Plattsburgh City School District
Education Law 2-d Rider for Contracts with Third Party Vendor

1. Definitions

    a. **Breach** means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
    b. **Chief Privacy Officer** means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.
    c. **Commercial or Marketing Purpose** means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
    d. **Contract or other written agreement** means a binding agreement between the District and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.
    e. **District** means Plattsburgh City School District.
    f. **Disclose or Disclosure** mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.
    g. **Education Records** means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
    h. **Educational Agency** means a school district, board of cooperative educational services (BOCES), school, or the Department.
    i. **Eligible Student** means a student who is eighteen years or older.
    j. **Encryption** means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.
    k. **FERPA** means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
    l. **NIST Cybersecurity Framework** means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.
    m. **Parent** means a parent, legal guardian, or person in parental relation to a student.
    n. **Personally Identifiable Information ("PII")**, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C

1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10).

o. **Release** shall have the same meaning as Disclosure or Disclose.

p. **School** means any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law §3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law §4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

q. **Student** means any person attending or seeking to enroll in an educational agency.

r. **Student Data** means personally identifiable information from the student records of an educational agency.

s. **Teacher or Principal Data** means 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.

t. **Third-Party Contractor** means 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 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 pursuant to Education Law §211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

u. **Unauthorized Disclosure** or **Unauthorized Release** means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

2. Contractor agrees that the security, confidentiality, and integrity of student data and/or teacher or principal data shall be maintained in accordance with:

   a. Applicable state and federal laws that protect the confidentiality of personally identifiable information;

   b. The terms and conditions of the contract between the District and the Contractor, including but not limited to the Parents Bill of Rights for Data Security and Privacy and the Supplemental Information to Parents Bill or Rights for Data Privacy and Security, attached hereto and signed by a representative of Contractor and the District; and Applicable District policies, which can be accessed on the District website at: http://www.plattscsd.org/district/student-data-privacy-page

3. Contractor shall not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit any other party, employee, subcontractor or other agent of Contractor to do so.

4. Parents, eligible students, teachers, principals, and other staff of District may file a complaint of breach or unauthorized release of PII with the District based on the contract or written agreement with Contractor. Upon receiving any such complaint, District shall notify the complainant that it received the complaint, that it shall commence an investigation into the complaint, and shall take any necessary precautions to protect PII. All complaints must be submitted to the District in writing. Following the investigation, the District shall provide the complainant with its findings not more than 60 calendar days form the date the District received the complaint, unless an extension is warranted pursuant to 8 NYCRR § 121.4(c). District shall keep a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

5. The District understands the Contractor may use subcontractors to fulfill its responsibilities under its contract with the District, its employees or agents, and/or educational agencies which contract with the District for such services as is being provided by the Contractor and thus Contractor shall manage its relationships with subcontractors to ensure the protection of personally identifiable information consistent with state and federal law.

   Contractor also agrees and acknowledges that the data protection obligations imposed on it by state and federal law, as well as the terms of the agreement between the District and the Contractor shall apply to any subcontractor it engages in providing its contracted services to the District.

6. Contractor agrees that it will disclose student data and/or teacher or principal data only to those officers, employees, agents, subcontractors, and/or assignees who need access to provide the contracted services. Contractor further agrees that any of its officers or employees, and any officers or employees of any assignee or subcontractor of Contractor, who have access to PII will receive training on the federal and state laws governing confidentiality of such data prior to receiving access to that data.

7. Upon the expiration of the contract or written agreement between the District and the Contractor, without a successor agreement in place, Contractor shall assist the District in exporting any and all student data and/or teacher or principal data previously received by Contractor back to the District. Contractor shall thereafter securely delete or otherwise destroy any and all student data and/or teacher or principal data remaining in the possession of Contractor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of such data) as well as any and all student data and/or teacher or principal data maintained on behalf of Contractor in secure data center facilities. Contractor shall ensure that no copy, summary, or extract of the student data and/or teacher or principal data or any related work papers are retained on any storage medium whatsoever by Contractor, its subcontractors or assignees, or the aforementioned secure data center facilities. Any and all measures related to the extraction, transmission, deletion or destruction of student data and/or teacher or principal data will be completed within 30 days of the expiration of the agreement between the District and Contractor, and will be accomplished using an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. To the extent that Contractor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request,

Contractor and/or its subcontractors or assignees will provide a certification to District from an appropriate officer that the requirements of this paragraph has been satisfied.

8. Student data and/or teacher or principal data transferred to Contractor will be stored in electronic format on systems maintained by Contractor in a secure data center facility located in the United States, or a data facility maintained by a Board of Cooperative Educational Services. In order to protect the privacy and security of student data and/or teacher or principal data stored in that manner, Contract will take measure aligned with industry best practices and the NIST Cybersecurity Framework Version 1.1. Such measures shall include, but are not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

9. Contractor acknowledges that it has the following obligations with respect to any student data and/or teacher or principal data provided by the District, and any failure to fulfill one of these obligations set forth in New York State Education Law § 2-d and/or 8 NYCRR Part 121 shall also constitute a breach of its agreement with the District:

    a. Adopt technologies, safeguards and practices that align with NIST Cybersecurity Framework;

    b. Comply with the data security and privacy policy of the District, Education Law § 2-d, and 8 NYCRR Part 121.

    c. Limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of § 2-d and the FERPA.

    d. Not use education records and/or student data for any purpose other than those explicitly authorized in the contract or written agreement;

    e. Not disclose any personally identifiable information to any other party who is not an authorized representative of Contractor using the information to carry out Contractor's obligations under this Agreement, unless (i) that other party has the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

    f. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody;

    g. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the US Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

    h. Notify the District of any breach of security resulting in an unauthorized release of student data by Contractor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but not more than seven (7) calendar days after discovery of the breach. Upon such a complaint or allegations, Contractor shall cooperate with the District and any law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII;

    i. Where a breach or unauthorized release of personally identifiable information is attributable to Contractor, Contractor will pay or reimburse the District for the cost of any notifications the District is required to make by applicable law, rule, or regulation; and

j. Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of student and/or teacher/principal data by Contractor or its assignees in violation of applicable state or federal law, the parents bill of rights for student data privacy and security, the data privacy and security policies of the District and/or biding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. Contractor shall be subject to the penalties set forth in 8 NYCRR § 121.11 for any violations as outlined in same.

Adopted: September 24, 2020