



New Hartford Central Schools

Information Technology Department

33 Oxford Road, New Hartford, NY 13413

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The New Hartford Central School District (“DISTRICT”) and Curiosity Media, Inc., ABCya.com, LLC (“Vendor”) are parties to a contract dated January 21, 2025 (“the underlying contract”) governing the terms under which DISTRICT accesses, and Vendor provides ABCya (“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 Curiosity Media, Inc., ABCya.com, LLC
- 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 New Hartford 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. Ownership and Location of Protected Information

7.1 Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2 DISTRICT shall have access to the DISTRICT's Protected Information at all times through the term of this Contract. DISTRICT 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 DISTRICT or its authorized users, or performing any other data analytics other than those required to provide the Product to DISTRICT. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to DISTRICT 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 DISTRICT.

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 DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT.
- 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 aforementioned 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 DISTRICT 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 DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).
- 11.2 Vendor will cooperate with DISTRICT 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:
 - 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.

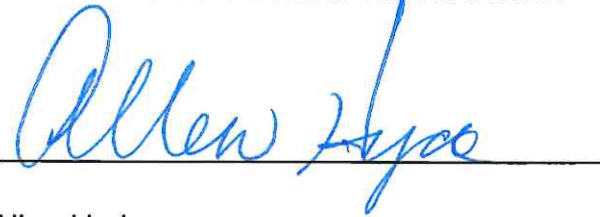
13. Additional Vendor Responsibilities

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 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;

- 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 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
- 13.7 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 New Hartford Central School District



Allen Hyde
Assistant Superintendent

Date:

For Curiosity Media, Inc., ABCya.com, LLC



Paul Mishkin
Chief Executive Officer

Date: January 21, 2025

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

New Hartford Central School District Parents Bill of Rights for Data Privacy and Security

The New Hartford Central School District seeks to use current technology, including electronic storage, retrieval, and analysis of information about students’ education experience in the district, to enhance the opportunities for learning and to increase the efficiency of our district and school operations.

The New Hartford Central School District seeks to insure that parents have information about how the District 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 § 2-d of the New York State Education Law. To further these goals, the New Hartford Central School District 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 Policies 7240, 7242, and 7250. You may access these Policies from the District’s website.
- 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 will be available at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> 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, NY 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the John Gillette, Chief Information and Technology Officer, New Hartford Central Schools, 33 Oxford Rd. New Hartford, NY 13413 OR to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

Supplemental Information about Third Party Contracts

In order to meet 21st century expectations for effective education and efficient operation, the District utilizes several products and services that involve third party contractors receiving access to student data, or principal or teacher data, protected by Section 2-d of the Education Law. The District recognizes that students, parents, and the school community have a legitimate interest in understanding which of the District’s vendors receive that data, for what purpose, and under what conditions. The District has undertaken the task of compiling the information, and of insuring that each new contract adequately describes

- (1) the exclusive purposes for which the data will be used,
- (2) how the contractor will ensure that any subcontractors it uses will abide by data protection and security requirements,
- (3) when the contract expires and what happens to the data at that time,
- (4) if and how an affected party can challenge the accuracy of the data as collected,
- (5) where the data will be stored, and
- (6) the security protections taken to ensure the data will be protected, including whether the data will be encrypted.

For New Hartford Central School District

For Curiosity Media, Inc., ABCya.com, LLC




Allen Hyde
Assistant Superintendent

Paul Mishkin
Chief Executive Officer

Date:

Date: January 21, 2025

Supplemental Information About This Contract

CONTRACTOR	Curiosity Media, Inc., ABCya.com, LLC
PRODUCT	ABCya
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 [e.g. Science instruction in Grades 1 - 3] .
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 January 21, 2026 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).

SUPPORT OPERATIONS

5301

PROTECTION OF STUDENT, TEACHER, AND PRINCIPAL PERSONAL INFORMATION (DATA SECURITY AND PRIVACY)

I. Statement of Policy

In order to conduct a successful education program, the New Hartford Central School District receives, creates, stores, and transfers information about students, teachers, and principals that is protected by state and federal law. The District takes active steps to protect the confidentiality of protected information in compliance with all applicable state and federal laws. The District expects all District officers, employees, and partners to maintain the confidentiality of protected information in accordance with state and federal law and all applicable Board Policies.

