Addendum D

Parents Bill of Rights for Data Privacy and Security SULLIVAN BOCES PARENT BILL OF RIGHTS

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The District's Bill of Rights will state in clear and plain English terms that:

a. A student's personal identifiable information (PII) cannot be sold or released for any commercial purposes;

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

c. State and federal laws protect the confidentiality of PII, 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;

d. A complete list of all student data elements collected by the state is available for public review at the following website http://www.nysed.gov/student-data-privacy/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; and

e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/student-data-privacy/form/reportimproper-disclosure. Parents can also send their written complaint to the Sullivan BOCES Data Protection Officer at 15 Sullivan Avenue, Suite 1, Liberty New York 12754

Addendum E

PARENTS' BILL OF RIGHTS - SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by SchedShape, Inc. **(the "Vendor")** are limited to the purposes authorized in the contract between the Vendor and Sullivan County BOCES **(the "BOCES")** dated December 5, 2025 **(the "Contract Date")**.

2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to, those outlined in applicable State and Federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"); Education Law § 2-d; 8 NYCRR § 121).

3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in: (choose one)

   ☐ The agreed upon format to BOCES (or)

   ☐ Will be destroyed by the Vendor as directed by the BOCES

4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the BOCES in a Vendor's product and/or service by following the BOCES's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by BOCES in the Vendor's product and/or service by following the appeal procedure in the BOCES's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES:** Confidential Data provided to the Vendor by the BOCES will be stored United States of America The measures that the Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum F

VENDOR'S DATA SECURITY AND PRIVACY PLAN

SchedShape
Data Security and Privacy Plan

1. Purpose and Scope

This plan describes the administrative, technical, and physical safeguards SchedShape uses to protect education records and other regulated information disclosed by educational agencies. It applies to all systems, data stores, environments, and subcontractors that support the SchedShape platform.

2. Regulatory Alignment

SchedShape's controls and practices are designed to align with the following standards and regulatory frameworks:

- FERPA and applicable state student-data privacy laws
- NIST SP 800-171 and NIST Cybersecurity Framework (CSF) principles
- SOC 2 Type I security and availability control families (as implementation goals)
- CIS Critical Security Controls

SchedShape is not representing full certification, but these frameworks guide its security posture.

3. Data Classification and Minimization

SchedShape classifies all student identifiers, including student name and student ID, as personally identifiable information.

We collect and process only the minimum data required to deliver the scheduling and integration services requested by districts.

No data is used for advertising, profiling, or resale.

4. Data Storage and Encryption

All data is stored exclusively in United States data centers.

Encryption in transit: TLS 1.2 or higher.

Encryption at rest: AES-256 for databases, object storage, and backups.

Credentials, tokens, and secrets are stored using industry-standard secret-management controls.

5. Access Control

SchedShape uses role-based access control to restrict access to authorized personnel with a legitimate business need.

All employee accounts use MFA.

Least-privilege principles apply to production access, which requires management approval and is logged.

District-level users control their own access rights within the application.

6. Authentication and Password Requirements

SSO and OAuth 2.0 support are provided where applicable.

Password requirements follow NIST 800-63 guidelines including length requirements, screening against known compromised passwords, and lockout thresholds.

7. Network and Infrastructure Security

Our cloud infrastructure is hosted on a major provider that maintains independent SOC 2, ISO 27001, and FedRAMP compliant environments.

We implement virtual private networks, firewalls, security groups, isolated subnets, and automated patching of managed services.

Inbound and outbound traffic is monitored and logged.

8. Application Security

SchedShape follows secure SDLC practices including code review, dependency scanning, and static analysis checks.

We use automated scanning for vulnerabilities in containers, libraries, and third-party components.

Penetration testing is conducted annually by an independent assessor or qualified internal staff.

9. Logging, Monitoring, and Incident Detection

SchedShape maintains centralized logging of authentication events, administrative actions, and system activity.

Security alerts are monitored and triaged.

Audit logs are retained for at least one year.

Anomaly detection tools are used to flag suspicious behavior.

10. Incident Response

Schedshape maintains a documented incident response plan. In the event of any confirmed or suspected unauthorized access to customer data, SchedShape will take immediate action to contain and investigate the incident and will promptly notify the customer. We will share available information about the nature, scope, and impact of the incident, coordinate on required remediation steps, and support any follow-up actions. SchedShape will not communicate with end users or external parties about the incident without the customer's direction, unless required by law.

11. Data Retention and Destruction

Data is retained only for the duration of the contract and active services.

Upon request or termination, data will be securely deleted within 60 days following NIST 800-88 guidance.

Backup retention is time-limited, encrypted, and purged according to our backup policy.

12. Subprocessors

SchedShape uses only vetted service providers with contractual obligations to maintain equivalent security controls.

A list of subprocessors is available upon request and will be updated as services change.

No subprocessor may access student PII except as required to perform contracted functions.

13. Employee Training and Background Screening

All employees with access to production systems undergo background checks permitted by law.

Staff receive annual training on data privacy, FERPA, security awareness, and incident reporting procedures.

14. Business Continuity and Disaster Recovery

SchedShape maintains a documented business continuity and disaster recovery plan.

We use redundant infrastructure, automated backups, and validated restore processes. Our objective is to restore critical operations within commercially reasonable timeframes.

15. Privacy Protections

SchedShape does not sell, share, or use customer data for marketing, advertising, or behavioral profiling.

Data is disclosed only to the limited third parties necessary to operate the service or when required by law.

If a legal obligation requires disclosure, SchedShape will provide advance notice to the customer to the extent permitted by applicable law.

16. Data Subject Rights

District administrators may request correction or deletion of data at any time. SchedShape does not claim ownership over any education records.

17. Contact

Security and privacy inquiries may be directed to:
Mike Fedosov, CTO
Michael@schedshape.com