

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

I. Explanation and Instructions

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

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

1. With respect to student data, personally identifiable information from the DOE’s education records, including but not limited to the following:
 - a. The student's name;
 - b. The name of the student's parent or other family members;
 - c. The physical or electronic address, device number (including telephone and mobile phone numbers, geolocation information and IP addresses) and other contact information of the student or student's family;
 - d. A personal identifier, such as the student's social security number, student number, or biometric record (including but not limited to fingerprints, facial images, iris scans and handwriting);
 - e. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
 - f. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty—including combinations of demographic, performance and school information that could lead to the student being identified); and
 - g. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
2. With respect to teacher or principal data, any annual professional performance review (APPR) data disclosed by the DOE to the Entity on an identifiable basis.

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

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

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

II. Questionnaire

1. Name of Entity

PowerSchool Group LLC

2. Type of Entity

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

Click or tap here to enter text.

3. Contract / Agreement Term

Contract Start Date: _____

Contract End Date: _____

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

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

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

Check all that apply:



☒ Student PII

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

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

☐ Other (You must explain below)

Click or tap here to enter text.

6. Subcontractor Written Agreement Requirement

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

Check one option only:

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

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

☐ Other (You must explain below)

Click or tap here to enter text.

7. Data Transition and Secure Destruction

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

☐ Securely transfer PII to School District, or a successor contractor at the School District's option and written discretion, in a format agreed to by the parties

☒ Securely delete and/or destroy PII

☐ Other (You must explain below)

Click or tap here to enter text.

8. Challenges to Data Accuracy

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

All requests for copies of PII or requests to challenge the accuracy of PII should be directed to the address in the Agreement.

Please select one option only:

☒ The Entity agrees to the procedure outlined above

☐ Other (You must explain below)

Click or tap here to enter text.

9. Security and Storage Protections

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

☒ Using a cloud or infrastructure owned tool hosted by a subcontractor

☐ Using an Entity-owned and/or internally hosted-solution

☐ No PII will be stored or hosted by Entity

☐ Other (you must explain below):

Click or tap here to enter text.

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

Data Security and Privacy Plan

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

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

- (a) To implement all state, federal, and local data security and privacy requirements, including those contained within this Data Security and Privacy Plan (“DSPP”), consistent with customer’s data security and privacy policy, Processor will: Review its data security and privacy policy and practices to ensure they are in conformance with all applicable federal, state, and local laws and the terms of this DSPP. In the event Processor’s policy and practices are not in conformance, Processor will implement commercially reasonable efforts to ensure such compliance.
- (b) As required by the NIST Cybersecurity Framework, to protect the security, confidentiality and integrity of the Customer Data that it receives under the MSA, Processor will have the following reasonable physical, administrative, and technical safeguards and practices in place throughout the term of the Agreement:

Data Security:

Processor ensures that both data-at-rest and data-in-transit (motion) is encrypted, and data leak protections are implemented.

Information Protection Processes and Procedures:

Processor performs data destructions according to the terms set in contracts and agreements. Processor also possesses a vulnerability management plan that will be developed and implemented.

Protective Technology:

To ensure that network communications are protected, log/audit records are ascertained, implemented, documented, and reviewed according to Processor/District policy.

Identity Management, Authentication and Access Control:

Processor manages remote access through credentials and identities that are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users.

- (c) If Processor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MSA, Processor will require such subcontractors, assignees, or other authorized agents to execute written agreements requiring those parties to protect the confidentiality and security of Protected Data under applicable privacy laws.

11. Encryption

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

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

☐ Other (you must explain below):

Click or tap here to enter text.