Appendix B: Data Security and Privacy Plan

SchFront and the Customer hereby agree to make this Data Security and Privacy Plan part of their Agreement for products and services.

Terms used in this Data and Security Privacy Plan (hereinafter the "Plan") shall have the same meanings as those found in Education Law Section 2-d(1) and the Regulations of the Commissioner of Education at Section 121.1 of Title 8 of the New York Codes, Rules and Regulations (8 NYCRR § 121.1), unless more broadly defined herein.

SchFront is a "Third Party Contractor" as that term is defined in the Education Law Section 2-d(1) and the Regulations of the Commissioner of Education at Section 121.1 of Title 8 of the New York Codes, Rules and Regulations (8 NYCRR § 121.1).

SchFront will implement and maintain all state, federal and local data security and privacy requirements over the term of the Agreement in a manner that is consistent with the data security and privacy policies of the Customer and each Permitted User that purchase SchFront's products and/or services pursuant to the Agreement by maintaining the implementation of required administrative, physical, and technical safeguards stipulated in the regulations.

The Administrative Safeguard Standard, "Evaluation," requires the periodic technical and nontechnical evaluation of SchFront's compliance in response to environmental and/or operational changes affecting the security of Customer data. Changes to state, federal and local data security and privacy requirements are defined as in-scope "environmental changes" and, as such, are monitored, evaluated, and integrated (or otherwise appropriately responded to) with other environmental and operational changes impacting the security and privacy of Customer data to ensure consistent SchFront compliance.

When new Customer Agreements are negotiated pursuant to the Agreement, SchFront will review and sign Customer-specific "Parent's Bill of Rights" and supplemental data security and privacy-related provisions of the Customer as required, provided such requirements do not conflict with or weaken SchFront's implemented administrative, physical, and technical safeguards and practices or violate applicable laws and regulations.

SchFront has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it receives, maintains, stores, transmits or generates pursuant to the Agreement:

SchFront has implemented and will maintain administrative/operational safeguards:

- Security Management Process - Risk analysis procedure, risk management procedure, sanction policy, information system activity monitoring and review procedures.
- Assigned Data Privacy and Security Responsibility - "Information Security Officer" responsible for the administration of SchFront information privacy and security policies and procedures.

- Workforce Security – Authorization and/or supervision definition, workforce clearance procedure, termination procedures, workforce development procedure.
- Information Access Management - Isolation of data and functions in systems using least privileged model of authentication, access authorization procedures, access establishment and modification guidelines and procedures.
- Security Awareness and Training – Training and routine security and privacy-related communication/reminders, content explicitly addressing protection from malicious software and external threats, content addressing SchFront requirements under applicable laws and regulations, content explicitly explaining SchFront policies and procedures developed to protect Customer data, monitoring of all system/data access and usage, password management/policy.
- Security Incident Procedures – Response and Reporting
- Contingency Plan – Data backup policy, disaster recovery procedure, emergency operation plan, testing and revision procedure, applications/data criticality analysis.
- Routine Evaluation – Periodic technical and nontechnical evaluation of SchFront's implemented administrative, physical, technical safeguards, and practices.
- Policies and Procedures for Third-Party Relationships – Only applicable if such relationships are allowed by the Agreement.

SchFront has implemented and will maintain physical safeguards:

- Facility Access Controls - Contingency operations, facility security plan, access control and validation procedures, maintenance records
- Workstation Use - Acceptable Use Policies for Assets and Data, Context-, Device-, and Location-specific Policies and Procedures for the secure access of systems and data.
- Workstation Security - Secure workstations, hardware, and devices to restrict access to authorized users.
- Device and Media Controls – Disposal, media re-use, accountability, data backup and storage

SchFront has implemented and will maintain technical safeguards:

- System/Data Access Control - Unique user identification, emergency access procedure, automatic logoff, encryption and decryption.
- Audit Controls – Hardware/software/procedural mechanism(s) to log and analyze activity in SchFront information systems that house or use Customer data.
- Integrity – Mechanism(s) to protect Customer data from improper alteration or destruction.

- Person or Entity Authentication – Mechanism(s) to validate the identities of persons/entities accessing SchFront systems and prevent unvalidated access.
- Transmission Security – Integrity controls, encryption.

