



Amended DATA SHARING AGREEMENT

WHEREAS, the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and its implementing regulations codified at 34 C.F.R 99. 1 et seq. make personally identifiable student information in education records (herein, "student information," "personally identifiable student data," "student data," or "data") confidential and, subject to certain exceptions, prohibits the disclosure of such information to third parties,

WHEREAS, FERPA and its implementing regulations allow for an educational agency or institution to share personally identifiable student-level data with contractors performing work on their behalf,

WHEREAS, FERPA and its implementing regulations at 34 C.F.R. 99.31(b)(1) allow for the sharing of personally identifiable student information with organizations under circumstances in which parental permission has been obtained,

WHEREAS, La R.S. 17:3913(F) requires protection of personally identifiable student information in a manner that allows only specifically authorized access individuals and entities the ability to do so,

WHEREAS, La R.S. 17:3914 allows for Local Educational Agencies to contract with a private entity for student and other educational services and release personally identifiable student information pursuant to the terms of the Contract,

WHEREAS, La R.S. 17:3914 allows for the Claiborne Parish School Board to share data outside the state of Louisiana for purposes of academic analysis of assessments,

WHEREAS, the Claiborne Parish School Board (hereinafter referred to as "District") and Amplify (hereinafter referred to as "Contractor") have entered into a contractual arrangement, pursuant to which the Contractor will provide services to the District.

WHEREFORE, the District and Contractor do enter into this Agreement subject to the terms and conditions as specified herein.

This Data Sharing Agreement, together with the Amplify Customer Terms located at <https://amplify.com/customer-terms/> (together, the "Agreement"), upon execution, shall supersede and replace all other Data Sharing Agreements that are in existence between the

District and the Contractor. Subject to the foregoing, the terms of any original Agreement shall remain in full force and effect in accordance to all applicable law. For sake of clarity, this Data Sharing Agreement shall take precedence over the Amplify Customer Terms to the extent there is any conflict.

1. Purpose of the Disclosure

The Contractor agrees to collect and use any data disclosed to it pursuant to this Agreement solely for the purposes of providing services to the District for Assessments and Services related to Amplify. Student data provided directly to the Contractor by the student or the student's parent/guardian is not subject to this Agreement.

Contractor shall comply with all applicable data protection, privacy laws, and regulations.

2. Data

The District may provide the following Student data outlined on Exhibit A via Clever, the authorized third party represented of the District:

In accordance with Louisiana Act 387, Contractor shall not include or use Social Security Numbers as the basis of primary student identifiers. The District reserves the right to withhold any of the foregoing data if determined, in their sole discretion, that disclosure of such data would violate any provision of state or federal law.

4. Confidentiality

This Agreement is entered into by Contractor and the District in accordance with the provisions of the Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232(g), et seq., (FERPA) and La. R.S. 17:3914. The Contractor hereby acknowledges that all documents which include student information contained in or derived from a student's education records are deemed confidential pursuant to FERPA and La. R.S. 17:3914 and therefore will not be disclosed by Contractor to any unauthorized third party as described within this Agreement.

Contractor shall retain the original version of the data and shall not make a copy or extract of the data available to anyone except personnel or authorized third party service providers who have a need for the data to perform the

services referenced in this Agreement. Contractor shall maintain the data in hard copy or electronic form, in an area that has limited access only to Contractor's authorized personnel. Contractor shall not permit removal of the data from the limited access area unless legally required. Contractor will ensure that access to the data maintained on computer files or databases is controlled by strong, modern authentication protocols. Contractor shall establish procedures to ensure that the data cannot be extracted from a computer file or database by unauthorized individuals. Contractor shall maintain all printouts, discs, or other physical products containing student-level data in locked cabinets, file drawers, or other secure locations when not in use. Contractor shall destroy the data provided to Contractor, including all copies, whether in electronic or hard copy form, when the services are completed or this Agreement is terminated, whichever occurs first.

Contractor is permitted to disclose confidential information and data to its employees, authorized third party service providers subcontractors, agents, consultants and auditors on a need to know basis only, provided that all such third party service providers, agents, consultants, and auditors have written confidentiality obligations to Contractor at least as restrictive as this Agreement.

