1405794.v1-7/3/25

builder, automated workflows, and robust dashboards to track the status of the forms; it also supports collecting payments via the forms, and parents can submit responses from any device. This product is available to customers without PowerSchool SIS.

PowerBuddy: PowerBuddy is a role-specific Conversational AI assistant for everyone in education. With their very own PowerBuddy, each student, parent, educator, counselor, and administrator will now have safe and secure access to individualized guidance, information, and resources at their fingertips, helping students receive the most optimal social, emotional, and academic support in a way never experienced before.

PowerBuddy will initially be incorporated into Schoology Learning offering students on-demand, one-on-one assistance with their assignments and tailored pathways transforming traditional learning into an immersive and engaging experience. Teachers will be able to use PowerBuddy to generate lesson plans, automate the creation of quizzes and assessments in Performance Matters, and personalize homework at scale, saving them time to focus on what's most important – interaction with students. Additionally, it will offer individualized college and career guidance through Naviance CCLR for both counselors and students. Parents can leverage PowerBuddy in My PowerSchool to inquire about their child's academic performance and other relevant information. They will receive proactive alerts if their child is falling behind, fostering transparency and empowering parents to participate in their child's education. Additionally, PowerBuddy will offer personalized, district-approved academic and social-emotional learning resources from ContentNav to actively support them in their child's learning. Furthermore, administrators can ask natural language questions about their data within Analytics & Insights and PowerSchool SIS to truly democratize information for decision-making. PowerBuddy will eventually be expanded across the entire PowerSchool ecosystem. It will be system-agnostic and will integrate with most education technology tools, including non-PowerSchool products.

PowerSchool DEX (Data Exchange) facilitates data integration and interoperability utilizing the Ed-Fi data and transmission standards from the Student Information System to some type of operational data store (for example to a State Department of Education, such as state compliance required by the Texas Education Agency via the Hosted Ed-Fi Operational Data Store).

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.

Predictive Enrollment Analytics: Predictive Enrollment Analytics allows districts to use data to forecast enrollment and represents their data sets geographically to support decision making. The product provides actionable intelligence about districts' student enrollment with data, descriptive and predictive statistics, and analytic tools; it helps districts better predict student enrollment and properly allocate resources.

Presence: Presence provides clients with an innovative and comprehensive CMS platform that simplifies the task of maintaining a school or district website.

SafeArrival: SafeArrival makes attendance management faster and easier. Clients utilize SafeArrival to quickly gather information about absences, as well as providing parents with a way to proactively report

docs\EDU002\00023\1405794.v1-7/3/25

upcoming absences.

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

SmartFind Express: SmartFind Express is used for the school district's absence management for teachers. SmartFind Express helps find eligible substitute teachers when regular teachers are absent. The school district configures the search rules for finding eligible substitutes for the days and times when the teachers are absent. Substitute teachers are contacted through automated phone calls or text messages about vacant positions (as job offers) by the system and the substitute teachers can accept or decline those offers. Substitute teachers can also view open available jobs on the system's web interface and accept or decline the jobs from the web.

Special Education: Special Education 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.

TalentEd Suite: 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.

docs\EDU002\00023\1405794.v1-7/3/25

Erie 1 BOCES (NY)

Final Audit Report 2026-03-18

Created:	2026-03-18
By:	TEC SDPA (mmcgrath@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAZGJ0kg8o1-CGCm9XpbPP9vf6uRQjSbBQ

"Erie 1 BOCES (NY)" History

Document created by TEC SDPA (mmcgrath@tec-coop.org)
2026-03-18 - 3:26:43 PM GMT

Document emailed to James Fregelette (jfregelette@e1b.org) for signature
2026-03-18 - 3:26:55 PM GMT

Email viewed by James Fregelette (jfregelette@e1b.org)
2026-03-18 - 7:20:15 PM GMT

Document e-signed by James Fregelette (jfregelette@e1b.org)
Signature Date: 2026-03-18 - 7:21:22 PM GMT - Time Source: server

Agreement completed.
2026-03-18 - 7:21:22 PM GMT

EXHIBIT "A"
DESCRIPTION OF SERVICES

Analytics and Insights: Analytics and 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.

Allocate: Allovue Allocate is a budgeting and financial management system designed to help school districts allocate resources based on student enrollment and other school-level data. It allows districts to model changing resource needs and funding requirements as enrollment and student needs evolve.

