DATA PRIVACY & SECURITY POLICY
STOREFRONT ACADEMY CHARTER SCHOOLS

This Policy addresses the responsibility of Storefront Academy Charter Schools ("the School") to adopt appropriate safeguards and controls to protect the confidentiality and integrity of its data and information technology resources, as required by Education Law Sec. 2-d and Part 121 of the Regulations of the Commissioner of Education. "the School" adopts this policy to implement the requirements of the law and to align the School's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

I. Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, "the School" will take steps to minimize its collection, processing, and transmission of Personally Identifiable Information (**"PII"**).

"The School" will monitor its data systems, develop incident response plans, limit access to PII to School employees, interns, volunteers, independent contractors, and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Additionally, "the School" will:

a) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and School policy.

II. Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

"The School" will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

III. Data Protection Officer

"The School" has designated an employee to serve as the School's Data Protection Officer. The Data Protection Officer for the School will be appointed by the School's Executive Director.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations to develop and maintain a comprehensive Data Privacy and Security Program. The Data Protection Officer will serve as the main point of contact for the School's Data Privacy and Security Program.

The School will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

IV. School Data Privacy and Security Standards

"The School" will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles.

The School will protect the confidentiality and privacy of student and teacher/principal PII while stored or transferred by:

a) Ensuring that every use and disclosure of PII by the School benefits students and the School by considering, among other criteria, whether the use and/or disclosure will:

1. Improve academic achievement;

2. Empower parents and students with information; and/or

3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents. The Data Protection Officer will, together with program offices, determine whether a proposed use of PII is not included in public reports or other documents, or otherwise publicly disclosed.

c) Using industry standard safeguards and best practices, such as encryption, firewalls, and passwords.

The School affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

V. Third-Party Contractors

School Responsibilities

"The School" will ensure that whenever it enters into a contract or other written agreement with a third-party contractor, and the contractor will receive student data or teacher or principal data from the School, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state laws and regulations, and School policy. The contract or written agreement with the third-party contractor will include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the School under which the third-party contractor will receive student data or teacher or principal data from the School, is required to adopt technologies, safeguards, and practices that align with the SACS Cybersecurity Framework and comply with School's data security and privacy policy, Education Law Section 2-d and its implementing regulations, and applicable laws impacting the School.

VI. Complaints of Breach or Unauthorized Release of Data

The School will inform parents/guardians, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the School will have procedures in place for parents, guardians, eligible students, teachers, principals, and other School staff to

file complaints with the School about breaches or unauthorized releases of student data and/or teacher or principal data.

VII. Reporting a Breach or Unauthorized Release

The School's Data Protection Officer will report every discovery or report of a breach or unauthorized release of data within the School to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the School will be required to promptly notify the School of any breach of security resulting in an unauthorized release of the data by the third-party contractor no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the School will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

IX. Annual Data Privacy and Security Training

The School will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

X. Adoption of Policy & Notification of Policy

This policy was adopted by the "The School" Board of Trustees on November 19, 2020. The policy will be published on the "The School" website.