This Policy shall be published on the District website. II. Scope

of Policy

A. Protected Information

1. The term Protected Information used in this Policy includes both, Protected Student Information, and Protected Teacher and Principal Information that is recorded in any form, including paper or digital, and text or image or sound.
2. The term Protected Student Information means personally identifiable information as defined in the federal regulations implementing the Family Educational Rights and Privacy Act (FERPA), found at 34 C.F.R. Section 99.3.
3. The term Protected Teacher and Principal Information means personally identifiable information about an individual's Annual Professional Performance Review (APPR) rating, as described in Education Law Section 3012-c(10).

B. Affected Persons and Entities

1. The term Student includes any person attending school in an educational agency, or seeking to become enrolled in an educational agency.
2. The term Parent includes the parent, legal guardian, or person in parental relation to a Student.
3. The term Data Subject includes any Student and the Parent of the Student, and any teacher or principal who is identified in Protected Information held by the District.

4. As used in this Policy, the term Third Party means any person or organization that (a) is not employed by this District and is not an Educational Agency and (b) receives Protected Information from this District. The term Third Party includes for-profit organizations, not-for-profit organizations, higher education institutions, and governmental agencies that are not Educational Agencies (such as law enforcement agencies).
5. As used in this Policy, the term Educational Agency includes public school districts, boards of cooperative educational services, charter schools, the State Education Department, certain pre-k programs, and special schools described in Section 2-d of the Education Law; higher education institutions are not Educational Agencies for purposes of this Policy. C. Other

Important Definitions

1. The term Breach means the unauthorized acquisition of, access to, use of, or disclosure of Protected Information by or to a person who is not authorized to acquire, access, use, or receive that Protected Information.
2. A Disclosure of Protected Information occurs when that information is released, transferred, or otherwise communicated to an unauthorized party by any means, including oral, written, or electronic; a disclosure occurs whether the exposure of the information was intentional or unintentional. A Disclosure is Unauthorized if it is not permitted by state or federal law or regulation, or by any lawful contract, or not made in response to a lawful order of a court or tribunal.
3. The term Commercial or Marketing Purpose means (a) the sale of Protected Student Information, (b) the use or disclosure of Protected Student Information by any party (including the District) for purposes of receiving remuneration, either directly or indirectly, (c) the use of Protected Student Information for advertising purposes, (d) the use of Protected Student Information to develop or improve a Third Party product or service, or (e) the use of Protected Student Information to market products or services to students.

D. Implementation with Other Policies and Laws

The District has adopted other Policies and practices to comply with state and federal laws such as FERPA, IDEA, and the National School Lunch Act. This Policy will be implemented to supplement, and not replace, the protections provided by those laws, as recognized in District Policies and practices.

III. General Principles for Use and Security of Protected Information

A. Intentional Use of Protected Information

1. All District staff and officers are expected to receive, create, store, and transfer the minimum amount of Protected Information necessary for the District to implement its education program and to conduct operations efficiently. In particular, the number of email documents containing Protected Information should be minimized.

2. Protected Student Information will only be disclosed to other District staff or Third Parties when that person or entity can properly be classified as a school official with a legitimate educational interest in that Protected Information, meaning that the person or entity requires that information to perform their job or fulfill obligations under a contract with the District.
3. Protected Information shall not be disclosed in public reports or other public documents.
4. Before Protected Student Information is disclosed to a Third Party, there shall be a determination that the disclosure of the Protected Information to that Third Party will benefit the student(s) whose information is being disclosed and the District.
5. Except as required by law or in the case of educational enrollment data, the District shall not report to the State Education Department student juvenile delinquency records, student criminal records, student medical and health records, or student biometric information.

B. Commercial and Marketing Use of Protected Information Prohibited

The District shall not sell protected information or use or disclose protected information for the purpose of receiving remuneration either directly or indirectly.

The District shall not facilitate the use of Protected Information by another party for that party's commercial or marketing purpose.

IV. Data Protection Officer

A. Board Designation

Upon the recommendation of the Superintendent, the Board will designate a Data Protection Officer. The designation shall be made by formal action at a Board meeting.