Applicant Tracking: Applicant Tracking System enables applicants to apply for positions through the provided job board, while administrators utilize the information submitted by applicants to make informed hiring decisions. The system facilitates the application process for job seekers and allows HR staff to evaluate candidates for hiring decisions.

Atrieve: Atrieve processes data for HR, Payroll and Financial accounting/management functions and provides simplified solutions to the school board's finance, HR, and payroll processes in their day-to-day activities.

Attendance Intervention: PowerSchool's Attendance Intervention product allows districts to use best-practice, data-driven family engagement tools proven to improve school attendance and reduce truancy and chronic absenteeism through strengthening partnership with students and their families. Attendance Intervention provides the ability to perform data-driven, automated attendance interventions, easier access to all families through two-way, translated, text-based communications, and a data-driven approach and research-backed family engagement strategies to drive impact.

Behavior Support: PowerSchool Behavior Support's behavior management solutions help educators more effectively manage social and emotional learning (SEL) and multi-tiered systems of support (MTSS) to help improve student well-being, school culture, and achieve more equitable outcomes. Users do this by collecting student behavior data to coordinate positive reward systems, restorative practices, and other interventions.

Budget: Allovue Budget is a comprehensive budgeting and financial management system designed to help school districts develop and manage their budgets collaboratively and strategically. It integrates budgeting with strategic planning, ensuring that spending plans align with district goals and priorities.

BusinessPlus: BusinessPlus helps business managers, CFOs, and HR staff manage complex business processes, employees, and workflows, and provides district staff the ability to manage budget, make important allocation decisions, run payroll, and manage employees, vendors, and other third parties in one integrated solution. BusinessPlus is used by larger districts (25K+ enrollment) with extremely complex and highly configurable and customizable workflows and other business functions.
Candidate Assessment: Candidate Assessment is a K-12 software designed to help schools find the best candidates for teaching positions. It uses research-backed assessments, predictive analytics, and clear

interview feedback to identify candidates' strengths and their potential impact on student learning.

Coaching & Mentoring: PowerSchool Mentoring and Coaching product aims to enhance teacher growth and collaboration by offering a scalable, personalized mentoring tool for school districts. Teachers can set individual goals within a Professional Development framework and conduct check-ins with their mentors.

Communicate: Communicate is the trust platform for managing parent and community engagement. Communicate is a multi-channel, mass notification platform that allows schools and districts to quickly and easily communicate with their school community.

Connected Intelligence: Connected Intelligence is a data as a service (DaaS) platform to help K-12 districts securely centralize their data for insights, analytics, and data-informed decision-making.

Curriculum & Instruction is a curriculum mapping and teacher lesson planning solution. Districts create and centralize their curriculum plan, supported by pacing guides. Build and share a curriculum framework that is cohesive and provides improved vertical alignment between instruction and national and state standards.

ContentNav is a learning object repository that centralizes instructional resources from publishers and districts. The platform allows for the creation and ingestion of content, tagged to metadata and standards, that facilitate global search. ContentNav integrates into the Schoology Learning platform, providing educators access to a complete library of school- or district-approved, standards-aligned instructional content, all in one location.

CustomApp: CustomApp is a platform that allows districts to create customized and branded school district iOS and Android mobile apps. CustomApp solutions are integrated with notifications, website content, social media, and other content to provide their parents and community with a comprehensive mobile experience.

Document Cloud: Document Management solution is designed to help schools and districts efficiently manage their documents in a secure, integrated platform. It allows schools to store and email student documents.

Ecollect: Ecollect allows districts to create, edit and share online K-12 forms to support their initiatives. The product is a plugin within PowerSchool SIS, so any user (regardless of persona) that uses the product would have had to go through the PowerSchool SIS account creation/activation process.

eFinancePlus: eFinancePlus helps business managers and HR staff manage complex business processes and workflows making it easier to process departmental tasks across various functions. eFinancePlus lets district staff manage budget, make allocation decisions, run payroll, and manage employees, vendors, and other third parties in one integration solution.

Employee Records: Employee Records is for K-12 School Districts for managing Human Resources (HR) paperwork and critical business activities. The product is a “form and process” management solution for

HR tasks. Employee Records enables the creation of custom forms to collect employee data related to onboarding, offboarding, and other employment contract needs.

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 SISs, and lotteries, streamlining related business processes. Registration is a multitenant cloud-based web application.

Enrollment Express: Enrollment Express is a student enrollment management system inside PowerSchool SIS.

eSchoolPlus: eSchoolPlus SIS solution provides functionality across PowerSchool solutions empowering users 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.

