



**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 Amplify Education, Inc. (“Vendor”) are parties to a contract located at [amplify.com/customer-terms](https://amplify.com/customer-terms) (“the underlying contract”) governing the terms under which DISTRICT accesses, and Vendor provides mCLASS DIBELS 8th Edition (“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 Amplify Education, Inc.
- 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 this Contract and 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 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 except to the extent such use is permitted by applicable law; 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. Notwithstanding the

foregoing, as a vendor to multiple state and district customers, Vendor cannot allow direct access to its systems. Upon request, Vendor will provide results of the most recent third party security assessment report that is relevant to District's data.

- 7.3 Vendor is prohibited from using Protected Information for 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; provided that technical personnel may access software applications containing Protected Information for the purpose of customer support. Any Protected Information must be stored solely in data centers in CONUS or Canada except as otherwise provided herein.

## **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 and if such entity has access to Protected Information, 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 materially similar 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 and DISTRICT request, 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

as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities in accordance with the Contract.

10.4

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 unless such third party agrees not to attempt to re-identify the data.

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

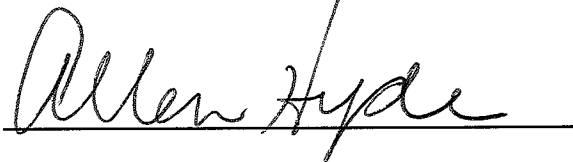
#### **13. Additional Vendor Responsibilities**

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 as follows: In transit: Vendor encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes. At rest: Vendor encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm.;
- 13.6 Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data that is Protected Information 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 out-of-pocket 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:

*July 20, 2023*

For Amplify Education, Inc.



Melissa Ulan  
SVP Product, Literacy

Date: 07 / 25 / 2023

## **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 CJ Amarosa, MIS Director, 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**

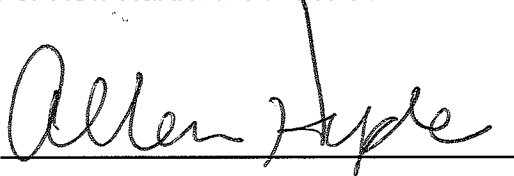
In order to meet 21st century expectations for effective education and efficient operation, the District utilizes several products and services that involve third party contractors receiving access to student data, or principal or teacher data, protected by Section 2-d of the Education Law. The District 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 Amplify Education, Inc.




Allen Hyde  
Assistant Superintendent

Melissa Ulan  
SVP Product, Literacy

Date: *July 20, 2023*

Date: 07 / 25 / 2023

**Supplemental Information About This Contract**

<b>CONTRACTOR</b>	Amplify Education, Inc.
<b>PRODUCT</b>	mCLASS DIBELS 8th Edition
<b>PURPOSE DETAILS</b>	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 K–6 assessment and intervention for early literacy. The purposes for which Amplify will use student, teacher, or principal data are described in Amplify’s Customer Privacy Policy, available at <a href="https://amplify.com/customer-privacy/">https://amplify.com/customer-privacy/</a> .
<b>SUBCONTRACTOR DETAILS</b>	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.
<b>DATA DESTRUCTION INFORMATION</b>	The agreement expires [Date] Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by, DISTRICT. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
<b>DATA ACCURACY INFORMATION</b>	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.
<b>SECURITY PRACTICES</b>	<p>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: In transit: Amplify encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes.</p> <p>At rest: Amplify encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm.</p>



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.

*New York Data Privacy and Security Addendum*

*The purpose of this Addendum is to facilitate educational agency compliance with New York State Education Law section 2-d and regulations promulgated thereunder ("NY Education Privacy Laws"), including the requirement under section 121.2 of the regulations that each educational agency shall 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 principal data be maintained in accordance with federal and state law and the educational agency's data security and privacy policy.*

*This Addendum supplements Amplify's Terms and Conditions for use of Amplify products licensed by the educational agency available at <https://amplify.com/customer-terms> (the "Agreement").*

*For the purposes of this Agreement, "breach," "commercial or marketing purpose," "disclose or disclosure," "education records," "encryption," "personally identifiable information," "release," "student data," "teacher or principal data," "unauthorized disclosure or unauthorized release" will be as defined by NY Education Privacy Laws.*

- 1. Bill of Rights for Data Privacy and Security. In accordance with section 121.3 of the regulations, Amplify hereby agrees to comply with the parents bill of rights for data privacy and security ("bill of rights") as promulgated by the educational agency. In accordance with section 121.3(c) of the regulations, see Attachment A for supplemental information to the bill of rights.*
- 2. Data Security and Privacy Plan. In accordance with Section 121.6 of the regulations, see Attachment B for Amplify's data security and privacy plan.*
- 3. Third Party Contractor Compliance. In accordance with Section 121.9 of the regulations, Amplify as a third-party contractor that will receive student data or teacher or principal data, represents and covenants that Amplify will:*
  - o (1) adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework;*
  - o (2) comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law § 2-d; and this Part 121;*
  - o (3) limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;*
  - o (4) not use the personally identifiable information for any purpose not explicitly authorized in its contract;*
  - o (5) not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i) 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 state and federal law, regulations and its contract with the educational agency; or (ii) unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.*
  - o (6) maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;*
  - o (7) use encryption to protect personally identifiable information in its custody while in motion or at rest; and*
  - o (8) not sell personally identifiable information 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;*

