Parents' Bill of Rights for Data Privacy and Security

In accordance with New York State Education Law Section 2-d, the Southern Westchester Board . of Cooperative Educational Services ("Southern Westchester BOCES") 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) New York Stated Education law Section 2-d (Section 2-d") and the Family Educational Rights and Privacy Act ("FERPA") protect the confidentiality of personally identifiable information. Section 2-d and FERPA assure the confidentiality of records with respect to "third parties." and provides parents with the right to consent to disclosures of personally identifiable information contained in their child's education records. Exceptions to this include school employees, officials and certain State and Federal officials who have a legitimate educational need to access such records. In additions, the Southern Westchester BOCES will, upon request of parents, legal guardians or eligible students, or if otherwise required by law, disclose student records to officials of another school district in which a student seeks to enroll. An eligible student is a student who has reached 18 years of age or attends a postsecondary institution.

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

(3) Personally, identifiable information includes, but is not limited to:

      i.   The student's name;

      ii.   The name of the student's parent or other family members;

      iii.   The address of the student or student's family;

      iv.   A personal identifier, such as the student's social security number. student number, or biometric record;

      v.   Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

      vi.   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; or

      vii.   Information requested by a person who the Southern Westchester BOCES reasonably believes knows the identity of the student to whom the education record relates.

(4) In accordance with FERPA, Section 2-d and Southern Westchester BOCES Policy No. 6320, Student Records: Access and Challenge, parents and legal guardians have the right to inspect and review the complete contents of their child's education record.

(5) Southern Westchester BOCES has the following safeguards in place: Encryption, firewalls and password protection, which must be in place when data is stored or transferred.

(6) 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 at the following links or can be obtained by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, NY 12234:

http://www.p12.nysed.gov/irs/data_reporting.html
http://data.nysed.gov/
http://www.p12.nysed.gov/irs/sirs/documentation/nyssisguide.pdf

(7) Eligible students, parents and legal guardians have the right to have complaints about possible breaches of student data addressed. Any such complaint should be submitted, in writing, to the Data Protection Officer of Southern Westchester BOCES at dpo@swboces.org or at 450 Mamaroneck Avenue, Harrison, New Yorkk 10528. Parents can direct any complaints regarding possible breaches via the electronic form on the Southern Westchester BOCES home page, under Resources, and Student Privacy. The complaint form can also be found by going to https://bit.ly/swbdatabreach. Alternatively, a written complaint may also be submitted to the Chief Privacy Officer of the New York State Education Department using the form available at http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure or writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234.

Supplemental Information for Agreement with ____Edlio_____
(hereinafter "Company")

(1) The personally identifiable student data or teacher or principal data (collectively, "the Data")
received by Company will be used exclusively for the following
purpose(s):_____

_____

**Data received by Edlio will be used in the development and publishing of school website
content and the dissemination of school information to Parent, Students, Teachers and
School Officials. This data may also be used by our Broadcast application to alert
parents of school related news.**

(2) The Company will ensure that all subcontractors and other authorized persons or entities to
whom Data will be disclosed will abide by all applicable data protection and security
requirements, including those mandated by New York State and federal laws and regulations,
by the following means: _____

_____

**As described in the previous section, Edlio requires any subcontractors with access to
sensitive data to abide by the same policies, procedures and recurring security training
as all full-time staff.**

(3) The Agreement with Company commenced on December 21, 2022. The initial term ends on
June 30,

2023_; however, the term is automatically renewed for 12 month periods unless Company
or Southern Westchester BOCES provide notice of non-renewal at least thirty days prior to
the expiration of the applicable term. Upon the expiration or termination of the Agreement,
all Data will be (check all that apply and fill in required information):

☐ Returned to Customers by <mark>90 days</mark> [date] in the following format(s):_____

_____

☐ Returned to Southern Westchester BOCES by <mark>90 days</mark> [date] in the following
format(s): _____

_____

X Securely deleted and/or destroyed by __TBD_ [date] in the following manner: Edlio will
delete and/or destroy data at the request of BOCES or after 90 days of contract termination.

_____.

☐ Other – explain _____

_____

_____

If student data or teacher or principal data is to be maintained by Company for any lawful purpose, such data shall remain in an encrypted format and shall be stored on systems maintained by Company in a secure data facility located within the United States.

(4) In the event that a student's parent or guardian or an eligible student seeks to challenge the accuracy of student data pertaining to the particular student, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures of Southern Westchester BOCES. In the event that a teacher or principal seeks to challenge the accuracy of teacher or principal data pertaining to the particular teacher or principal, which data may include records maintained, stored, transmitted or generated by the Third-party Contractor pursuant to its Agreement with Southern Westchester BOCES, the challenge will be directed to Southern Westchester BOCES and processed in accordance with the procedures Southern Westchester BOCES has established for challenging annual professional performance review ("APPR") data.

(5) Describe where the Data will be stored (in a manner that will protect data security) and the security protections that will be taken by Company to ensure the Data will be protected and data security and privacy risks mitigated:_____ _____

Data will be stored according to industry best practices within our cloud storage provider AWS at their north-west facilities in Oregon. Edlio continues to monitor and adopt stringent security standards as outlined by NIST, PCI and CIS. Some of the more common security practices include annual independent Penetration Testing, monthly Vulnerability Scans, routine cadence software security patching and MFA requirements for all accounts with elevated access to volume data. Single Sign-On (SSO) support for popular Identity Providers (IDPs) as well as optional two-factor authentication for secure login. We handle all data storage, security, and backups and ensure the highest level of security. We have adopted industry leading security practices to include advanced network protection technologies to prevent common attack trajectories such as DDoS, brute force, and API traffic surge. A nationwide content delivery network (cdn) has been implemented to improve website performance and provide for enhanced business continuity.

(6) Describe how the Data will be protected using encryption while in motion and at rest:

Data is protected using encryption while in motion and at rest for all platforms. This includes SSL\TLS security for data encryption while in motion. Data at rest is stored within AWS. Data at rest is secured using algorithms and key lengths consistent with the most recent NIST guidelines. Encryption has been adopted for our RDS database, SFTP servers and AWS S3 buckets. SSL certificates and ongoing management are included for each customer.

Company Name: _____ Edlio LLC _____

Authorized Signature: _____

Authorized Signer's Name & Title: _____ Anni Baghdasarian, President _____

Date: _____ 3/1/23 _____

SCHEDULE C-2

[Signed copy of Customers' Parents' Bill of Rights for Data Privacy and Security]