Headed2: By connecting Headed2's college, career, military, and life readiness platform to PowerSchool's industry,-leading suite of solutions, students of all ages will benefit from intuitive planning tools designed to help them explore options as they research and prepare for future success.

Intersect: Intersect is a recruitment optimization solution for higher education admissions offices to connect with Naviance students and support them through the application and enrollment process.

Manage: Allovue Manage provides staffing and financial accounting analytics to districts using data from their Enterprise Resource Planning (ERP) and Hunman Resources (HR) systems of record.

MyPowerHub: MyPowerHub streamlines interactions between families and schools and assists school technology leaders in managing PowerSchool solutions by offering a centralized access point tailored to educators, students, and family members. The platform provides centralized access to student information from various PowerSchool applications, enhancing home engagement in student performance by allowing families and educators to monitor progress on assignments.

MTSS: MTSS [Multi-Tiered System of Supports] is a comprehensive K-12 solution designed to help educators establish personalized student plans and intervention teams. It provides critical data to identify at-risk students, assign and monitor interventions, communicate with stakeholders and track progress toward goals from one location. It enables a streamlined, data-driven practice with configurable workflows for easy and actionable analysis.

Naviance: 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.

Naviance for Elementary: Naviance for Elementary is a career and life exploration platform for elementary students focused on early pathway equity. It provides built-in CCLR lessons, career exploration content, and a gamified experience for career awareness.

Perform Enterprise: An assessment creation and delivery platform where users can create assessment content such as items, observational measures and assessments. Users can find instructional opportunities through sophisticated data analysis of assessment results, aggregated standards result, imported student attendance, discipline and grades data, and third-party assessment results.

Performance Matters Assessment: Performance Matters Assessment is a comprehensive assessment tool that supports the creation, administration, and analysis of educational assessments. The product is used by School/Districts to improve personalized learning and establish a secure database that is accessible to various products across the platform.

Permission Click: Permission Click provides schools with a platform to deploy online forms for parents, teachers, staff, coaches, and district administration. It offers custom forms with a drag-and-drop builder, automated workflows, and robust dashboards to track the status of the forms; it also supports collecting payments via the forms, and parents can submit responses from any device. This product is available to customers without PowerSchool SIS.

PowerBuddy: PowerBuddy is a role-specific Conversational AI assistant for everyone in education. With their very own PowerBuddy, each student, parent, educator, counselor, and administrator will now have safe and secure access to individualized guidance, information, and resources at their fingertips, helping students receive the most optimal social, emotional, and academic support in a way never experienced before.

PowerBuddy will initially be incorporated into Schoology Learning offering students on-demand, one-on-one assistance with their assignments and tailored pathways transforming traditional learning into an immersive and engaging experience. Teachers will be able to use PowerBuddy to generate lesson plans, automate the creation of quizzes and assessments in Performance Matters, and personalize homework at scale, saving them time to focus on what's most important – interaction with students. Additionally, it will offer individualized college and career guidance through Naviance CCLR for both counselors and students. Parents can leverage PowerBuddy in My PowerSchool to inquire about their child's academic performance and other relevant information. They will receive proactive alerts if their child is falling behind, fostering transparency and empowering parents to participate in their child's education. Additionally, PowerBuddy will offer personalized, district-approved academic and social-emotional learning resources from ContentNav to actively support them in their child's learning. Furthermore, administrators can ask natural language questions about their data within Analytics & Insights and PowerSchool SIS to truly democratize information for decision-making. PowerBuddy will eventually be expanded across the entire PowerSchool ecosystem. It will be system-agnostic and will integrate with most education technology tools, including non-PowerSchool products.

PowerSchool DEX (Data Exchange) facilitates data integration and interoperability utilizing the Ed-Fi data and transmission standards from the Student Information System to some type of operational data store (for example to a State Department of Education, such as state compliance required by the Texas Education Agency via the Hosted Ed-Fi Operational Data Store).

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.

Predictive Enrollment Analytics: Predictive Enrollment Analytics allows districts to use data to forecast enrollment and represents their data sets geographically to support decision making. The product provides actionable intelligence about districts' student enrollment with data, descriptive and predictive statistics, and analytic tools; it helps districts better predict student enrollment and properly allocate resources.

Presence: Presence provides clients with an innovative and comprehensive CMS platform that simplifies the task of maintaining a school or district website.

