

APPENDIX A

SECTION A

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-d of the New York State Education Law, parents and eligible students are entitled to certain protections regarding personally identifiable student information. The **Suffern Central School District** is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below:

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 stored or maintained by the educational agency.
3. The District is committed to implementing safeguards associated with industry standards and best practices under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection, which 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.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the NYS Education Department, Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to Mr. Paul Zeller, Data Privacy Officer Suffern Central School District 45 Mountain Ave. Hillburn, New York 10931. pzeller@sufferncentral.org or at 845-357-7783, ext. 11284.
6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of personally identifiable information occurs.
7. The District has entered into contracts with certain third party contractors ("TPC") who have been sent personally identifiable student data as defined in 34 C.F.R. §99.3 and/or personally identifying teacher and/or principal data as defined by Education Law §3012-c(10). The following information about such contractors appears in such supplemental information to this document for each contract with a TPC, as required by law:
 - The exclusive purposes for which the student or teacher or principal data will be used by the TPC, as defined in the contract;
 - How the TPC will ensure that its subcontractors or other authorized individuals who will be in receipt of the data will abide by the applicable data privacy and security requirements of the federal and state laws and regulations (e.g., FERPA; Education Law §2-d);
 - The duration of the contract that sets forth its expiration date and description of what will be done with the data upon the expiration of the contract (e.g. whether, when and in what format the data will be returned to the educational agency or destroyed); and

- If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the data that is collected.

8. The District employees that handle personally identifiable information will receive training on applicable state and federal laws, the District's policies, and safeguards associated with industry standards and best practices that protect such information.

9. Agreements with TPCs will ensure that the subcontractors, persons or entities with whom the TPC will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

10. A parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected by filing a written request with the Superintendent of Schools or his administrative designee, Mr. Paul Zeller, Data Privacy Officer, Suffern Central School District, 45 Mountain Avenue, Hillburn, New York 10931, pzeller@sufferncentral.org.

APPENDIX A
SECTION B

Supplemental Information Agreement between
Suffern C.S.D. and Paradigm Cyber Ventures, LLC

The Suffern C.S.D. ("District") has entered into an Agreement with Paradigm Cyber Ventures, LLC, which governs the availability to the District of the following products or services:

Pursuant to the Agreement (which includes a Data Sharing and Confidentiality Agreement), the District may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving Protected Data from the District is to provide the District with the functionality of the products or services listed above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within the Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or entities to perform one or more of its obligations under the Agreement (including subcontracting hosting of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized persons or entities to whom it will disclose the Protected Data to execute legally binding agreements acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable data protection, privacy and security requirements required of Vendor under the Agreement and applicable state and federal law and regulations.

Duration of Agreement and Protected Data upon Termination or Expiration:

- The Agreement commences on July 1, 2026 and expires on June 30, 2027.
- Upon expiration of the Agreement without renewal, or upon termination of the Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the District in exporting all Protected Data previously received back to the District for its own use, prior to deletion, in such formats as may be requested by the District.
- In the event the Agreement is assigned to a successor Vendor (to the extent authorized by the Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor

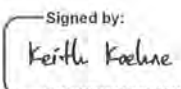
and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide the District with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents, guardians, or eligible students (students who are 18 or older or attending postsecondary institution) can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law Sections and with Sections 121.1(i) and 121.3(c)(6) of the Regulations of the Commissioner of Education.

Name: Keith Koehne Date: 9/24/2026

Signature:  E3B32828404041C...

By signing above, you agree to comply with the terms of the Suffern C.S.D. Data Sharing and Confidentiality Agreement and the Suffern C.S.D. Parents Bill of Rights for Data Privacy and Security, including the required Supplemental Information.