Contract Addendum

Compliance with New York State Education Law Section 2-d

The parties to this Contract Addendum are the Dunkirk City School District (the "District") and *Inter-State Studio & Publishing Co.* ("Company" or "Vendor"). The District is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d"), and Vendor is a third party contractor, as that term is used in Section 2-d, pursuant to which Vendor receives access to student/teacher/principal data regulated by Section 2-d from the District that uses Vendor's product pursuant to the agreement between the District and Vendor. The District and Vendor have entered into this Contract to conform to the terms of the requirements of Section 2-d. To the extent that any term of the Vendor's own acceptable use policy conflicts with the terms of this Contract, the terms of this Contract shall apply and be given effect.

As used in this Contract Addendum, the term "student data" means personally identifiable information from student records that Vendor receives from the District, as defined by Section 2-d.

As used in this Contract Addendum, the term "teacher or principal data" means personally identifiable information from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential.

The Vendor shall submit to the District the completed attached addendum for review before final approval of this contract and it shall stay in effect for the duration of this contract. Any changes to the information provided must be communicated to the District and a new contract must be established.

A. Education Law Section 2-d(5)(d)

Vendor agrees that the security, confidentiality, and integrity of student/teacher/principal data shall be maintained in accordance with state and federal laws that protect the confidentiality of student/teacher/principal data, and also in accordance with Parents' Bill of Rights for Data Security and Privacy, which is attached to this Agreement and made a part of this Agreement.

B. Education Law Section 2-d(5)(e)

Vendor agrees that it will disclose student/teacher/principal data received from the District only to those officers, employees, and agents who have a legitimate educational interest in that data. Vendor further agrees that any of its officers or employees, and any officers or employees of any assignee of Vendor who have access to personally identifiable information will receive training on the federal and state law governing confidentiality of such data prior to receiving access to that data.

C. Education Law Section 2-d(3)(b)(1) and (c)(1)

The exclusive purpose for which Vendor is being provided access to personally identifiable information is to provide educational services. Student/teacher/principal data received by Vendor, or by any assignee of Vendor, from the District shall not be sold or used for marketing or commercial purposes.

D. Education Law Section 2-d(3)(c)(2)

Vendor shall ensure that to the extent that it comes into possession of student/teacher/principal data, it will only share that data with additional third parties if those third parties are contractually bound to observe this same student/teacher/principal data privacy agreement and abide by all the same security measures, and if such sharing of student/teacher/principal data is necessary for purposes of carrying out the underlying contract for educational services.

E. Education Law Section 2-d(3)(c)(3)

Upon expiration of this agreement without a successor agreement in place, the Vendor shall assist the District in exporting all student/teacher/principal data previously received from the District. The Vendor shall securely delete any copy of the data remaining in the Vendor's possession within ten (10) days of termination of services.

This contract will stay in effect throughout the duration that said contractor provides services to the District. This contract expires and must be renewed at any time the contractor makes any changes to their user end agreement or when there is a change in storing method or location of the District's student/teacher/principal data. The Vendor will make the District aware of any said changes so new agreements can be implemented.

F. Education Law Section 2-d(3)(c)(4)

In the event that a parent, student, or eligible student wishes to challenge the accuracy of student data concerning that student or eligible student, that challenge shall be processed through the procedures provided by the student's district of enrollment for amendment of education records under the Family Educational Rights and Privacy Act ("FERPA").

G. Education Law Section 2-d(3)(c)(5) and (5)(e)and (5)(f)(4) and (5)(f)(5)

Student/teacher/principal data transferred to Vendor by the District will be stored in electronic format on systems maintained by Vendor in a secure data center facility, or a data facility maintained by a board of cooperative educational services, in the United States. The measures that Vendor will take to protect the privacy and security of student/teacher/principal data while it is stored in that manner are associated with industry best practices and those set forth by the Secretary of the U.S. Department of HHS in guidance issued under Section

13402(H)(2) including, but not necessarily limited to disk encryption, file encryption, firewalls, and password protection.