Professional Learning: Professional Learning solution provides administrators of schools with ability to centralize, manage, and track professional development for educators and staff in their district. Within the application, educators will be able to register and access learning materials to support their career growth.

SafeArrival: SafeArrival makes attendance management faster and easier. Clients utilize SafeArrival to quickly gather information about absences, as well as providing parents with a way to proactively report upcoming absences.

SchoolSpring: This system serves as an Applicant Tracking System (ATS) and a Job Board for candidates. It enables applicants to apply for positions through the provided job board, while administrators utilize the information submitted by applicants to make informed hiring decisions.

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

SmartFind Express: SmartFind Express is used for the school district's absence management for teachers. SmartFind Express helps find eligible substitute teachers when regular teachers are absent. The school district configures the search rules for finding eligible substitutes for the days and times when the teachers are absent. Substitute teachers are contacted through automated phone calls or text messages about vacant positions (as job offers) by the system and the substitute teachers can accept or decline those offers. Substitute teachers can also view open available jobs on the system's web interface and accept or decline the jobs from the web.

Special Education: Special Education 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.

TalentEd Suite: 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.

Data Category	Elements	Analytics & Insights (Student Analytics)	Analytics & Insights (Student Readiness Analytics)	Analytics & Insights (Risk Analysis)	Analytics & Insights (Community engagement)	Analytics & Insights (Talent Analytics)
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name					
	User name	TRUE	TRUE	TRUE	TRUE	TRUE
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth					
	Place of birth					
	Age					
	Gender					
	Ethnicity					
	Race					
	Language information					
	Nationality					
	Photo					
Contact	Email address					
	Street address					
	Postal code					
	Telephone number					
	Location details					
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password	TRUE	TRUE	TRUE	TRUE	TRUE
	IP address					
	Cookies					
	Browser history					
	Metadata using the application					
	Social media profile					
Employment	Profession/Role					
	Job type					
	Job title					
	Job level					
	Work experience					
	Professional certifications and licenses					
	Trade union membership					
	Employee classification					
	Professional license or certification number					
	Training Programs					
Educational	Academic degrees obtained					
	GPA					
	grades, performance, ranking					
	Schools and universities attended					
	Course of Study					
Financial	Financial account number					
	Credit card number					
	Salary					
	Income					
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number					
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status					
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information					
	Health insurance policy number					

Data Category	Elements	Analytics & Insights (Student Analytics)	Analytics & Insights (Student Readiness Analytics)	Analytics & Insights (Risk Analysis)	Analytics & Insights (Community engagement)	Analytics & Insights (Talent Analytics)
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence					
	Absence dates					
Others	Signature					
	Initials					
	Behavior					
	Survey Responses					
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above					

Data Category	Elements	Analytics & Insight Continuous Improvement Planning	Applicant Tracking	Allocate	Attendance Intervention Suite	Atrieve ERP
Name	Name [first and last]	TRUE	TRUE		TRUE	TRUE
	Parent/guardian name					
	User name	TRUE	TRUE	TRUE	TRUE	TRUE
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth		TRUE			TRUE
	Place of birth					
	Age		TRUE			TRUE
	Gender		TRUE			TRUE
	Ethnicity		TRUE			TRUE
	Race		TRUE			
	Language information					
	Nationality					TRUE
	Photo					
Contact	Email address		TRUE	TRUE	TRUE	TRUE
	Street address		TRUE			TRUE
	Postal code		TRUE			TRUE
	Telephone number		TRUE		TRUE	TRUE
	Location details					
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID				TRUE	
	Password	TRUE		TRUE		
	IP address		TRUE		TRUE	
	Cookies					
	Browser history					
	Metadata using the application			TRUE		
	Social media profile					
Employment	Profession/Role					TRUE
	Job type					
	Job title		TRUE	TRUE	TRUE	TRUE
	Job level			TRUE		TRUE
	Work experience					
	Professional certifications and licenses		TRUE			TRUE
	Trade union membership					TRUE
	Employee classification					
	Professional license or certification number					TRUE
	Training Programs					
Educational	Academic degrees obtained		TRUE			TRUE
	GPA					
	grades, performance, ranking					
	Schools and universities attended		TRUE		TRUE	TRUE
	Course of Study					
Financial	Financial account number					
	Credit card number					
	Salary			TRUE		
	Income					
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number		TRUE			TRUE
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status		TRUE			
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information					
	Health insurance policy number					TRUE