Contractor agrees that if this Agreement is terminated or expires, upon District's request, Contractor shall return all data to the District in a usable electronic format. Contractor further agrees to erase, destroy, and render unreadable, all data in its entirety in a manner that prevents its physical reconstruction through the use of commonly available file restoration utilities. Upon request, Contractor shall certify in writing that these actions have been completed within 90 days of the termination of the Contract or within sixty (60) days from receipt of any request by the District, whichever comes first.

5. Restrictions on Use

Contractor shall not distribute, use, or share Student data for any purpose not expressly permitted in this Agreement, including commercial advertising, marketing, or any other commercial purpose. Contractor cannot disclose any document, whether in hard copy or electronic form, or otherwise disclose to any unauthorized third party any Student data or information in any form whatsoever or under any circumstances which would directly or indirectly make a student's identity traceable, except as otherwise required by law. Contractor shall provide data in a structured, commonly used, and machine-readable format upon request by the District to facilitate data portability for parents and students. Contractor may also disclose Student data to government agencies to comply with the law or in response to legal or administrative processes such as subpoenas. Prior to disclosing any Student data in response to a legal or administrative process such as a subpoena, Amplify shall provide notice to the District and provide the District a reasonable opportunity to object to the disclosure (move to quash). The term "unauthorized third party" for purposes of this Agreement does not include governmental agencies and educational institutions that have authority over schools or students (e.g., Louisiana Department of Education); students or their parents/guardians; parties with whom students or their

parents/guardians have authorized Contractor to disclose the Student data; or authorized third party who have agreed in writing to provide at least as restrictive protections for student data as this Agreement.

As required by Federal and State law, Contractor further agrees that no data of any kind shall be revealed, transmitted, exchanged or otherwise passed to any unauthorized third party.

6. Indemnification

Contractor shall defend, indemnify and hold harmless the District and any and all of the District's directors, officers, officials, employees, agents, contractors and representatives against and from any and all costs, expenses, damages, injury or loss, including reasonable attorney's fees, to which they or any of them may be subject from any third-party claims arising out of any cause related to a Security Breach (as defined below), except to the extent that they are due to the fault or negligence of the District.

7. Ownership

Any data delivered or transmitted to the Contractor by the District pursuant to this Agreement is the property of the District and shall only be used by the Contractor as allowed in this Agreement and will be retained and destroyed in accordance with this Agreement.

While data delivered by the District remains the property of the District, Contractor shall fulfill all legal obligations to provide parents and students access to their own student records as required by FERPA, La. R.S. 17:3913(F), and La. R.S. 17:3914.

8. Security Measures

Contractor must protect personally identifiable information by appropriate security measures, including, but not limited to, the use of user names, secure passwords, encryption, security questions, etc. Contractor network must maintain a high level of electronic protection to ensure the integrity of sensitive information and to prevent unauthorized access in these systems. The Contractor agrees to perform regular reviews of its protection methods and perform system auditing to maintain protection of its systems. Contractor agrees to maintain secure systems that are patched, up to date, and have all appropriate security updates installed.

To ensure that the only individuals and entities who can access student data are those that have been specifically authorized by Contractor to access personally identifiable student data, Contractor shall implement appropriate forms of modern authentication and authorization protocols to identify and permit the specific individual who is accessing the information. Contractor must individually determine the appropriate level of security that will provide the necessary level of protection for the student data it maintains. Contractor shall not allow any individual or entity unauthenticated, unauthorized, or insecure access to confidential personally identifiable student records or data at any time.

Contractor shall implement appropriate measures to ensure the confidentiality, integrity, and availability of personally identifiable information, protect against any unanticipated access or disclosure of information.

Contractor agrees that any and all personally identifiable student data will be stored, processed, and maintained in a secure location and solely on designated servers. No District data, at any time, will be processed on or transferred to any portable computing device or any portable storage medium, unless that storage medium is in use as part of the Contractor's designated backup and recovery processes. All servers, storage, backups, and network paths utilized in the delivery of the service shall be contained within the United States unless specifically agreed to in writing by the District.

Contractor shall develop a policy for the protection and storage of audit logs. The policy shall require the storing of audit logs and records on a server separate from the system that generates the audit trail. Contractor must restrict access to audit logs to prevent tampering or altering of audit data. Retention of audit trails shall be based on a schedule determined after consultation with operational, technical, risk management, and legal staff.

9. Security Audits

Pursuant to in La. R.S. 17:3914, and all applicable state and federal law, the Contractor shall conduct security audit checks pertaining to Contractor's security and usage of student data. Upon request, Contractor will provide the District with results of the most recent third party security assessment report that is relevant to District's data.

