Data Security and Privacy Policy

In accordance with New York State Education Law § 2-d, South Jefferson CS District (District) hereby implements the requirements of Commissioner's regulations (8 NYCRR part 121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the District will benefit students and the District (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The District also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the District will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see policy # 7240 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the District will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The District will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR
300.610 through 300.627. The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR 121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this
policy.

References:
Education Law § 2-d
8 NYCRR Part 121
Family Educational Rights and Privacy Act of 1974, 20 USC § 1232(g)), 34 Code of Federal Regulations (CFR) Part 99
Individuals with Disabilities Education Act (IDEA), 20 USC § 1400 et seq., 34 CFR 300.610–300.627

SOUTH JEFFERSON CENTRAL SCHOOL DISTRICT

District Office
PO Box 10
Adams, NY 13605
(315) 583-6104

CONTRACT ADDENDUM
Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The South Jefferson Central School District ("DISTRICT") and [Vendor Name] ("Vendor") are parties to a contract dated [Insert date here] ("the underlying contract") governing the terms under which DISTRICT accesses, and Vendor provides, [name of product(s) covered by contract] ("Product"). DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1 "Protected Information", 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 (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.

2.2 "Vendor" means name of vendor identified above.

2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.

2.4 "DISTRICT" means the South Jefferson Central School District.

2.5 "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6 "Student" means any person attending or seeking to enroll in an educational agency.

2.7 "Eligible Student" means a student eighteen years or older.

2.8 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9 "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the DISTRICT Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Purpose for Sharing Protected Information

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.

8. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Informationwith such entities if those entities 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.

9. Protected Information and Contract Termination

9.1 The expiration date of this Contract is defined by the underlying contract.

9.2 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.

9.3 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.

9.4 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.

9.5 To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

9.6 Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

10. Data Subject Request to Amend Protected Information

10.1 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 Educational Rights and Privacy Act (FERPA).

10.2 Vendor will cooperate with DISTRICT in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

11. Vendor Data Security and Privacy Plan

11.1 Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

11.2 Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

a. align with the NIST Cybersecurity Framework 1.0;

b. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

c. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy (Attachment B);

d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

e. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

f. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

g. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

h. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and

i. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

12. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

12.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

12.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

12.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the DISTRICT unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

12.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

12.5 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);

12.6 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

12.7 Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

For South Jefferson Central School District

For [Vendor Name]

_____

_____

President of the Board of Education

Date:_____

Date:_____

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 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	[Product Name]
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 [insert here]
SUBCONTRACTOR DETAILS	Vendor represents that it will only share Protected Informationwith 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 [insert here]. 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).

For South Jefferson Central School District

_____

Scott Slater, Superintendent

Date:_____

For [Vendor Name]

_____

Date:_____

Attachment B – South Jefferson Central School District Data Security and Privacy Policy

In accordance with New York State Education Law § 2-d, the District hereby implements the requirements of Commissioner's regulations (8 NYCRR part 121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the District will benefit students and the District (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The District also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the District will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see South Jefferson Central School Policy 7240 -Student Records and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the District will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The District will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR 121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

References:

Education Law § 2-d
8 NYCRR Part 121
Family Educational Rights and Privacy Act of 1974, 20 USC § 1232(g)), 34 Code of Federal Regulations (CFR) Part 99
Individuals with Disabilities Education Act (IDEA), 20 USC § 1400 et seq., 34 CFR 300.610–300.627

Attachment C – Vendor's Data Security and Privacy Plan

The DISTRICT Parents Bill of Rights for Data Privacy Security, a signed copy of which is included as Attachment B to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

[INSERT Links or Text, as provided by the Vendor]