Data Category	Elements	Analytics & Insight Continuous Improvement Planning	Applicant Tracking	Allocate	Attendance Intervention Suite	Atrieve ERP
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence					
	Absence dates					
Others	Signature					
	Initials		TRUE		TRUE	
	Behavior					
	Survey Responses				TRUE	
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above					

Data Category	Elements	Behavior Support	Budget Suite	Business Plus	Candidate Assessment	Coaching & Mentoring
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name					
	User name	TRUE		TRUE		TRUE
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth	TRUE		TRUE		
	Place of birth					
	Age			TRUE		
	Gender			TRUE		
	Ethnicity			TRUE		
	Race			TRUE		
	Language information					
	Nationality					
	Photo					
Contact	Email address	TRUE	TRUE	TRUE	TRUE	TRUE
	Street address			TRUE		
	Postal code			TRUE		
	Telephone number	TRUE		TRUE	TRUE	
	Location details				TRUE	
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password			TRUE		
	IP address	TRUE	TRUE			
	Cookies					
	Browser history					
	Metadata using the application					
	Social media profile					
Employment	Profession/Role			TRUE	TRUE	TRUE
	Job type					
	Job title		TRUE	TRUE	TRUE	TRUE
	Job level		TRUE	TRUE		
	Work experience					
	Professional certifications and licenses			TRUE		
	Trade union membership					
	Employee classification					
	Professional license or certification number			TRUE		
	Training Programs					
Educational	Academic degrees obtained			TRUE		
	GPA					
	grades, performance, ranking					
	Schools and universities attended			TRUE		
	Course of Study					
Financial	Financial account number		TRUE			
	Credit card number					
	Salary		TRUE	TRUE		
	Income		TRUE			
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number			TRUE		
	National identification number					
	Individual tax identification number			TRUE		
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status			TRUE		
	Marital status			TRUE		
	Vehicle identification number					
	Insurance			TRUE		
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information					
	Health insurance policy number					

Data Category	Elements	Behavior Support	Budget Suite	Business Plus	Candidate Assessment	Coaching & Mentoring
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition			TRUE		
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence					
	Absence dates					
Others	Signature					
	Initials					
	Behavior					
	Survey Responses	TRUE				
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above		TRUE			
			Student Intervention Data			

Data Category	Elements	Connected Intelligence	Content Nav	Curriculum & Instructions	Document Management	Ecollect Forms
Name	Name [first and last]			TRUE	TRUE	TRUE
	Parent/guardian name					
	User name				TRUE	
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth					TRUE
	Place of birth					
	Age					
	Gender					TRUE
	Ethnicity					
	Race					
	Language information					
	Nationality					
	Photo					
Contact	Email address			TRUE	TRUE	TRUE
	Street address					TRUE
	Postal code					
	Telephone number					TRUE
	Location details					
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password					
	IP address			TRUE		
	Cookies					
	Browser history					
	Metadata using the application					
	Social media profile					
Employment	Profession/Role					
	Job type					
	Job title					
	Job level					
	Work experience					
	Professional certifications and licenses					
	Trade union membership					
	Employee classification					
	Professional license or certification number					
	Training Programs					
Educational	Academic degrees obtained					
	GPA					
	grades, performance, ranking					
	Schools and universities attended					
	Course of Study					
Financial	Financial account number					
	Credit card number					
	Salary					
	Income					TRUE
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number					
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status					
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information					
	Health insurance policy number					

Data Category	Elements	Connected Intelligence	Content Nav	Curriculum & Instructions	Document Management	Ecollect Forms
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence					
	Absence dates					
Others	Signature					TRUE
	Initials				TRUE	
	Behavior					
	Survey Responses					
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above				TRUE	TRUE
		No Standalone data required	ConetentNav collects data only from Content Partners			

