

# PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

SCIO CENTRAL SCHOOL DISTRICT is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education

Law Section 2-d and its implementing regulations, SCIO CENTRAL SCHOOL DISTRICT informs the school community of the following:

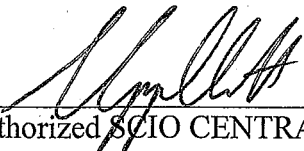
1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record.
3. State and federal laws protect the confidentiality of personally identifiable information, 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 New York State is available for public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints should be directed in writing to SCIO CENTRAL SCHOOL DISTRICT Data Privacy Officer, 3968 Washington Street Scio, NY 14880 or by using the form available at the following website: <https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/>. Complaints may also be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first written above.

Matt Stricker

Matt Stricker (Oct 14, 2020 14:07 CDT)

Authorized Vendor Signature



Authorized SCIO CENTRAL SCHOOL DISTRICT  
Signature

Oct 14, 2020

Date

10/14/2020

Date

Collects:  Student Data  Teacher or Principal Data  Does not collect either

Educational agencies including Cattaraugus-Allegany-Erie-Wyoming BOCES are required to *post information about third-party contracts on the agency's website* with the Parents Bill of Rights. To that end, please complete the table below with information relevant to NYS Education Law 2-d and Part 121.3 of the Commissioner's Regulations. Note that this applies to all software applications and to mobile applications ("apps").

**Part 1: Exclusive Purposes for Data Use**

The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor: To provide products and services to the Scio Central School District

**Part 2: Subcontractor Oversight Details – Select the appropriate option below.**

- This contract has no subcontractors.
- This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey data protection and security requirements consistent with those that the third-party contractor is required to obey under state and federal law:

**Part 3: Contract Lifecycle Practices**

The contract expires on \_\_\_\_\_ unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, protected data will be deleted by the contractor, via shredding, de-identification, mass deletion, and upon request, may be exported for use by Sa before deletion.

**Part 4: Student Educational Records / Improper Disclosure**

- A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website.
- B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form.

**Part 5: Security Practices**

A. Protected data provided to the contractor will be stored: (include *where* and *how*) Vendor will store the protected data on servers in a secured facility in the United States. Vendor will maintain a comprehensive information security program and will use reasonable and appropriate administrative, procedural and technical measures, consistent with industry standards, to protect the security, confidentiality and integrity of the protected data.

B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include: Vendor abides by a comprehensive data governance model that incorporates rules, policies, standards and procedures based on ISO 27001 and NIST 8.0 security and privacy frameworks. Vendor stores, processes and protects protected data in accordance with industry standards and applicable law. Vendor's comprehensive information security program protects data from unauthorized access, use and disclosure using reasonable and appropriate physical, administrative and technical safeguards. Vendor performs periodic risk assessments of its information security program and prioritize remediation of identified security vulnerabilities. At all times, Vendor shall maintain

appropriate physical, technical and administrative security measures, including protection against, unauthorized access, unlawful use, accidental loss, corruption, or destruction of protected data, as set forth in our Data Privacy and Security Documentation. Vendor regularly monitors compliance with these measures and commits to never materially decrease the overall security of the services during an agreed upon term.

**Part 6: Encryption Practices**

By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).