H. Education Law Section 2-d(5)(f) and (6)

Vendor acknowledges that it has the following obligations with respect to any student/teacher/principal data received by the District and any failure to fulfill one of these statutory obligations shall be a breach of the Underlying Agreement:

- limit internal access to education records to those individuals that are determined to have legitimate educational reasons within the meaning of Section 2-d and FERPA;
- not use education records for any purpose other than those explicitly authorized in this Agreement;
- not disclose any student/teacher/principal data to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (1) that other party has the prior written consent of the parent or eligible student/teacher/principal, or (2) 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;
- maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of student/teacher/principal data in its custody;
- 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 U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;
- comply with the District's policy(ies) on data security and privacy, Section 2-D, and Part 121 of the Regulations of the Commissioner of Education;
- not sell student/teacher/principal data or 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 another party to do so;
- notify the educational agency from which student/teacher/principal data is received of any breach of security resulting in an unauthorized release of student data by the Vendor 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;

- cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of student/teacher/principal data;

- pay for or promptly reimburse the District for the cost of notification in the event the District is required pursuant to Section 2-d to notify affected parents, students, teachers or principals of any unauthorized release of protected data attributed to the Vendor its assignees.

It is understood that if the New York State Department of Education Chief Privacy Officer determines that a third party contractor or its assignee, in violation of applicable state or federal law, the data privacy and security policies of the educational agency provided by such educational agency to the third party contractor and/or binding contractual obligations relating to data privacy and security, has released any student data or teacher or principal data received from an educational agency to any person or entity not authorized by law to receive such data pursuant to a lawful subpoena or otherwise, the New York State Department of Education Chief Privacy Officer, after affording the third party contractor with notice and an opportunity to be heard, shall be authorized to fully exercise their duty as outlined in New York State Department of Education Section 2-D.

Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Dunkirk City School District hereby sets forth the following Parents' Bill of Rights for Data Privacy and Security, which is applicable to all students and their parents and legal guardians.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes;
2. In accordance with FERPA, Section 2-d -Student Records: Access and Challenge, parents have the right to inspect and review the complete contents of their child's education record;
3. The District has the following safeguards in place to protect student data, including personally identifiable information (PII) stored or transferred by the District.
   a. All databases that have student information are protected by a secure password and login. These logins are monitored and kept up to date.
   b. Student information is only accessible by those who are deemed warranted of having the information.
4. New York State, through the New York State Education Department, collects a number of student data elements for authorized uses. A complete list of all student data elements collected by the State is available for public review online.. Parents may also obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, N.Y. 12234.
5. Parents have the right to submit complaints about possible breaches of student data or teacher or principal APPR data. Any such complaint must be submitted, in writing,

to: Mr. Michael Mansfield, Superintendent of Schools, 620 Marauder Drive, Dunkirk, New York, 14048. Additionally, parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; the e-mail address is cpo@mail.nysed.gov. SED's complaint process is under development and will be established through regulations from the department's chief privacy officer, who has yet to be appointed.

Additional student data privacy information

This bill of rights is subject to change based on regulations of the commissioner of education and the SED chief privacy officer, as well as emerging guidance documents from SED. For example, these changes/additions will include requirements for districts to share information about third-party contractors that have access to
student data, including:

- How the student, teacher or principal data will be used;
- How the third-party contractors (and any subcontractors/ others with access to the data) will abide by data protection and security requirements;
- What will happen to data when agreements with third-party contractors expire;
- If and how parents, eligible students, teachers or principals may challenge the accuracy of data that is collected; and
- Where data will be stored to ensure security and the security precautions taken to ensure the data is protected, including whether the data will be encrypted.

Please click here for a list of software that the district utilizes and their privacy policies

ADDENDUM – SUPPLEMENTAL INFORMATION

The supplemental information obtained below will be included with the Dunkirk City School District (the "District") Parents' Bill of Rights as required by New York State Education Law Section 2-d [3][c]. The Parents' Bill of Rights and this supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

1. The Vendor agrees to use Student Data and/or Teacher or Principal Data for the exclusive purposes listed below:

See additional Document

2. The Vendor will provide to the District, in writing, a statement indicating how it will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose such Student Data and/or Teacher or Principal Data, if any, will abide by data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law Section 2-d).

See additional document

3. The Vendor will provide the District with a written description of what will happen to Student Data and/or Teacher or Principal Data upon expiration of this Agreement or other written agreement (e.g., whether, when, and in what format data will be returned to the District, and/or whether, when, and how the data will be destroyed).

See additional document

4. The Vendor will provide the District with a written description of how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data and/or Teacher or Principal Data that is collected.

