DATA SECURITY AND PRIVACY

Objective:

The objective of the Sharon Springs CSD in the development and implementation of this Data Privacy Policy, is to be transparent with the community about the information we collect, how we use information, how we share information, how we protect information, how to contact us with questions, concerns or to report potential violations, and to comply with our obligations under all federal, state and local laws. Specifically, Ed-Law 2D.

Policy on Data Security and Privacy:

The Board of Education recognizes its responsibility to enact policies that provide privacy and security for student, teacher and principal data in accordance with law. This is particularly relevant in the context of the administration of student, teacher and principal data, which is collected, surveys that collect personal information, and the disclosure of personal information for marketing purposes and in conducting physical exam

Authority and Definitions:

Ed-Law 2D Terms and Conditions

a) "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.

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

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d) "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.

e) "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.

f) "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.

g) "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

h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) "Eligible student" means a student who is enrolled in the district

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology

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

l) "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.

m) "Parent" means a parent, legal guardian, or person in parental relation to a student

n) "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c (10).

o) "Release" has the same meaning as disclosure or disclose.

p) "Student" means any person attending or seeking to enroll in an educational agency

q) "Student data" means personally identifiable information from the student records of an educational agency

"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 is confidential and not subject to release under the provisions of Education Law Sections 3012-c and3012-d

r) "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 district 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.

s) "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

Parent and Student Rights Under State and Federal Law:

This Policy shall include all protections given to parents/persons in parental relationship and students pursuant all State and federal laws that protect student data, including but not limited to Board policies implementing the Family Educational Rights in Privacy Act and the Americans with Disabilities Act. Any reference to parent in this policy will include a parent and anyone in parent relationships.

Parents Bill of Rights:

The Superintendent, or designee, shall publish a Parents Bill of Rights in an appropriate location on the District's website which shall inform parents:

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, and the process for requesting such review;
3. State and federal laws protect the confidentiality of personally identifiable information, 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;

A complete list of all student data elements collected by New York State is available for public review on the State's website, including link to that information, or by writing to the address and individual designated by the State including the contact information; and

4. Parents have the right to have complaints about possible breaches of student data addressed, and the process for making such complaints. Complaints should be directed to the Data Protection Officer, with contact information

Use and Disclosure of Personally Identifiable Data:

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the District will take steps to minimize its collection, processing, and transmission of PII.

Data Protection Officer:

The School District has designated a School District employee to serve as the School District's Data Protection Officer. 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, as well as serving as the main point of contact for data privacy and security for the School District. The School District will provide training to the Data Protection Officer to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

District Data Privacy and Security Standards:

The District 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

Privacy and Security of Student Data:

The Board of Education is committed to protecting the privacy and security of each and every student's data. In accordance with law, the following shall govern parental rights concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents/guardians have the right to inspect and review the complete contents of their child's education record

3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.

4. A complete list of all student data elements collected by the State Education Department is available for public review at: http://www.nysed.gov/common/nysed/files/programs/student-

data-privacy/collected-dataelements.pdf, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents/guardians have the right to file complaints about possible breaches of student data. Parents/guardians may submit a complaint regarding a potential breach by the School District to the Superintendent of Schools or his/her designee. The School District shall promptly acknowledge any complaints received and commence an investigation into the complaint, while taking the necessary precautions to protect personally identifiable information. The School District shall provide a response detailing its findings from the investigation no more than sixty (60) days after receipt of the complaint. Complaints pertaining to the State Education Department or one of its third-party vendors should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.

7. If the District enters into a contract with a third party in which student, teacher, or principal data is shared with a third party, the School District will require the third party to provide evidence that it has adopted a data and security plan in accordance with Education Law, section 2-d and will post as supplemental information be appended to the Parents' Bill of Rights the following information:

    a. . the exclusive purposes for which the student data will be used;
    b. how SERVICE PROVIDER will ensure that subcontractors, persons or entities that SERVICE PROVIDER will share the student data with, if any, will abide by data protection and security requirements;
    c. that student data will be returned or destroyed upon expiration of the Agreement;
    d. if and how a parent, student, or eligible student may challenge the accuracy of the student data that is collected; and
    e. where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

8. . Parents may access the State Education Department's Parents' Bill of Rights at: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf

The School District will post a Parents' Bill of Rights in accordance with the requirements of Education Law

9. The School District will designate a Data Protection Officer on an annual basis who shall be responsible for the implementation of policies and procedures required by law and to serve as the point of contact for data security and privacy for the School District. The School District will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the School District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the School District's data and/or technology infrastructure. The School District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1

Annual Data Privacy and Security Training:

The Superintendent or designee shall ensure that annual data privacy and security awareness training is provided the District's 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. This training may be delivered using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce

Third Party Contractors:

Any and all contracts between the District and third-party contractors, under which a contractor will receive student data or teacher or principal data, shall include provisions requiring that the contractor maintain the confidentiality of shared student data or teacher or principal data in accordance with law, regulation, and District policy.

In addition, the District will ensure that the contract or written agreement includes a signed copy of the Parents Bill of Rights and the contractor's data privacy and security plan, in compliance with Part 121 of the Commissioner's regulations and that has been accepted by the District.

The District will publish on its website a supplement to the Bill of Rights for any contract or other written agreement it has entered with a third-party contractor that will receive PII from the District, The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

Agreements subject to this policy include any 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

Notification of Breach or Unauthorized Release:

The School District will notify affected parents, eligible students, teachers and/or principals of a breach or unauthorized release of information as set forth in Policy 8635, Information Security Breach and Notification.

Should there be a breach of the District's electronic data, which includes unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security confidentiality, or integrity of personal information maintained by the District, and does not include good faith acquisition of personal information by an employee or agent of the District for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure, the District shall provide the following notifications in addition to those required above, when it has been determined that there has been, or it is reasonably believed to have been a breach:

The District will notify the affected individual. Such notice shall be directly provided to the affected persons.