Data Category	Elements	eFinancePlus	Employee Records	Enrollment	Enrollment Express	eSchoolPlus
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name			TRUE		
	User name	TRUE				TRUE
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth	TRUE		TRUE	TRUE	TRUE
	Place of birth				TRUE	TRUE
	Age	TRUE				
	Gender	TRUE			TRUE	TRUE
	Ethnicity	TRUE			TRUE	TRUE
	Race	TRUE			TRUE	TRUE
	Language information					
	Nationality				TRUE	TRUE
	Photo					
Contact	Email address	TRUE	TRUE	TRUE	TRUE	TRUE
	Street address	TRUE			TRUE	TRUE
	Postal code	TRUE			TRUE	TRUE
	Telephone number			TRUE	TRUE	TRUE
	Location details		TRUE			
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password	TRUE				
	IP address	TRUE				TRUE
	Cookies	TRUE				
	Browser history					
	Metadata using the application	TRUE				TRUE
	Social media profile					
Employment	Profession/Role					
	Job type		TRUE			
	Job title	TRUE				
	Job level	TRUE				
	Work experience					
	Professional certifications and licenses	TRUE				
	Trade union membership	TRUE				
	Employee classification					
	Professional license or certification number					
	Training Programs	TRUE				
Educational	Academic degrees obtained	TRUE				TRUE
	GPA					
	grades, performance, ranking					TRUE
	Schools and universities attended	TRUE			TRUE	TRUE
	Course of Study	TRUE				TRUE
Financial	Financial account number	TRUE				
	Credit card number	TRUE				
	Salary	TRUE				
	Income				TRUE	
	Assets/Investments					
	Expenses/Debt					TRUE
	Credit Score					
Sensitive	Social Security Number	TRUE				TRUE
	National identification number				TRUE	
	Individual tax identification number	TRUE				
	Economically Disadvantaged status					
	Immigration Status				TRUE	
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status				TRUE	
	Marital status					
	Vehicle identification number	TRUE				
	Insurance	TRUE			TRUE	
	License plate number					
	Other sensitive data					
Health	Heath Information				TRUE	TRUE
	Height					TRUE
	Weight					TRUE
	Genetic data					
	Diagnosis					TRUE
	Health symptoms					TRUE
	Health treatment					TRUE
	Medication				TRUE	TRUE
	Disability information					
	Health insurance policy number	TRUE			TRUE	TRUE

Data Category	Elements	eFinancePlus	Employee Records	Enrollment	Enrollment Express	eSchoolPlus
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					TRUE
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders	TRUE				
Attendance	Attendance records					TRUE
	Reason of absence					
	Absence dates					
Others	Signature	TRUE			TRUE	
	Initials	TRUE				
	Behavior					TRUE
	Survey Responses	TRUE				
	Disciplinary records					
	Security questions/answers			TRUE		
	Any other data not listed above					TRUE

Data Category	Elements	Headed2	Intersect	Manage	MyPowerHub	MTSS
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name					
	User name	TRUE	TRUE	TRUE		
	Preferred name					
	Maiden name					
	ID/ EID numbers					TRUE
	Emergency contact					
Demographic	Date of birth					
	Place of birth					
	Age	TRUE				TRUE
	Gender					
	Ethnicity					
	Race					
	Language information					
	Nationality					
	Photo					
Contact	Email address	TRUE	TRUE	TRUE	TRUE	TRUE
	Street address	TRUE				
	Postal code	TRUE				
	Telephone number		TRUE			
	Location details					
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password			TRUE		
	IP address	TRUE	TRUE			
	Cookies	TRUE				
	Browser history					
	Metadata using the application			TRUE		
	Social media profile		TRUE			
Employment	Profession/Role	TRUE				
	Job type					
	Job title	TRUE	TRUE	TRUE		
	Job level	TRUE				
	Work experience					
	Professional certifications and licenses	TRUE				
	Trade union membership					
	Employee classification					
	Professional license or certification number					
	Training Programs					
Educational	Academic degrees obtained	TRUE				
	GPA					TRUE
	grades, performance, ranking	TRUE				TRUE
	Schools and universities attended	TRUE			TRUE	TRUE
	Course of Study					
Financial	Financial account number					
	Credit card number					
	Salary					
	Income	TRUE				
	Assets/Investments	TRUE				
	Expenses/Debt	TRUE				
	Credit Score					
Sensitive	Social Security Number					
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status					
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information					
	Health insurance policy number					

Data Category	Elements	Headed2	Intersect	Manage	MyPowerHub	MTSS
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					TRUE
	Reason of absence					
	Absence dates					
Others	Signature					
	Initials				TRUE	
	Behavior					
	Survey Responses					
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above			TRUE		