B. Responsibilities of Data Protection Officer

1. The Data Protection Officer shall be responsible for the implementation of this Policy, under the supervision of the Superintendent and consistent with other Board Policies.
2. The Data Protection Officer shall serve as the initial point of contact for data security and privacy matters affecting the District, including communications with the Chief Privacy Officer of the State Education Department.
3. In addition to specific responsibilities identified in this Policy, the Data Protection Officer shall oversee the District assessment of its risk profile and assist the Superintendent in identifying appropriate steps to decrease the risk of Breach or Unauthorized Disclosure of Protected Information, in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

V. Actions to Reduce Cybersecurity Risk

A. NIST Cybersecurity Framework

1. The District shall plan, install, maintain, operate, and upgrade its digital information network systems, infrastructure, and practices in alignment with the NIST Cybersecurity Framework, version 1.0, with the goal of steadily reducing the risk of unauthorized disclosure of, or access to, the Protected Information stored on and transmitted through the network.
2. In accordance with the approach of the NIST Cybersecurity Framework, the Superintendent shall direct appropriate District personnel, including the Data Protection Officer, to continually assess the current cybersecurity risk level of the District, identify and prioritize appropriate “next steps” for the District to take to reduce cybersecurity risk, and implement actions to reduce that risk, consistent with available fiscal and personnel resources of the District.
3. Decisions regarding procurement and implementation of hardware and software, and decisions regarding the collection and use of Protected Information, shall take into consideration the anticipated benefit to the education program or operations of the District, and the potential increase or decrease in the risk that Protected Information will be exposed to unauthorized disclosure.

B. Setting Expectations for Officers and Employees

1. Notice of this Policy shall be given to all officers and employees of the District.
2. Officers and employees of the District shall receive cybersecurity training designed to help them identify and reduce the risk of unauthorized disclosures of Protected Information. Each employee shall receive such training at least annually. This training shall include information about the state and federal laws that govern Protected Information and how to comply with those laws and meet District expectations for use and management of Protected Information.

VI. Parents Bill of Rights for Data Privacy and Security

A. Content of the Parents Bill of Rights for Data Privacy and Security

The District publishes on its website and will maintain a Parents Bill of Rights for Data Privacy and Security that includes all elements required by the Commissioner’s Regulations, including supplemental information about data-sharing agreements as described in Part B below.

B. Public Access to the Parents Bill of Rights for Data Privacy and Security.

The Parents Bill of Rights for Data Privacy and Security shall be posted on the District website. The website copy of the Parents Bill of Rights for Data Privacy and Security shall include links to the following supplemental information about each contract between the District and a Third Party that receives Protected Information:

1. The exclusive purposes(s) for which the District is sharing the Protected Information with the Third Party;

2. How the Third Party will ensure that any other entities with which it shares the Protected Information, if any, will comply with the data protection and security provisions of law and the contract;
3. When the agreement expires and what happens to the Protected Information when the agreement expires;
4. That a Data Subject may challenge the accuracy of the Protected Information through the process for amending education records under the Education Records Policy of the District (Protected Student Information) or the appeal process under the APPR Plan of the District (Protected Teacher and Principal Information);
5. Where the Protected Information will be stored (described in a way that protects data security); and
6. The security protections that will be taken by the Third Party to ensure that the Protected Information will be protected, including whether the data will be encrypted.

VII. Standards for Sharing Protected Information with Third Parties

A. Written Agreement For Sharing Protected Information With a Third Party Required

1. Protected Information shall not be shared with a Third Party without a written agreement that complies with this Policy and Section 2-d of the Education Law.
2. Disclosing Protected Information to other educational agencies does not require a specific written agreement, because educational agencies are not Third Parties. However, any such sharing must comply with FERPA and Board Policy.
3. When the District uses a cooperative educational services agreement (CoSer) with a BOCES (the CoSer BOCES) to access an educational technology platform that will result in Protected Information from this District being received by a Third Party, this District will confirm that the product is covered by a contract between the CoSer BOCES and the Third Party that complies with Education Law Section 2-d. This District will confirm with the CoSer BOCES the respective responsibilities of this District and the CoSer BOCES for providing breach notifications and publishing supplemental information about the contract.

B. Review and Approval of Online Products and Services Required

1. District staff do not have authority to bind the District to the Terms of Use connected to the use of online software products, regardless of whether there is a price attached to the use of the online product. Any staff member considering the use of an online product to perform the duties of their position should carefully read the online Terms of Service to determine whether accepting those terms will be considered binding on the District by the vendor.

