Data Security and Privacy Policy

South Shore Charter Schools ("South Shore") believes that providing students with a secure and welcoming physical and virtual environment that enables a world-class education is essential to our mission. South Shore is committed to promoting best practices and policies that will strengthen data privacy and security at our schools and prepare all students to participate in a digital future.

Definitions

● **"Eligible student"** means a student eighteen years or older.

● **"Parent"** means a parent, legal guardian, or person in parental relation to a student.

● **"Student II"** means any person attending or seeking to enroll in a South Shore school.

● **"Building principal"** means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

● **"Student"** is personally identifiable information from a student's education record, including, but not limited to, the student's name, the name of the student's parent or other family members, the address of the student or student's family, a personal identifier, such as the student's social security number, student number, or biometric record, and other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.

● **"Teacher or Principal data"** means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that are confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.

● **"Student data"** means personally identifiable information from the student records of an educational agency.

● **"Release"** has the same meaning as disclosure or disclose.

● **"Disclose"** or **"disclosure"** means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

● **"Breach"** means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

● **"Unauthorized disclosure"** or **"unauthorized release"** means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

● **"Commercial or marketing purpose"** means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

● **"Contract or other written agreement"** means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

● **"Education records"** means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

● **"Educational agency"** means a school district, charter school, or the New York State Education Department (NYSED).

● **"Third-party contractor"** means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

● **"Encryption"** means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

● **"FERPA"** means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

● **"NIST Cybersecurity Framework"** means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

How Does South Shore Charter Schools Protect Student PII and Teacher and Principal Data?

South Shore protects Student PII and Teacher or Principal Data by:

● Utilizing the National Institute of Standards and Technology's Cybersecurity Framework v 1.1 (NIST Cybersecurity Framework) as the standard for its Data Privacy and Security Program.

● Not selling Student PII or Teacher or Principal Data nor using or disclosing it for any marketing or commercial purpose or facilitating its use or disclosure by any other party for any marketing or commercial purpose or permitting another party to do so.

● Taking steps to minimize its collection, processing and transmission of Student PII and Teacher or Principal Data.

● Requiring that third party contractors maintain the confidentiality of Student PII and Teacher or Principal Data in accordance with federal and state law and this Data Security and Privacy Policy.

● Ensuring that every use and disclosure of Student PII benefits Students and South Shore (*e.g.*, improves academic achievement, empowers Parents and Students with information, and/or advances efficient and effective school operations).

● Not including Student PII in public reports without permission by Parents. South Shore, at times, may share pictures, video, and/or newsletters that celebrate the South Shore community and Student achievements. Such media may contain Student names, images, or

information pertaining to a Student's achievement. Prior to sharing such information, South Shore staff ensure that appropriate consent has been obtained from the Parent or Eligible Student.

● Ensuring that only authorized individuals are able to review a Student's education records and ensuring that this review is conducted in a confidential manner that protects the records from unauthorized access. Records may be viewed by authorized individuals in person in the Main Office of the applicable South Shore school, or records may be delivered to authorized individuals by mail or by electronic transmission that is password protected and encrypted. School officials responsible for responding to requests for education records may only provide student education records to limited categories of individuals, including Parents and new schools of former Students, pursuant to written procedures. All other requests for education records are handled by legal counsel for South Shore to ensure compliance with the Family Educational Rights Privacy Act (FERPA) and New York Education Law § 2-d.

● Taking steps to verify the identity of Parents or Eligible Students who submit requests to inspect and review an education record, and complying with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

● Transmitting the records in a way that complies with applicable state and federal law and regulations, and employing safeguards associated with industry standards and best practices, such as encryption and password protection, when education records requested by a Parent or Eligible Student are electronically transmitted.

● Not reporting to the New York State Education Department ("NYSED"), except as required by law or in the case of educational enrollment data, the following student data elements: juvenile delinquency records; criminal records; medical and health records; and student biometric information.

How Do Third Party Contractors Protect Information?

Third party contractors who have access to Student PII or Teacher or Principal Data must refrain from disclosing Student PII or Teacher or Principal Data without the express written permission of South Shore Charter Schools, and refrain from using Student PII or Teacher or Principal Data on the contractor's own behalf or on behalf of anyone other than South Shore.

South Shore is committed to using this requirement as a selection criteria when choosing third party contractors. South Shore works with third party contractors to establish a data security and privacy plan and a contract that:

● Outlines how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements.

● Specifies the administrative, operational and technical safeguards and practices it has in place to protect Student PII and Teacher or Principal Data.

● Specifies how the third party's officers, employees, and assigns who have access to Student PII or Teacher or Principal Data will receive training on the laws governing confidentiality of such data.