The following are SchFront's responsibilities as a third-party contractor to the Customer, a NYS educational agency:

- Controlling and managing the access of approved SchFront employees (and Subcontractor/Assignee users, as applicable), collectively "SchFront Users," to SchFront systems and Customer data, including:
    - Thoroughly vetting SchFront Users before authorizing their access to SchFront systems and Customer data.
    - Providing training and communication to SchFront Users about laws and regulations governing the access and usage of Customer data, acceptable use, and usage monitoring and sanctions prior to granting access to SchFront systems and Customer data.
    - Ensuring SchFront Users are allowed only the minimal access to SchFront systems and Customer data that they need to do their job.
    - Ensuring that SchFront User system and data-related access levels are reviewed and adjusted as necessary when their role within SchFront (or in the context of the Subcontractor/Assignee relationship) changes, including upon employment or contract conclusion/termination.
- Monitoring SchFront User system activity to ensure that SchFront Users adhere to SchFront "Acceptable Use" rules and access/use Customer data exclusively for the purposes defined by applicable Customer Agreement.
- Leveraging technologies, practices, and safeguards that align with the NIST CSF and comply with Customer data security and privacy policy, including:
    - Using encryption technology to protect data while in motion and in SchFront custody from unauthorized disclosure.
    - Securely retaining and backing-up Customer data housed in SchFront Systems.
    - Securely housing SchFront systems and Customer data in environments that reflect industry best-practices and comply with state and federal laws and regulations for privacy and security.
    - Implementing the Plan, managing the implementation, and monitoring the continued compliance of the Plan with applicable laws and regulations.
    - Providing SchFront Users with routine training, as appropriate, addressing the secure and private usage of SchFront systems and Customer data in all contexts of access and usage deemed acceptable under the Agreement.

- Returning and/or destroying, as applicable, Customer data in SchFront procession following the conclusion/termination of the Customer agreement, per the terms of the Agreement.
- Directing all requests for access to, or challenges to the accuracy of, Customer data a (i.e. by parents, guardians, students, teachers, or any other type of Customer End-User) to the Customer for handling.
- Reviewing and accepting Customers' Parent's Bill of Rights for Data Privacy and Security.
- Forbidding and protecting against the sale, use, or disclosure of Customer data by SchFront Users for marketing or commercial purposes.
- Performing routine risk assessment and updating implemented administrative, physical, technical safeguards, and practices as necessary to mitigate new/changed risk.
- Monitoring SchFront User compliance with the Plan.
- Notifying impacted Customer(s) of any breach or unauthorized release of Customer data after discovery of a breach.

  Cooperating with the Customer(s) and law enforcement to protect the integrity of investigations regarding breach or unauthorized release of Customer data.

Officers and employees of SchFront (and its subcontractors and assignees, as applicable) who will have access to Customer student, teacher or principal data will receive training on the federal and state laws governing the confidentiality of such data prior to receiving access to the data. This training will be provided during the new SchFront User "onboarding" period to all new officers and employees of the Company (and its subcontractors and assignees, as applicable) who will to be given access to Customer data.

SchFront will not utilize sub-contractors in the performance of the Agreement.

SchFront has implemented extensive usage and access monitoring and logging on SchFront controlled systems and environments to identify aberrant, unacceptable, unauthorized, overtly malicious, or otherwise threatening usage/access.

In addition, SchFront has provided and communicated the means by which data security and privacy related concerns may be reported both internally and externally (i.e. via the "SUBMIT A TICKET" link at https://support.schoolfront.com/home/ or via email address, mailto:abuse@schoolfront.com).

With the implementation of the administrative safeguard standard, "Security Incident Procedures & Reporting," SchFront has created and deployed processes and procedures for managing data privacy and security incidents. If a reported or otherwise identified security incident is suspected to be a data privacy breach, the SchFront Information Security Officer will:

1. Determine what information, systems, or environments were suspected to be breached.
2. Identify the scope, time frame and source(s) of breach, type of breach, whether data encryption was used and for what, possible suspects (internal or external, authorized or unauthorized, employee or non-employee user).
3. Bring in an incident response expert or law enforcement to conduct an investigation (as necessary and appropriate).
4. Monitor all systems for active intrusions and attacks.
5. Confirm there are no other compromised data, systems, or environments.
6. Determine the notification requirements (statutory or contractual) and complete breach communication tasks as required within the specified timeframe (if applicable).

Upon the expiration or termination of the Agreement, if requested by the Customer, SchFront will assist the Customer in exporting all student, teacher or principal data previously received from the Customer or generated by SchFront pursuant to the Agreement.

In addition, SchFront will remove Customer student, teacher or principal data previously received from the Customer or generated by SchFront pursuant to the Agreement from accessible SchFront systems and will remove all Customer access to SchFront information systems. Digital notice will be provided to the Customer following the completion of Customer data removal.

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