2. If the use of an online product will result in the vendor receiving Protected Information, then the vendor is a Third Party and any agreement to use the online product must meet the requirements of this Policy and Education Law Section 2-d. Therefore, no staff member may use an online product that shares Protected Information until use of that product has been reviewed and approved by the Data Protection Officer.
3. The Superintendent, in consultation with the Data Protection Officer, shall establish a process for the review and approval of online technology products proposed for use by instructional or non-instructional staff.

C. Minimum Required Content for Third Party Contracts

1. Protected Information may not be shared with a Third Party unless there is a written, properly authorized contract or other data-sharing agreement that obligates the Third Party to:
 - a. maintain the confidentiality of the Protected Information in accordance with all applicable state and federal laws;
 - b. maintain the confidentiality of the Protected Information in accordance with this Policy;
 - c. use the shared Protected Information only for the purpose(s) specifically described in the contract, and to not use the Protected Information for any Commercial or Marketing Purpose;
 - d. limit access to Protected Information to only those officers and employees who need access in order to perform their duties in fulfilling the contract on behalf of the Third Party;
 - e. ensure that no officer or employee of the Third Party will be given access to Protected Information until they have received training in the confidentiality requirements of state and federal laws and this Policy;
 - f. not disclose any Protected Information to any other party who is not an authorized representative of the Third Party using the information to carry out Third Party's obligations under the contract, unless (i) Third Party has the prior written consent of the Data Subject 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 the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
 - g. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
 - h. 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);

- i. notify the District of any breach of security resulting in an unauthorized release of Protected Information by the Third Party or its assignees in violation of state or federal law, or in violation 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
 - j. where a breach or unauthorized disclosure of Protected Information is attributed to the Third Party, the Third Party shall pay for or promptly reimburse the District for the full cost incurred by this District to send notifications required by the Education Law.
2. The contract or other data-sharing agreement with the Third Party must include the Third Party's Data Security and Privacy Plan that is accepted by the District. The Plan must include a signed copy of the District Parents Bill of Rights for Data Privacy and Security, and shall:
 - a. warrant that the Third Party's practices for cybersecurity 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 Third Party will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with this Policy;
 - d. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under the contract;
 - e. demonstrate that it complies with the requirements of Section 121.3(c) of the Commissioner's Regulations;
 - f. specify how officers or employees of the Third Party 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 Third Party will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;
 - h. specify how the Third Party 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 the District; and
 - i. describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Third Party when the contract is terminated or expires.

3. The contract or other data-sharing agreement with the Third Party must also include information sufficient for the District to publish the supplemental information about the agreement described in Part VI-B of this Policy.

VIII. District Response to Reported Breaches and Unauthorized Disclosures

A. Local Reports of Possible Breach or Unauthorized Disclosures

1. Data Subjects and other District staff who have information indicating that there has been a Breach or Unauthorized Disclosure of Protected Information may report that information to the Data Protection Officer.
2. The report of suspected Breach or Unauthorized Disclosure must be made in writing. A report received by email will be considered a written report. The report shall provide as much information as is available to the reporting party concerning what Protected Information may have been compromised, when and how the possible Breach or Unauthorized Disclosure was discovered, and how the Data Privacy Officer may contact the reporting party. The Data Protection Officer shall make a form available online and in each school office to be used for reporting a suspected Breach or Unauthorized Disclosure.
3. The Data Protection Officer, or designee, shall take the following steps after receiving a report of a possible Breach or Unauthorized Disclosure of Protected Information:
 - a. promptly acknowledge receipt of the report;
 - b. determine, in consultation with appropriate technical staff, what, if any, technology-based steps should be taken immediately to secure against further compromise of Protected Information;
 - c. conduct a thorough fact-finding to determine whether there has been a Breach or Unauthorized Disclosure of Protected Information, and, if so, the scope of the Breach or Unauthorized Disclosure and how it occurred;
 - d. if a Breach or Unauthorized Disclosure of Protected Information is found to have occurred, implement the Cybersecurity Incident Response Plan to correct and ameliorate the Breach or Unauthorized Disclosure and provide appropriate notifications to the SED Chief Privacy Officer and affected Data Subjects; and
 - e. when the fact-finding process is complete, provide the reporting party with the findings made at the conclusion of the fact-finding process; this should occur no later than 60 days after the receipt of the initial report, and, if additional time is needed, the reporting party shall be given a written explanation within the 60 days that includes the approximate date when the findings will be available.
4. The Data Protection Officer shall maintain a record of each report received of a possible Breach or Unauthorized Disclosure, the steps taken to investigate the report, and the findings resulting from the investigation in accordance with applicable record retention policies, including Retention and Disposition Schedule for New York Local Government Records (LGS-1).

