



WAYNE - FINGER LAKES

Board of Cooperative Educational Services

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES and Voiceitt, Inc. ("Vendor") are parties to a contract dated (the underlying contract) governing the terms under which BOCES accesses, and Vendor provides, Assistive Technology(AT) and Aug ("Product"). Wayne-Finger Lakes BOCES 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 BOCES or is created by the Vendor's product or service in the course of being used by BOCES.
- 2.2. "Vendor" means Voiceitt, Inc.
- 2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES.
- 2.4. "BOCES" means the Wayne-Finger Lakes BOCES.
- 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 BOCES 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 BOCES 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. Ownership and Location of Protected Information

- 7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.
- 7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.
- 7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.
- 7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. 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 Wayne-Finger Lakes BOCES.

9. 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 Information with 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.



10. Protected Information and Contract Termination

- 10.1. The expiration date of this Contract is defined by the underlying contract.
- 10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.
- 10.3. 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.
- 10.4. 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 afore mentioned secure data center facilities.
- 10.5. 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.
- 10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

- 11.1. 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 BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).
- 11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

- 12.1. 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.
- 12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:
- 12.3. Align with the NIST Cybersecurity Framework 1.0;
- 12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;
- 12.5. 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 BOCES data security and privacy policy (Attachment B);
- 12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;
- 12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
- 12.8. 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.



- 12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected.
- 12.10. 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 BOCES; and
- 12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. 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:

- 13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;
- 13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;
- 13.3 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 BOCES 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 BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- 13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
- 13.5 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);
- 13.6 Vendor will notify the BOCES 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

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




Signatures

For Wayne-Finger Lakes BOCES



Date

For Voiceitt, Inc.

DocuSigned by:

_____ 22E8B63661B3406...

Date 6/10/2025



Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

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. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
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.
4. A complete list of all student data elements collected by the State is available at <http://www.nysed.gov/data-privacy-security/student-data-inventory> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

A handwritten signature in black ink, appearing to read "William Allen", written over the "Signatures" label.

For Wayne-Finger Lakes BOCES

Date

A handwritten date "6/17/25" in black ink, written over the "Date" label.

For Voiceitt, Inc.

DocuSigned by:
A handwritten signature in black ink, appearing to read "Mike Duncan", written over the "DocuSigned by:" label.
22E8B63661B3406...
Date 6/10/2025

Attachment B – Wayne-Finger Lakes BOCES Data Privacy and Security Policy

P5262 PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND SUPERVISORY DATA

The Wayne-Finger Lakes (W-FL) BOCES is committed to maintaining the privacy and security of student data and teacher and supervisory data and will follow all applicable laws and regulations for the handling and storage of this data in W-FL BOCES and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The W-FL BOCES adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the W-FL BOCES data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

- a. "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or supervisory data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or supervisory data.
- b. "Supervisory" means a supervisor subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.
- c. "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 eighteen years or older.
- j. "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).

- 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 supervisory 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.
- r. "Teacher or supervisory data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of teachers or supervisors that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.
- s. "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or supervisory 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 supervisory data from W-FL BOCES to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, or a not-for-profit corporation or other nonprofit organizations, other than an educational agency.
- t. "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.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and supervisory data, the W-FL BOCES will take steps to minimize its collection, processing, and transmission of PII. Additionally, the W-FL BOCES 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 supervisory data be maintained in accordance with law, regulation, and W-FL BOCES policy.
- c. Except as required by law or in the case of educational enrollment data, the W-FL BOCES will not report to NYSED the following student data elements:

- a. Juvenile delinquency records;
- b. Criminal records;
- c. Medical and health records; and
- d. Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or supervisory data by a person acting exclusively in the person's capacity as an employee of the W-FL BOCES.

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 supervisory 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 supervisory data.

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

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

- a. Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the W-FL BOCES that relate to student data or teacher or supervisory 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
- b. Based upon a review of these records, require the W-FL BOCES to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the W-FL BOCES to perform a privacy impact and security risk assessment.

Data Protection Officer

The W-FL BOCES will designate an employee to serve as the W-FL BOCES' Data Protection Officer at the Annual Reorganizational Meeting or by Board resolution during the school year, if necessary.

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 W-FL BOCES.

The W-FL BOCES 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

W-FL BOCES Data Privacy and Security Standards

The W-FL BOCES 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 Framework provides a common taxonomy and mechanism for organizations to:

- a. Describe their current cybersecurity posture;
- b. Describe their target state for cybersecurity;
- c. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- d. Assess progress toward the target state; and
- e. Communicate among internal and external stakeholders about cybersecurity risk.

The W-FL BOCES will protect the privacy of PII by:

- a. Ensuring that every use and disclosure of PII by the W-FL BOCES benefits students and the W-FL BOCES by considering, among other criteria, whether the use and/or disclosure will:
- b. Improve academic achievement;
- c. Empower parents and students with information; and/or
- d. Advance efficient and effective W-FL BOCES operations.
- e. Not including PII in public reports or other public documents.

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

Third-Party Contractors

W-FL BOCES Responsibilities

The W-FL BOCES will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or supervisory data from the W-FL BOCES, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or supervisory data be maintained in accordance with law, regulation, and W-FL BOCES policy.

In addition, the W-FL BOCES will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the W-FL BOCES.