● Requires subcontractors to protect Student PII and Teacher or Principal Data according to student privacy laws and South Shore's Data Security and Privacy Policy.

● Specifies how the third-party contractor will identify and manage breaches and unauthorized disclosures of Student PII or Teacher or Principal Data.

● Includes a requirement to notify South Shore of breaches and unauthorized disclosures of Student PII or Teacher or Principal Data and to pay for or promptly reimburse South Shore for the cost of notification of such breach to Parents, Eligible Students, teachers, and/or principals.

● Describes whether, how and when data will be returned to South Shore, transitioned to a successor contractor, or deleted or destroyed when the contract is terminated or expires.

● Includes a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

● States the exclusive purposes for which the Student PII or Teacher or Principal Data will be used.

● States if and how a Parent, Student, Eligible Student, teacher or principal may challenge the accuracy of the Student PII or Teacher or Principal Data that is collected.

● States where the Student PII or Teacher or Principal Data will be stored and how the data will be protected.

● Addresses how the data will be protected using encryption while in motion and at rest.

Third party contractors with access to Student PII or Teacher or Principal Data are obligated by New York Education Law § 2-d to:

● Adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework and maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Student PII or Teacher or Principal Data in its custody.

● Comply with this Data Security and Privacy Policy and federal and state student privacy laws.

● Limit internal access to Student PII or Teacher or Principal Data to only those employees or subcontractors that need access to provide the contracted services.

● Not use Student PII or Teacher or Principal Data for any purpose not explicitly authorized in its contract.

● Not disclose Student PII or Teacher or Principal Data to any other party without the prior written consent of the Parent or Eligible Student: (i) except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal laws; or (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to South Shore no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

● Use encryption to protect Student PII or Teacher or Principal Data in its custody while in motion or at rest.

● Not sell Student PII or Teacher or Principal Data 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.

Compliance with South Shore's Computer Policy and Usage Agreement

All officers and staff must comply with South Shore's Acceptable Use Policy when using Zea's resources. Access of privileges will be granted in accordance with the user's job responsibilities. Access of privileges will be limited to the extent necessary to accomplish assigned tasks in accordance with South Shore's mission and business functions. Access privileges will be discontinued for those who are no longer with South Shore.

Training for Employees

South Shore will annually provide data privacy and security awareness training to their officers and employees with access to Student PII or Teacher or Principal Data. Such training shall include but not be limited to training on the state and federal laws that protect Student PII and Teacher or Principal Data, and how employees can comply with such laws.

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 Chief Privacy Officer has the power, among others, to:

Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by South Shore that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and

Based upon a review of these records, require South Shore to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring South Shore to perform a privacy impact and security risk assessment.

Data Protection Officer

South Shore shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law § 2-d and to serve as the point of contact for data security and privacy for the educational agency. South Shore's Data Protection Officer shall have the appropriate knowledge, training, and experience to administer the functions described in Education Law § 2-d and its implementing regulations. The Data Protection Officer may perform these functions in addition to other job responsibilities.

Reports and Notifications of Breach and Unauthorized Release of Student PII or Teacher or Principal Data

South Shore shall:

● Report breaches or unauthorized releases of Student PII or Teacher or Principal Data to the NYSED Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery. "Breach" means the unauthorized acquisition, access, use, or disclosure of Student PII or Teacher or Principal Data by or to a person not

authorized to acquire, access, use, or receive the Student PII or Teacher or Principal Data. ● Notify affected Parents, Eligible Students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 days after the discovery or receipt of a report of a breach by a third-party contractor. Notification may be delayed if it would interfere with an ongoing investigation by law enforcement or would disclose an unfixed security vulnerability, and South Shore shall send notification within 7 days after the security vulnerability is fixed or the risk of interference with the law enforcement investigation ends.

Notifications required by this section shall:

● Be clear, concise, and use language that is plain and easy to understand.

● Include a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known, a description of the types of Student PII or Teacher or Principal Data affected, an estimate of the number of records affected, a brief description of the educational agency's investigation or plan to investigate, and contact information for representatives who can assist Parents or Eligible Students that have additional questions.

● Be sent to affected Parents, Eligible Students, teachers or principals by email, telephone, or first-class mail to the last known address.

Parents' Rights Under FERPA and Education Law § 2-d

Under the Family Educational Rights and Privacy Act ("FERPA"), Parents and Eligible Students have the rights set forth in South Shore 2024-25 FERPA and Directory Information Notice

Under New York state's education law, Parents have rights regarding the privacy and security of their child's Student PII, as set forth in the Parents' Bill of Rights for Data Privacy and Security

The Parents' Bill of Rights for Data Privacy and Security and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of South Shore's data and/or technology infrastructure.