5. When this reporting and fact-finding process results in confirmation of a Breach or Unauthorized Disclosure of Protected Information, the Data Protection Officer, or designee, shall follow the notification procedures described in Part VIII. B., below.
6. The availability of this process for reporting suspected Breaches or Unauthorized Disclosures of Protected Information shall be communicated to all staff and all student households, in addition to the general posting of this Policy on the District website.

B. Notification of Breach or Unauthorized Disclosure of Protected Information

1. Third Parties who learn of the Breach or Unauthorized Disclosure of Protected Information received from the District are required by law to notify the District of that occurrence no more than seven days after their discovery of the Breach or Unauthorized Disclosure. When the District receives such a notification, the Data Protection Officer, or designee, shall promptly obtain from the Third Party the following information if it is not already included in the notice:
 - a. a brief description of the Breach or Unauthorized Disclosure;
 - b. the dates of the incident;
 - c. the dates of the discovery by the Third Party;
 - d. the types of Protected Information affected; and
 - e. an estimate of the number of records affected.
2. When the District is notified by a Third Party of a Breach or Unauthorized Disclosure of Protected Information in the custody of the Third Party, the Data Protection Officer shall notify the Chief Privacy Officer of the State Education Department of that information within ten calendar days of receiving it from the Third Party, using the form provided by the Chief Privacy Officer.
3. When the District learns of an Unauthorized Disclosure of Protected Information originating within the District, whether as the result of a report made under this Policy or otherwise, the Data Protection Officer shall notify the Chief Privacy Officer of the State Education Department of that information within ten calendar days of discovering the Unauthorized Disclosure, using the form provided by the Chief Privacy Officer.
4. When the District has received notification from a Third Party of a Breach or Unauthorized Disclosure of Protected Information, or has otherwise confirmed that a Breach or Unauthorized Disclosure of Protected Information has occurred, the District shall notify all affected Data Subjects by first class mail to their last known address, by email, or by telephone, of the Breach or Unauthorized Disclosure. Notifications by email shall be copied into the record of the incident. Logs of telephone notifications shall be maintained with each record signed by the District employee making the contact. Each notification shall include the following information:

- a. each element of information described in paragraph 1 above,
 - b. a brief description of the District investigation of the incident or plan to investigate; and
 - c. contact information for the Data Protection Officer as a point of contact for any questions the Data Subject may have.
5. The notification of affected Data Subjects shall be made in the most expedient way possible and without unreasonable delay, but no later than 60 calendar days after the discovery of the Breach or Unauthorized Disclosure or the receipt of the notice from the Third Party. If notification within the 60 day period would interfere with an ongoing law enforcement investigation or would risk further disclosure of Protected Information by disclosing an unfixed security vulnerability, notification may be delayed until no later than seven calendar days after the risk of interfering with the investigation ends or the security vulnerability is fixed.
 6. Where notification of affected Data Subjects is required because of a Breach or Unauthorized Disclosure attributed to a Third Party, the Data Protection Officer shall prepare and submit to the Third Party a claim for reimbursement, as provided in Section 2-d of the Education Law.
 7. Where notification of affected Data Subjects is required because of a Breach or Unauthorized Disclosure of Protected Information under this Policy, the Data Protection Officer shall also determine whether the District is required to provide any notifications pursuant to the Information Security Breach policy.

New

Hartford Central School District

Legal Ref: NYS Education Law Section 2-d; Family Educational Rights and Privacy Act
FERPA 20 U.S.C. 1232g

Cross Ref: 6600, Education Records
5300, Information Security Breach

Adopted: 03/30/21

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 A to this Addendum, is incorporated into and made a part of this Data Security and Privacy Plan.

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY

PLAN **CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN**

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Contractor will implement applicable state, federal and local data security and privacy contract requirements over the life of the Contract and only use PII in accordance with the Contract and applicable laws pertaining to data privacy and security, including Education Law § 2-d.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor employs automated log collection and audit trails for production Systems. – Connections originating from untrusted network segments will be governed by firewall rules and other security safeguards that grant the minimal access required to access the intended service provided by the company. – System passwords and access keys are stored in a privileged location accessible only to security administrators, and all credentials are changed from factory default settings. – Production systems receive regular maintenance to apply security patches. – Physical access to systems requires security RFID badges and biometric authentication, and is limited to IT staff performing physical maintenance.