10. Security Breach

As used in this Agreement "Security Breach" means any act or omission that compromises either (i) the security, confidentiality or integrity of personally-identifiable student information or (ii) the physical, technical, administrative or organizational safeguards put in place by Contractor that relate to the protection of the security, confidentiality or integrity of personally-identifiable student information, that leads to unauthorized access to or disclosure of student information. This definition applies regardless of whether Contractor stores and manages the data directly or through a contractor, such as a cloud service provider. Contractor shall establish and implement a clear data breach response plan outlining organizational policies and procedures for addressing a potential Security Breach.

Contractor's response plan shall require prompt response for minimizing the risk of any further data loss and any negative consequences of the Security Breach, including potential harm to affected individuals.

Contractor shall take commercially reasonable steps, in accordance with industry standards, to prevent Security Breaches. Contractor shall also take commercially reasonable steps, in accordance with industry standards, to promptly remedy any Security Breach and prevent any further Security Breach at Contractor's expense in accordance with standard industry practices and applicable law.

Contractor agrees to comply with the requirements of La. R.S. 51 :3071 et seq. (Louisiana Database Breach Notification Law) as well as any other applicable laws that require the notification in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a Security Breach,, Contractor agrees to notify the

District promptly, and in any event, in the timeframe required by applicable law and to indemnify, hold harmless and defend the District and its employees from and against any and all third-party claims, damages, or causes of action related to the Security Breach. Contractor shall: (i) provide the District with the name and contact information for an employee of Contractor who shall serve as the District's primary security contact and shall be available to assist District as a contact in resolving issues and fulfilling obligations associated with a Security Breach; (ii) promptly notify the District via email or phone call to the District contacts which have been provided to the Contractor as soon as becoming aware of a Security Breach. Immediately following Contractor's notification to the District of a Security Breach, the District and Contractor shall coordinate with each other to investigate the Security Breach. Contractor agrees to fully cooperate with District in their handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and (iii) providing information to assist the District with any notices to persons or organizations affected by the Security Breach as required by law.

11. Term of Agreement

This Agreement shall begin on 07/01/2026 and shall terminate on 06/30/2027. The effective date of this Agreement may be extended only if an amendment to that effect is duly executed by the parties and approved by the necessary authorities prior to said termination date. If either party informs the other that an extension of this Agreement is deemed necessary, an amendment may be prepared by one party for appropriate action by the other party.

12. Termination

Either party may terminate this Agreement upon written notice to the other party in the event that the other party materially breaches its obligations under the Agreement and fails to cure such breach within thirty (30) days after receiving written notice of such breach.

The Contractor may request amendment or termination of this Agreement giving written notice within thirty (30) days to the District, subject to the approval of the District. The District shall pay Amplify for all Assessments and Services delivered through the date of termination.

13. Assignment of Contract

Contractor shall not assign any interest in this Agreement by assignment, transfer, or novation, without prior written consent of the District. Notwithstanding the foregoing, assignment shall be permitted to an affiliate or in the event of a merger, acquisition, or reorganization, or a sale of substantially all of Amplify's assets relating to this Agreement. Nothing in this provision shall preclude the Contractor from subcontracting with third parties to perform work contemplated herein. Contractor is responsible for ensuring that any such authorized third party service provider adhere to, and agree to be bound by provisions that are no less stringent than the provisions of this Agreement, and Provider shall remain fully responsible for the acts or omissions of such authorized third party service provider.

14. Jurisdiction, Venue and Governing Law

Contractor acknowledges and agrees that unauthorized disclosure, use, or retention of protected student information may irreparably damage the District in such a way that adequate compensation could not be obtained solely in monetary damages. Accordingly, the District shall have the right to seek injunctive relief restraining the actual or threatened unauthorized disclosure, use, or retention of any protected student information, in addition to any other remedy otherwise available (including reasonable attorney fees). Contractor hereby waives the posting of a bond with respect to any action for injunctive relief.

Exclusive jurisdiction and venue for any and all suits between the District and Contractor arising out of, or related to, this Agreement shall be filed and adjudicated in the state or federal courts of Parish of Claiborne, State of Louisiana.

The laws of the State of Louisiana, without regard to Louisiana law on conflicts of law, shall govern this Agreement.