Data Category	Elements	Naviance	Perform	Performance Matters	Permission Click	Predective Enrollment Analytics
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	
	Parent/guardian name			TRUE		
	User name	TRUE				
	Preferred name					
	Maiden name					
	ID/ EID numbers			TRUE		TRUE
	Emergency contact					
Demographic	Date of birth	TRUE		TRUE		
	Place of birth					
	Age	TRUE				
	Gender	TRUE		TRUE		
	Ethnicity	TRUE		TRUE		
	Race	TRUE		TRUE		
	Language information			TRUE		
	Nationality	TRUE				
	Photo					
Contact	Email address	TRUE	TRUE		TRUE	
	Street address	TRUE		TRUE		TRUE
	Postal code	TRUE				TRUE
	Telephone number	TRUE		TRUE		
	Location details		TRUE			
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID					
	Password	TRUE				
	IP address	TRUE				
	Cookies					
	Browser history					
	Metadata using the application					
	Social media profile					
Employment	Profession/Role					
	Job type					
	Job title	TRUE				
	Job level					
	Work experience			TRUE		
	Professional certifications and licenses					
	Trade union membership					
	Employee classification					
	Professional license or certification number					
	Training Programs	TRUE				
Educational	Academic degrees obtained	TRUE		TRUE		
	GPA			TRUE		
	grades, performance, ranking	TRUE		TRUE		TRUE
	Schools and universities attended	TRUE				
	Course of Study	TRUE		TRUE		
Financial	Financial account number					
	Credit card number					
	Salary					
	Income					
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number					
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status			TRUE		
	Immigration Status					
	Migration Status			TRUE		
	Passport number					
	Sexual orientation					
	Military Status					
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					
	Height					
	Weight					
	Genetic data					
	Diagnosis					
	Health symptoms					
	Health treatment					
	Medication					
	Disability information			TRUE		
	Health insurance policy number					

Data Category	Elements	Naviance	Perform	Performance Matters	Permission Click	Predective Enrollment Analytics
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition	TRUE				
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence					
	Absence dates					
Others	Signature					
	Initials					
	Behavior					
	Survey Responses	TRUE				
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above					TRUE

Data Category	Elements	Professional Learning	Schoology Learning	SchoolSpring Job Board	SmartFind Express	Student Information System
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name					
	User name	TRUE	TRUE	TRUE	TRUE	TRUE
	Preferred name					
	Maiden name					
	ID/ EID numbers					
	Emergency contact					
Demographic	Date of birth		TRUE	TRUE		TRUE
	Place of birth					TRUE
	Age		TRUE	TRUE		TRUE
	Gender		TRUE	TRUE	TRUE	TRUE
	Ethnicity		TRUE	TRUE	TRUE	TRUE
	Race		TRUE	TRUE		TRUE
	Language information					
	Nationality		TRUE			
	Photo					
Contact	Email address	TRUE	TRUE	TRUE	TRUE	TRUE
	Street address		TRUE	TRUE	TRUE	TRUE
	Postal code		TRUE	TRUE		TRUE
	Telephone number		TRUE	TRUE	TRUE	TRUE
	Location details					
Transport	Bus assignment					
	Bus Pickup/drop location					
	Bus ID number					
Online	Device ID		TRUE			
	Password					TRUE
	IP address		TRUE	TRUE		TRUE
	Cookies		TRUE			
	Browser history					
	Metadata using the application					
	Social media profile					
Employment	Profession/Role		TRUE		TRUE	
	Job type					
	Job title		TRUE	TRUE		
	Job level					
	Work experience					
	Professional certifications and licenses			TRUE		
	Trade union membership					
	Employee classification				TRUE	
	Professional license or certification number					
	Training Programs					TRUE
Educational	Academic degrees obtained		TRUE	TRUE		TRUE
	GPA					
	grades, performance, ranking		TRUE			TRUE
	Schools and universities attended			TRUE		TRUE
	Course of Study					TRUE
Financial	Financial account number					
	Credit card number					
	Salary					
	Income					
	Assets/Investments					
	Expenses/Debt					
	Credit Score					
Sensitive	Social Security Number			TRUE		TRUE
	National identification number					
	Individual tax identification number					
	Economically Disadvantaged status					
	Immigration Status					
	Migration Status					
	Passport number					
	Sexual orientation					
	Military Status			TRUE		
	Marital status					
	Vehicle identification number					
	Insurance					
	License plate number					
	Other sensitive data					
Health	Heath Information					TRUE
	Height					TRUE
	Weight					TRUE
	Genetic data					
	Diagnosis					
	Health symptoms					TRUE
	Health treatment					TRUE
	Medication					TRUE
	Disability information					
	Health insurance policy number					TRUE