3	Address the training received by your employees and any subcontractors engaged in the provision of services under the	Contractor shall ensure that all its employees, officers and subcontractors who have access to PII have received or will receive training on the federal and
---	---	--

Page 12 of 18

	Contract on the federal and state laws that govern the confidentiality of PII.	state laws governing confidentiality of such data prior to receiving access.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	<p>Contractor seeks out service providers that shares their commitment to maintaining the privacy and security of Personal Data and requires their subprocessors to respect their user data to the same or greater degree as we do. Contractor has implemented a variety of physical, administrative and technological safeguards designed to preserve the integrity and security of their personal information they collect and to protect against unauthorized access to data. These include internal reviews of data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where personal data is stored.</p> <p>Contractor restricts access to personal information to Contractor's employees, contractors, and agents who need to know that information in order to operate, develop or improve their services.</p>

5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	<p>Contractor maintains security incident management policies and procedures and will, to the extent permitted by law, promptly notify customers of any unauthorized disclosure of PII. Contractor maintains Security Incident Response Plan includes policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Personal Data or information systems. There are also procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and</p>
---	--	---

		document security incidents and their outcomes.
--	--	---

6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	<p>Unless otherwise directed by a School or Parent, Contractor will delete or de identify personal information of student and child users after a period of inactivity, after the termination or cancellation of the license subscription, or after termination of their agreement with the School, in accordance with the terms of any applicable written agreement with the School, written requests from unauthorized School administrators, and our standard data retention schedule. Authorized School administrators may contact Contractor at compliance@ixl.com to request additional information about Contractor's standard data retention schedule and available options for customizing Contractor's standard data retention schedule to meet individual School requirements.</p>
7	Describe your secure destruction practices and how certification will be provided to the EA.	<p>Unless otherwise directed by a School or parent, Contractor will delete or de identify personal information of student and child users after a period of inactivity after the termination or cancellation of the license subscription, or after termination of their agreement with the School, in accordance with the terms of any applicable written agreement with the School, written requests from authorized School administrators, and their standard data retention schedule. Authorized School administrators may contact Contractor at compliance@ixl.com to request additional information about their standard data retention schedule and available options for customizing Contractor's standard data retention schedule to meet individual School requirements.</p>

8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	As outlined herein, Contractor's practices are designed and implemented with the goal of maximizing the security and privacy of all customer data. This includes limiting access to EA data to employees with a business need and encrypting all data in transit and at rest. Please inquire if more information is needed.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Contractor have asset management controls and policies in place for physical devices and software within our organization. Contractor have mapped organizational comms and data flows and cataloged external subprocessors. Contractor have also categorized information systems and organizational resources in accordance with applicable company policies.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Contractor have established and communicated priorities for organizational mission and objective. Contractor have also put in place contingency plans and disaster recovery policies to inform decisions and deliver mission critical services.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Contractor have established and communicated organizational cybersecurity policies, and coordinated and aligned roles and responsibilities with internal roles and external partners. Legal requirements and obligations regarding cybersecurity and privacy are understood and managed.

	<p>Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including</p>	<p>Contractor identify, document, and patch asset vulnerabilities on a regular schedule. Contractor also identify, document, and remediate both internal and external threats. We identify and prioritize risk responses.</p>
--	---	---