15. Survival

Contractor's obligation under Clauses 2, 4, 5, 6, 7, and 14 shall survive expiration and/or termination of this Agreement. Contractor's obligations under Clauses 8, 9, and 10 shall survive expiration and/or termination of this Agreement until the Contractor has fully complied with its obligation to destroy data as set forth herein, along with all applicable legal penalties.

IN WITNESS WHEREOF, the parties have executed this Agreement as of May 26, 2026.

Amplify Education, Inc.

Catherine Mackay

Authorized Representative

Catherine Mackay

Authorized Representative Name (Print)

President and COO

Title

06/17/2026

Date

CLAIBORNE PARISH SCHOOL BOARD

B Sheppard

Bewanichi Sheppard (Signature)

Bewanichi Sheppard

(Print)

Federal Program and Technology Supervisor

Title

6-17-26

Date

EXHIBIT A:
SCHEDULE OF DATA

Amplify Schedule of Student Data

	Data Elements	Purpose	Used by Amplify?	Provided by District, or Collected by Application?
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	For support purposes; in aggregate, to inform product improvements	Required	Collected by Application
	Other application technology meta data	For support purposes; in aggregate, to inform product improvements	Required	Collected by Application
	Other application technology meta data - Please specify:	For support purposes; in aggregate, to inform product improvements	* Browser User Agent * Operating system brand and version * Browser brand and version	Collected by Application
Application Use Statistics	Meta data on user interaction with application	For support purposes; in aggregate, to inform product improvements	If students are rostered: Required	Collected by Application
	Meta data on user interaction with application - Please specify:	For support purposes; in aggregate, to inform product improvements	User interactions, timestamps, etc.	Collected by Application
Assessment	Observation data	For observational assessment incorporated into the product	If students are rostered: Optional	Collected by Application
Demographics	Date of Birth	For rostering purposes	If students are rostered: Optional	Provided by District
	Gender	For optional aggregate reporting	If students are rostered: Optional	Provided by District
	Ethnicity or race	For optional aggregate reporting	If students are rostered: Optional	Provided by District
	Language information (native, preferred or primary language spoken by student)	To support in-app language choices, and optional aggregate reporting	If students are rostered: Optional	Provided by District
	Other demographic information	For optional aggregate reporting	Optional	Provided by District
	Other demographic information - Please specify:	For content or feature selection	Additional CEDS-aligned demographics may be optionally supplied for aggregate reporting purposes	Provided by District
Enrollment	Student school enrollment	For rostering purposes	If students are rostered: Required	Provided by District
	Student grade level	For rostering purposes and content alignment	If students are rostered: Required	Provided by District
	Homeroom	For rostering purposes	Optional	Provided by District
	Specific curriculum programs	For rostering purposes and content alignment	If students are rostered: Required	Provided by District
Schedule	Student scheduled courses	For rostering purposes and content alignment	If students are rostered: Required	Provided by District
	Teacher names	For rostering purposes	Required	Provided by District
Special Indicator	English language learner information	To support in-app language choices, and optional aggregate reporting	If students are rostered: Optional	Provided by District
	Low income status	For optional aggregate reporting	If students are rostered: Optional	Provided by District
	Student disability information	For optional aggregate reporting	Optional	Provided by District
	Specialized education services (IEP or 504)	For optional aggregate reporting	If students are rostered: Optional	Provided by District
	Other indicator information	For optional aggregate reporting	If students are rostered: Optional	Provided by District
Special Indicator	Other indicator information - Please specify:	For optional aggregate reporting	Additional CEDS-aligned demographic indicators may be optionally supplied for aggregate reporting purposes	Provided by District
Student Contact Information	Email	For logging in	If students are rostered: Required	Provided by District
Student Identifiers	Local (School district) ID work data - Please specify	For rostering purposes	If students are rostered: Required	Provided by District
Student Identifiers	State ID number		Optional	
Student Identifiers	Student app username	For logging in	If students are rostered: Optional	Provided by District
Student Identifiers	Student app passwords	For logging in	If students are rostered: Optional	Collected by Application
Student Name	First and/or Last	For rostering purposes	If students are rostered: Required	Provided by District
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program - student reads below grade level)	For application adaptivity and student performance reporting	If students are rostered: Required	Collected by Application
Student work	Student generated content; writing, pictures etc.	For classroom interactivity and student performance reporting	If students are rostered: Required	Collected by Application
Student work	Other student work data (media; audio + image uploads)	Uploading student work (screenshots, images)	Optional	Collected by Application