Data Category	Elements	Professional Learning	Schoology Learning	SchoolSpring Job Board	SmartFind Express	Student Information System
	Medical record number					
Biometric	Finger prints					
	Retina scan					
	Voice print					
	DNA sequence					
	Facial photographs/recognition					
Religious	Religious affiliation					
	Place of worship membership					
Political	Political official position or appointment					
	Political party affiliation					
Criminal/ Legal	Criminal charges					
	Criminal convictions					
	Legal judgments or orders					
Attendance	Attendance records					
	Reason of absence				TRUE	
	Absence dates				TRUE	
Others	Signature					
	Initials			TRUE		
	Behavior					
	Survey Responses					
	Disciplinary records					
	Security questions/answers					
	Any other data not listed above		TRUE			

Data Category	Elements	School Messenger Communicate	School Messenger Presence	School Messenger SafeArrival	Special Programs
Name	Name [first and last]	TRUE	TRUE	TRUE	TRUE
	Parent/guardian name			TRUE	
	User name		TRUE	TRUE	TRUE
	Preferred name				
	Maiden name				
	ID/ EID numbers	TRUE			
	Emergency contact				
Demographic	Date of birth		TRUE		TRUE
	Place of birth				TRUE
	Age				TRUE
	Gender		TRUE		TRUE
	Ethnicity				TRUE
	Race				TRUE
	Language information				TRUE
	Nationality				
	Photo				
Contact	Email address		TRUE	TRUE	TRUE
	Street address		TRUE		TRUE
	Postal code		TRUE		TRUE
	Telephone number	TRUE	TRUE	TRUE	TRUE
	Location details				
Transport	Bus assignment				
	Bus Pickup/drop location				
	Bus ID number				
Online	Device ID				
	Password		TRUE		
	IP address				
	Cookies				
	Browser history				
	Metadata using the application				
	Social media profile		TRUE		
Employment	Profession/Role				TRUE
	Job type				
	Job title		TRUE		TRUE
	Job level				
	Work experience				
	Professional certifications and licenses				TRUE
	Trade union membership				
	Employee classification				
	Professional license or certification number				TRUE
	Training Programs				
Educational	Academic degrees obtained				
	GPA				
	grades, performance, ranking				
	Schools and universities attended				
	Course of Study				TRUE
Financial	Financial account number				
	Credit card number				
	Salary				
	Income				
	Assets/Investments				
	Expenses/Debt				
	Credit Score				
Sensitive	Social Security Number				TRUE
	National identification number				TRUE
	Individual tax identification number				TRUE
	Economically Disadvantaged status				
	Immigration Status				TRUE
	Migration Status				
	Passport number				
	Sexual orientation				
	Military Status				
	Marital status				
	Vehicle identification number				
	Insurance				
	License plate number				
	Other sensitive data				
Health	Heath Information				
	Height				
	Weight				
	Genetic data				
	Diagnosis				
	Health symptoms				
	Health treatment				
	Medication				
	Disability information				
	Health insurance policy number				

Data Category	Elements	School Messenger Communicate	School Messenger Presence	School Messenger SafeArrival	Special Programs
	Medical record number				
Biometric	Finger prints				
	Retina scan				
	Voice print				
	DNA sequence				
	Facial photographs/recognition				
Religious	Religious affiliation				
	Place of worship membership				
Political	Political official position or appointment				
	Political party affiliation				
Criminal/ Legal	Criminal charges				
	Criminal convictions				
	Legal judgments or orders				
Attendance	Attendance records				
	Reason of absence			TRUE	
	Absence dates				
Others	Signature				TRUE
	Initials				
	Behavior				
	Survey Responses		TRUE		
	Disciplinary records				
	Security questions/answers				
	Any other data not listed above				
			Hair Color, Eye Color		

EXHIBIT "E" - GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Erie 1 Board of Cooperative Educational Services** ("New York Originating LEA") which is dated 03/18/2026, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed Exhibit "E" to Provider at the following **email address: legalnotices@powerschool.com**

PowerSchool Group LLC

BY: _____ Date: March 17, 2026

Printed Name: Jon Scrimshaw Title/Position: Chief Accounting Officer

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between **Erie 1 Board of Cooperative Educational Services** and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5 of the Originating DPA. **

By: Andrea Galenski Date: 2026-10-28

Printed Name: Andrea Galenski Title: Superintendent of Schools

SCHOOL DISTRICT NAME: Cheektowaga-Sloan Union Free School District

DESIGNATED REPRESENTATIVE OF LEA:

Name: Brian Zybala

Title: Director of Data and Techonlogy

Address: 166 Halstead Ave, Sloan, NY 14212

Phone: 716-897-7888

Email: bzybala@cheektowagasloan.org