## AGREEMENT REGARDING DATA SECURITY AND PRIVACY

Agreement dated as of April 7, 2022, by and between the Floral Park-Bellerose Union Free School ("District") and Studies Weekly, Inc. ("Contractor").

WHEREAS, the District has entered into a contract or other written agreement, as defined in Part 121 of the Commissioner's Regulations, with Contractor for certain services or products, a copy of which is annexed hereto; and

WHEREAS, Contractor is a third-party contractor as defined in Part 121 of the Commissioner's Regulations, that will receive student data or teacher or principal data from the District pursuant to said contract or other written agreement for purposes of providing services to the District; and

WHEREAS, the parties agree that if any provision of this Agreement conflicts with a provision of said contract or other written agreement, the provision as set forth in this Agreement shall supersede and prevail over said other provision;

NOW, THEREFORE, in consideration of the mutual covenants, conditions and agreements contained herein, and for other good and valuable consideration, including the above-referenced contract or other written agreement, the Contractor and the District hereby agree as follows:

A. The Contractor shall comply with all District policies and state, federal, and local laws, regulations, rules, and requirements related to the confidentiality of records and data security and privacy, including the District's Parents' Bill of Rights and Supplemental Information, annexed hereto and incorporated herein as Attachment "A".

B. The Contractor may receive personally identifiable information from student records ("Education Records") and/or personally identifiable information from annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release pursuant to Education Law § 3012-c and 3012-d (collectively, "PII Data"). The Contractor shall, therefore, comply with the following provisions in order to maintain the security and confidentiality of personally identifiable information:

(i) adopt technologies, safeguards and practices in alignment with the NSIT Cybersecurity Framework;

(ii) comply with the school district's data security and privacy policy;

(iii) limit the Contractor's internal access to Education Records to individuals with legitimate educational interests;

(iv) use PII Data only for the purposes explicitly authorized by this Agreement and not for any other purpose;

not disclose any personally identifiable information from PII Data to any other party without prior written consent, unless disclosure is required by statute or court order and written notice is given to the District (notice is not required if it is expressly prohibited by a statute or court order);

(v) maintain reasonable safeguards to maintain confidentiality of personally identifiable information in PII Data;

(vi) use legally mandated encryption technology[1] to protect data from unauthorized disclosure while the data is in motion or in the contractor's custody; and

(vii) not sell, use or disclose student, teacher or principal personally identifiable information for any marketing or commercial purpose.

C. The Contractor represents and warrants that its contract or written agreement with the District includes the Contractor's data security and privacy plan that is acceptable to the District. The Contractor's data security and privacy plan shall, at a minimum:

(i) outline how the Contractor will implement State and federal data security and privacy contract requirements for the life of the contract and is consistent with the school district's data security and privacy policy;

(ii) specify administrative, operational and technical safeguards the third-party contractor will use to protect personally identifiable information;

(iii) show that it complies with requirements of §121.3(c) of the Commissioner's Regulations;

(iv) specify how the third-party contractor's employees and any assignees with access to student data, or teacher or principal data receive or will receive training on relevant confidentiality laws, before receiving access to such data;

(v) specify if the third-party contractor will use subcontractors and how it will ensure personally identifiable information is protected;

(vi) specify an action plan for handling any breach or unauthorized disclosure of personally identifiable information and promptly notify the school district of any breach or unauthorized disclosure; and

(vii) describe whether, how and when data will be returned, transitioned to a successor contractor, deleted or destroyed when the contract ends or is terminated.

D. The Contractor must notify the District of any breach of security resulting in an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employee's, assignees or subcontractors. This notification must be made in the most expedient way possible and without delay. In addition, the Contractor must notify the District of the breach of security in writing. This written notification must be sent by the Contractor in the most expedient way possible and without unreasonable delay, and not later than seven (7) calendar days after discovery of the breach of security resulting in an unauthorized

[1] 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.

release of personally identifiable information from PII Data, to the designated District representative and either personally delivered or sent by nationally recognized overnight carrier to the District. In the case of an unauthorized release of personally identifiable information from PII Data by the Contractor or the Contractor's officers, employees, assignees or subcontractors, the Contractor must reimburse the District for all the District's costs associated with the District's obligation to notify the State's chief privacy officer, parents, students, teachers and/or principals of the unauthorized release.

IN WITNESS WHEREOF, the parties hereto have set their respective hands and seals as of the date and year first above written.

DISTRICT CONTRACTOR: Studies Weekly, Inc.

BY: ______________________ BY: ______________________

Ron Taylor, Chief Technology Officer

DATE: ______________________ DATE: 4/7/2022

# Parents' Bill of Rights Regarding Data Privacy and Security

Pursuant to Education Law Section 2-d, the Floral Park-Bellerose School District ("District") hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security,

1) A student's personally identifiable information cannot be sold or released for any commercial purposes;

2) Parents have the right to inspect and review the complete contents of their child's education record;

3) State and Federal laws protect the confidentiality of personally identifiable information (as defined under Education Law Section 2-d(d)), and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

4) A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Daniel Cunneely, Data Privacy Officer, Floral Park-Bellerose UFSD, 1 Poppy Place, Floral Park, New York 11001 at 516-434-2745 or dcunneely@fpbsd.org or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York, email to CPO@mail.nysed.gov.

6) Each contract the District enters into with a third party contractor where the third party contractor receives student data, or teacher or principal data, shall include the following supplemental information:
   a. The exclusive purpose for which the student data, or teacher or principal data, will be used;
   b. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by the data protection and security requirements;
   c. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

   d. If and how a parent, student eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
   e. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

7) The Parents’ Bill of Rights shall be subject to change pursuant to the direction from the New York State Education Department Chief Privacy Officer, and the Regulations of the Commissioner of Education.