- *Where Amplify engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on Amplify by state and federal law and this Agreement shall apply to the subcontractor.*
4. *Reports and Notifications of Breach and Unauthorized Release. In accordance with section 121.10 of the regulations, Amplify will:*
- *promptly notify the educational agency of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach;*
  - *cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.*
  - *where a breach or unauthorized release is attributed to Amplify, Amplify shall pay for or promptly reimburse the educational agency for the full cost of such notification. In compliance with this section, notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known; a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.*
5. *General.*
- *The laws of the State of New York shall govern the rights and duties of Amplify and the educational agency.*
  - *If any provision of the contract or the application of the contract is held invalid by a court of competent jurisdiction, the invalidity does not affect other provisions or applications of the contract which can be given effect without the invalid provision or application.*
  - *This Agreement controls over any inconsistent terms or conditions contained within any other agreement entered into by the parties concerning student, teacher and principal data.*

## ATTACHMENT A

### SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

1. *The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract:*

*The purposes for which Amplify will use student, teacher, or principal data are described in Amplify's Customer Privacy Policy, available at <https://amplify.com/customer-privacy/>.*

2. *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 principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., FERPA; Education Law §2-d):*

*Amplify requires all subcontractors or other authorized persons with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.*

3. *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 principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed):*

*The Agreement will last for the time period described in the applicable purchasing document, unless earlier terminated in accordance with the Agreement. Student, teacher, or principal data will be returned or destroyed in accordance with whichever is the sooner of 1) the period necessary to fulfill the purposes outlined in Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, or 3) the educational agency's option and direction.*

4. *If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected:*

*A parent, student, eligible student, teacher or principal may contact the educational agency directly to discuss the correction of any such erroneous information. If Amplify receives a request to review student data in Amplify's possession directly from such a party, Amplify agrees to refer that individual to the educational agency and to notify the educational agency within a reasonable time of receiving such a request. Amplify agrees to work cooperatively with the educational agency to permit a parent, student, eligible student, teacher or principal to review student, teacher, or principal data that has been shared with Amplify and correct any erroneous information therein.*

5. *Where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated:*

*Amplify leverages Amazon Web Services (AWS) as its cloud hosting provider. Further information regarding Amplify's security program can be found on Amplify's Information Security page at <https://amplify.com/security>.*

6. *Address how the data will be protected using encryption while in motion and at rest:*

*In transit: Amplify encrypts all student personal information in transit over public connections, using Transport Layer Security (TLS), commonly known as SSL, using industry-standard ciphers, algorithms, and key sizes.*

*At rest: Amplify encrypts student personal information at rest using the industry-standard AES-256 encryption algorithm*

## ATTACHMENT B

### DATA SECURITY AND PRIVACY PLAN

*In accordance with Section 121.6 of the regulations, the following is Amplify's data security and privacy plan:*

1. *Outline how the third-party contractor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy:*

*Amplify's privacy policy, available at [amplify.com/customer-privacy/](https://amplify.com/customer-privacy/), outlines how Amplify's practices enable its customers to control use, access, sharing and retention of personal information in compliance with FERPA and other applicable privacy laws and regulations. Upon request, Amplify will also certify compliance with the educational agency's data security and privacy policy.*

2. *Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the contract:*

*Administrative, operational and technical safeguards and practices to protect PII under the Agreement are described in Amplify's Information Security page at <https://amplify.com/security>.*

3. *Demonstrate that it complies with the requirements of Section 121.3(c) of this Part 121:*

*The supplemental information required by Section 121.3(c) of this Part 121 are attached to this Addendum as Attachment A.*

4. *Specify how officers or employees of the third-party contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access:*

*Amplify has a comprehensive information security training program that all employees and individuals with access to Amplify systems undergo upon initial hire or engagement, with an annual refresher training. We also provide information security training for specific departments based on role.*

5. *Specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected:*

*Amplify may use independent contractors engaged by Amplify in the ordinary course of business or for purposes that are incidental or ancillary to the provision of services under the Agreement. Amplify requires all contractors with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.*