See additional document

5.
The Vendor will provide the District with a written description of where the Student Data and/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 that such data will be protected, including, how such data will be protected using encryption while in motion and at rest.

See additional document

Agreed and accepted on this day: July 22, 2024

Print name : Cindy McCloskey

Sign name : Cindy McCloskey 7-22-2024
For: *Inter-State Studio & Publishing Co.* Date

Print name : Michele Heenan

Sign name : Michele Heenan 7-23-24
For: Dunkirk City School District, CIO Date

Dunkirk City School District
Page 4-5, Questions 1-5
7.22.2024

1.) The Vendor agrees to use Student Data and/or Teacher or Principal date for the exclusive purpose listed below:
School Picture Packages, ID cards, Admin downloads, Yearbooks, Banners, Poster and/or other related service items.

2.) The Vendor will provide to the District, in writing, a statement indicating how it will ensure that any subcontractors, or other authorized persons or entities to whom the Company will disclose such Student Data and/or Teacher or Principal Data, if any, will abide by data protection and security requirements, including, but not limited to, those outlined in applicable state and federal laws and regulations (e.g., FERPA, Education Law Section 2-d):

The only possible outside entity to receive Student and/or Teacher data directly from Inter-State is the vendor providing yearbook creation software, and the only data shared directly is name, grade, and image.

In many cases, schools transfer data directly to the yearbook vendor without Inter-State's involvement. Additionally, Inter-State does not provide yearbooks for some schools, eliminating any possibility of data sharing with outside vendors in those cases.

Yearbook software vendors receiving direct transfers are certified annually to comply with all federal privacy laws.

3.) The Vendor will provide the District with a written description of what will happen to Student Data and/or Teacher or Principal Data upon expiration of this Agreement or other written agreement (e.g., whether, when, and in what format data will be returned to the District, and/or whether, when, and how the data will be destroyed).

[Copied from https://inter-state.com/privacy]

When Inter-State is engaged by a school or other organization as its official photographer, the photos we capture for that organization are deleted in the ordinary course of business within a reasonable time after we have fulfilled our contractual obligations, with the exception of photos associated with customers who elect to purchase from us (Inter-State Customers). If you are an Inter-State Customer, our goal is to make the photos we create available to you for years to come, and we will endeavor to retain a digital copy of one or more of your current and future source photos for you to claim and archive in your Inter-State account indefinitely, if you choose to do so. For example, if you purchase your child's first grade school photo, and Inter-State photographs your child the following year, we may associate that photo with you and make the digital image available to you to purchase and store in your Inter-State account.

If you wish, you can take steps to have your photos deleted from our systems earlier, by contacting us at issnet@inter-state.com. We may require certain information from you to validate your request before deletion. Please be aware, however, that Inter-State may deny your request and retain your photos under certain limited circumstances – for example, if we have a contractual commitment to a school or other organization you are affiliated with (such as providing yearbook photos or the yearbook itself), if doing so would violate a law or court order, or if it would be unreasonably burdensome. Also, please be aware that, if you shared your photo with other purchasers, your photo deletion request will not affect any photos retained in others' photo libraries or those purchasers' archiving preferences.

4.) The Vendor will provide the District with a written description of how a parent, student, eligible student, teacher or principal may challenge the accuracy of the Student Data and/or Teacher or Principal Data that is collected.

[Copied from https://inter-state.com/privacy]

Parents have the right to access any data we have on them or their children in order to review or correct it. We will honor a parent's image/data deletion and/or modification request, subject to verification, and authorization of the school when deletion would impact our ability to deliver an item or service requested by the school.

We generally recommend these requests be handled through the school, but requests for access, modification/deletion not affecting an item or service requested by the school, or any questions about your personal data may also be directed to issnet@inter-state.com.

5.) The Vendor will provide the District with a written description of where the Student Data and/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 that such data will be protected, including, how such data will be protected using encryption while in motion and at rest.

It depends on where data is in our workflow. Outside our hardened perimeter, it will be encrypted. Inside our hardened perimeter, it will be on storage devices password protected from unauthorized network access through directory rights management and/or 2FA.

Servers inside our perimeter are also physically protected from unauthorized access in our server room which is constructed with concrete walls and a steel vault style door. Limited access is granted only to required technology and safety staff.