The third-party contractor's data privacy and security plan must, at a minimum:

- a. Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with W-FL BOCES policy;
- b. Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;
- c. Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);
- d. Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or supervisory data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;
- e. Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;
- f. Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the W-FL BOCES;
- g. Describe whether, how, and when data will be returned to the W-FL BOCES, transitioned to a successor contractor, at the W-FL BOCES's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and
- h. 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 W-FL BOCES under which the third-party contractor will receive student data or teacher or supervisory data from the W-FL BOCES, is required to:

- a. Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;
- b. Comply with W-FL BOCES policy and Education Law Section 2-d and its implementing regulations;
- c. Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);
- d. Not use the PII for any purpose not explicitly authorized in its contract;
- e. Not disclose any PII to any other party without the prior written consent of the parent or eligible student:
 - a. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the W-FL BOCES; or
 - b. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the BOE, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

- f. Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;
- g. Use encryption to protect PII in its custody while in motion or at rest; and
- h. 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.
- i. Ensure that where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Cooperative Educational Services through another BOCES

The W-FL BOCES may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or supervisory data from the W-FL BOCES under all circumstances.

For example, the W-FL BOCES may not need its own contract or agreement where:

- a. It has entered into a cooperative educational service agreement (CoSer) with another BOCES that includes use of a third-party contractor's product or service; and
- b. That other BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the W-FL BOCES's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or supervisory data from the W-FL BOCES is received by a third-party contractor pursuant to a CoSer, the W-FL BOCES will consult with the other BOCES to, among other things:

- a. Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the W-FL BOCES's use of a third-party contractor's product or service under a particular CoSer;
- b. Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that another BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;
- c. Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or supervisors about any breach or unauthorized release of PII that a third-party contractor has received from the W-FL BOCES pursuant to another BOCES contract; and
- d. Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the W-FL BOCES receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the W-FL BOCES pursuant to another BOCES contract.

Click-Wrap Agreements

Periodically, W-FL BOCES staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

W-FL BOCES staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or supervisory data from the W-FL BOCES unless they have received prior approval from the W-FL BOCES's Data Privacy Officer or designee.

The W-FL BOCES will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

The W-FL BOCES will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the W-FL BOCES will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or supervisory data from the W-FL BOCES.

The Bill of Rights will contain all required elements including supplemental information for each contract the W-FL BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or supervisory data from the W-FL BOCES. The supplemental information must be developed by the W-FL BOCES and include the following information:

- a. The exclusive purposes for which the student data or teacher or supervisory data will be used by the third-party contractor, as defined in the contract;
- b. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or supervisory data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
- c. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or supervisory data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the W-FL BOCES, and/or whether, when, and how the data will be destroyed);
- d. If and how a parent, student, eligible student, teacher, or supervisor may challenge the accuracy of the student data or teacher or supervisory data that is collected;
- e. Where the student data or teacher or supervisory data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
- f. Address how the data will be protected using encryption while in motion and at rest.

The W-FL BOCES 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 W-FL BOCES. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the W-FL BOCES's data and/or technology infrastructure.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the W-FL BOCES under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the W-FL BOCES in a manner prescribed by the W-FL BOCES.

The W-FL BOCES will ensure that only authorized individuals are able to inspect and review student data. To that end, the W-FL BOCES will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the W-FL BOCES and not to a third-party contractor. The W-FL BOCES may require that requests to inspect and review education records be made in writing.

The W-FL BOCES will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the W-FL BOCES through its annual FERPA notice. A notice separate from the W-FL BOCES's annual FERPA notice is not required.

The W-FL BOCES will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The W-FL BOCES may provide the records to a parent or eligible student electronically as long as the parent consents. The W-FL BOCES must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Supervisory Data

The W-FL BOCES will inform parents, 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 W-FL BOCES has established the following procedures for parents, eligible students, teachers, supervisors, and other W-FL BOCES staff to file complaints with the W-FL BOCES about breaches or unauthorized releases of student data and/or teacher or supervisory data:

- a. All complaints must be submitted to the W-FL BOCES's Data Protection Officer in writing.
- b. Upon receipt of a complaint, the W-FL BOCES will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.
- c. Following the investigation of a submitted complaint, the W-FL BOCES will provide the individual who filed the

complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the W-FL BOCES.

- d. If the W-FL BOCES requires additional time, or where the response may compromise security or impede a law enforcement investigation, the W-FL BOCES will provide the individual who filed the complaint with a written explanation that includes the approximate date when the W-FL BOCES anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, supervisors, and other W-FL BOCES staff.

The W-FL BOCES 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.

Reporting a Breach or Unauthorized Release

The W-FL BOCES will report every discovery or report of a breach or unauthorized release of student data or teacher or supervisory data within the W-FL BOCES 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 supervisory data pursuant to a contract or other written agreement entered into with the W-FL BOCES will be required to promptly notify the W-FL BOCES of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, W-FL BOCES policy, and/or binding 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.

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

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or supervisory data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the W-FL BOCES and law enforcement to protect the integrity of

investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or supervisory data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, W-FL BOCES policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than 30 days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

- a. Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years;
- b. Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or supervisory data be precluded from accessing student data or teacher or supervisory data from any educational agency in the state for a fixed period of up to five years;
- c. Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or supervisory data will not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or supervisory data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or
- d. Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or supervisory data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or supervisory data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

The W-FL BOCES will notify affected parents, eligible students, teachers, and/or supervisors in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the W-FL BOCES or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the W-FL BOCES will notify parents, eligible students, teachers, and/or supervisors within seven calendar

days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a. A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;
- b. A description of the types of PII affected;
- c. An estimate of the number of records affected;
- d. A brief description of the W-FL BOCES's investigation or plan to investigate; and
- e. Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or supervisor by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the W-FL BOCES for the full cost of this notification.

Annual Data Privacy and Security Training

The W-FL BOCES 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. The W-FL BOCES may deliver this training using online training tools. Additionally, this training may be included as part of the training that the W-FL BOCES already offers to its workforce.

Notification of Policy

The W-FL BOCES will publish this policy and provide notice of the policy to all its officers and staff.

Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627



Attachment C – Vendor’s Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attach)