Function	Category	Contractor Response
	<p>mission, functions, image, or reputation), organizational assets, and individuals.</p>	
	<p>Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>Contractor have established risk management processes that are agreed upon by organizational stakeholders. Contractor clearly express organizational risk tolerance, which is determined by security standards compliance and sector-specific regulations.</p>
	<p>Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.</p>	<p>Contractor assess and choose third-party subprocessors, including AWS, using risk assessment processes. Contractor use contracts with third party partners to implement appropriate measures that manage security and risk tolerance. Our third-party partners are also routinely assessed using industry standard audits, such as SOC 2, to ensure appropriate security of information systems.</p>
<p>PROTECT (PR)</p>	<p>Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>Contractor manage and protect access to physical assets using RFID badges, and access is limited to IT staff performing physical maintenance. Contractor require unique user credentials and two-factor authentication to access network environments containing user data. Contractor have policies in place for managing identity and credential lifecycles. Our production hosts run on Amazon Web Services, which is SOC 2 compliant. Contractor limit remote access to VPN and manage ACLs by principle of least necessary privilege.</p>
	<p>Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.</p>	<p>Contractor provide all personnel with IT onboarding training upon starting employment and randomly select employees for security assessment practical examination on an ongoing basis. Privileged personnel undergo additional training commensurate with their roles and responsibilities. Contractor communicate expectations regarding additional roles and responsibilities to employees and third-party stakeholders as needed.</p>
	<p>Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>Contractor protect data in transit using TLS and SSH. All data stored in ABCya production environment is encrypted at rest using AES-256 bit encryption. Contractor use real-time replication and verify the integrity of the replica on a continuous basis. ABCya periodically creates a database clone from offline backups. Contractor use over-provisioning, redundancy, geographic distribution, and uninterruptible power supplies to ensure high availability. Contractor also separate development and testing environments from our production environment.</p>

	<p>Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.</p>	<p>Contractor create and maintain baseline configuration of systems and put system lifecycle policies in place for managing information systems. Contractor continuously conduct, maintain, and test backups of information. Contractor destroy data in accordance with policy. Contractor track changes to system configuration and put configuration change control processes in place. Contractor also implement and manage incident response and disaster recovery plans. Contractor include cybersecurity in HR practices. Contractor also have developed and implemented a vulnerability management plan.</p>
	<p>Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>Contractor perform and log maintenance and repair of organizational assets with approved tools. Contractor also approve, log, and perform remote maintenance of organizational assets in a manner that prevents unauthorized access.</p>

Function	Category	Contractor Response
	<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>Contractor have implemented mechanisms to achieve resilience requirements in normal and adverse situations, including using a third-party CDN/proxy and web application firewall (WAF) to mitigate against possible DDoS attacks</p>
<p>DETECT (DE)</p>	<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>Contractor have established a baseline of network operations and expected data flows and actively monitor for events. We analyze detected events to understand incidents and their impact. Contractor collect and correlate event data from multiple sources and sensors, and determine the impact of events based on that data. Contractor have also established incident alert thresholds.</p>
	<p>Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>Contractor monitor the network to detect potential cybersecurity events. Our physical production environment is monitored 24/7. Contractor run software internally to identify and alert us about real-time security events such as excessive failed login attempts, suspicious network traffic, etc and store event logs in a tamper proof fashion.</p>
	<p>Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>Contractor have well-defined roles and responsibilities for detection and incident response, and our detection activities comply with applicable policies and requirements. We seek to continually communicate and improve detection information and processes.</p>
<p>RESPON D (RS)</p>	<p>Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>Contractor have documented our incident response and recovery plan and made stakeholders aware of their roles. Steps include investigation by the appropriate members of our security team, resolution via engineering (for code vulnerabilities) or IT (for OS/networking vulnerabilities), testing the fix to ensure it truly resolves the issue, and quickly applying the validated fix to production.</p>

	<p>Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>Contractor ensure that personnel know their roles and order of operations when response is needed. Incidents are reported and information is shared consistent with policy criteria. Contractor coordinate with stakeholders consistent with our response plans.</p>
	<p>Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>Contractor investigate notifications from detection systems and evaluate and categorize the impact of incidents consistent with our response plans. The goal of the investigation is to figure out where the vulnerability exists and what impact it has. Once the type of issue is identified, Contractor can move on to resolution.</p>
	<p>Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>Contractor contain and mitigate threats to prevent expansion of an event. Contractor mitigate or document newly-identified vulnerabilities based on their associated risk levels.</p>
	<p>Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>Contractor conduct thorough postmortems for all incidents and update response strategies to account for new information learned.</p>
<p>RECOVER (RC)</p>	<p>Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>Contractor execute recovery plans during or after a cybersecurity incident to ensure that systems are restored. Through redundancy, geographic distribution, and offline backups, we can restore data to its state up to three weeks in the past.</p>

Function	Category	Contractor Response
	<p>Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>Through thorough postmortems, Contractor incorporate lessons learned and reflect new information in our recovery plans.</p>
	<p>Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<p>Contractor communicate recovery activities to internal and external stakeholders as well as executive and management teams. Contractor also comply with all state and federal requirements for notifying impacted parties.</p>