6. *Specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency:*

*If there has been an unauthorized release, disclosure or acquisition of the educational agency's student, teacher, or principal data, Amplify will notify the educational agency in accordance with applicable laws and regulations. Such notification will include the following steps: Amplify will notify the educational agency after Amplify determines that the educational agency's student, teacher, or principal data were released, disclosed, or acquired without authorization, (a "Security Incident"), without unreasonable delay, subject to applicable law and authorization of law enforcement personnel, if applicable. To the extent known, Amplify will identify in such a notification the following: (i) the nature of the Security Incident, (ii) the steps Amplify has executed to investigate the Security Incident, (iii) the type(s) of personally identifiable information that was subject to the unauthorized disclosure, release, or acquisition, (iv) the cause of the Security Incident, if known, (v) the actions Amplify has done or will do to remediate any deleterious effect of the Security Incident, and (vi) the corrective action Amplify has taken or will take to prevent a future Security Incident.*

7. *Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.*

*Upon the termination or expiration of the Agreement and upon the educational agency's request, student, teacher, or principal data will be returned, transitioned, and/or destroyed in accordance with 1) Amplify's Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, and 3) in accordance with the educational agency's direction.*





**New Hartford Central School  
District**  
**33 Oxford Road, New Hartford, NY 13413**

**Release and/or Sharing of Student/Teacher/Principal Data Form**

Third-Party Contractors requesting access to student data and/or teacher or principal data ("data") must complete this form to ensure the confidentiality and security of data as required by Board of Education policy and all applicable local, state, and federal laws. Attach addendums to the questions if more space is needed

<b>Contractor/Company: Amplify Education, Inc.</b> <b>Representative Name and Title: Jennifer Fosegan, Account Executive</b> <b>Contractor Phone Number: (800) 823-1969</b>
<b>1. Describe the data that is being requested and/or stored:</b> Please see attached Amplify mCLASS Schedule of Student Data.
<b>2. Exclusive purposes of the use of the data:</b>  The purposes for which Amplify will use student, teacher, or principal data are described in Amplify's Customer Privacy Policy, available at <a href="https://amplify.com/customer-privacy/">https://amplify.com/customer-privacy/</a> .
<b>3. Will any third-party subcontractors have access to the data?      Yes</b>  If yes, how will you ensure that subcontractors, and any persons or entities that the third party subcontractor may share the data with, will abide by data protection and data security requirements: Amplify requires all subcontractors or other authorized persons with access to student, teacher, or principal data to agree in writing to abide by all applicable state and federal laws and regulations. Additionally, as between Amplify and the educational agency, Amplify takes full responsibility for the actions of any such parties.
<b>4. What happens to the data upon expiration of the agreement or relationship with the District?</b> <b>The Agreement will last for the time period described in the applicable purchasing document, unless earlier terminated in accordance with the Agreement. Student, teacher, or principal data will be returned or destroyed in accordance with whichever is the sooner of 1) the period necessary to fulfill the purposes outlined in Amplify's Customer Privacy Policy and the Agreement, 2) applicable state and federal laws and regulations, or 3) the educational agency's option and direction.</b>
<b>5. How would a parent, student, eligible student, teacher or principal challenge the accuracy of the data that is collected or stored?</b> <b>A parent, student, eligible student, teacher or principal may contact the educational agency directly to discuss the correction of any such erroneous information. If Amplify receives a request to review student data in Amplify's possession directly from such a party, Amplify agrees to refer that individual to the educational agency and to notify the educational agency within a reasonable time of receiving such a request. Amplify agrees to work cooperatively with the educational agency to permit a parent, student, eligible student, teacher or principal to review student, teacher, or principal data that has been shared with Amplify and correct any erroneous information therein.</b>

**6. Describe where the data will be stored so as to protect data security and the security protections that will be taken to ensure such data will be protected, including whether such data will be encrypted and if so, how?**

**Amplify leverages Amazon Web Services (AWS) as its cloud hosting provider. Further information regarding Amplify's security program can be found on Amplify's Information Security page at <https://amplify.com/security>.**



## NEW HARTFORD CENTRAL SCHOOL DISTRICT PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The New Hartford Central School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the District informs the school community of the following:

- 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.
- 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 New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints to the District should be directed in writing to Data Protection Officer, New Hartford Central School District, 33 Oxford Rd, New Hartford, NY, 13413 or to [jgillette@nhart.org](mailto:jgillette@nhart.org). Complaints to the State Education Department should be submitted, in writing, to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure> , or to [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

This bill of rights is subject to change and will be revised from time to time in accordance with regulations issued by the Commissioner of Education and guidance received from the State Education Department

**APPENDIX TO PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the New Hartford Central School District may enter into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following information will be included in the contract, Data Protection Agreement, or Terms of Service/Privacy Policy Contract Addendum with this Bill of Rights:

- 1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
- 2) 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 principal 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);
- 3) 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 principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
- 4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
- 5) Where the student data or teacher or principal 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
- 6) Address how the data will be protected using encryption while in motion and at rest.

Name Melissa Ulan Title SVP Product, Literacy Signature Melissa Ulan

Company Name Amplify Education, Inc. Product Name: mCLASS DIBELS 8th Edition

By signing the above, you agree to comply with the terms of the New Hartford Central School District Parents' Bill of Rights for Data Privacy and Security, to the extent the foregoing provisions are applicable to your company.