Attachment A – Parents' Bill of Rights for Data Security and Privacy

South Jefferson Central School District
Parents Bill of Rights for Data Privacy and Security

The South Jefferson Central School District, in order to comply with Education Law 2-C and 2-D of NY Education Law publishes this Parents' Bill of Rights for Data Privacy and Security.

New York Education Law Section 2-d and Part 121 of the Commissioner's regulations require school districts to ensure that all of their contracts or other written agreements with third-party contractors pursuant to which the third-party contractor receives Education Law Section 2-d protected district student data and/or teacher or principal data for purposes of providing services to the district, include certain provisions as specified within the statute and its implementing regulations. All third party contractors will receive and agree to comply with the Parent's Bills of Rights and Student Records Policy. The District will notify the Contractor of any significant changes to either policy,

Parents (includes legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by South Jefferson Central School. This right may not apply to parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls, and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security, and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to file complaints with the South Jefferson Central School about possible breaches and unauthorized disclosures by the District or third party contractors of PII. Complaints should be directed to the Data Privacy Security Officer, PO Box 10 Adams, NY, 13605 or by phone to 315 583-6104. Complaints may also be submitted to NYSED at www.nysed.gov/data-privacy-security; by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. South Jefferson Central School employees that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. South Jefferson Central School contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Supplemental Information About This Contract

For purposes of further ensuring confidentiality and security of student data — as well as the security of personally-identifiable teacher or principal data — the Parents' Bill of Rights (above) and the following supplemental information will be included in each contract that the South Jefferson Central School District enters into with a third-party contractor with access to this information:

CONTRACTOR	**<<Vendor Name>>**
PRODUCT	**<<Name of product>>**
PURPOSE DETAILS	The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT. The product or services are used to provide **<<Product purpose>>**
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Information with subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.
DATA DESTRUCTION INFORMATION	The agreement expires **<<Contract Expiration Date>>.** Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
DATA ACCURACY INFORMATION	In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Education Rights and Privacy Act.
SECURITY PRACTICES	The data is stored in the continental United States (CONUS) or Canada. Vendor will maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).