

## ADDENDUM TO CONTRACT

This Addendum to Contract ("Addendum") is entered into by and between Louisiana Consortium of Immersion Schools» (hereinafter "«LCIS»") and the Calcasieu Parish School B(hereinafter "School Board") The Addendum is effective as of the \_\_\_1st\_\_\_ day of \_\_\_December\_\_\_\_\_, 2022.

During the 2014 Louisiana Legislative Session, the State of Louisiana enacted new laws governing the collection, disclosure and use of students' personally identifiable information. The new laws require that any contracts between a school system and a third-party, who is entrusted with personally identifiable information of any student, contain the statutorily prescribed minimum requirements as to the use of personally identifiable information. In order to comply with the requirements of the new laws, this Addendum and the terms contained herein are hereby incorporated into the attached agreement entered into between «Vendor» and the School Board.

In accordance with La. R.S. 17:3914(F), «Vendor» agrees to protect personally identifiable information in a manner that allows only those individuals, who are authorized by «Vendor» to access the information, the ability to do so. Personal identifiable information should be protected by appropriate security measures, including, but not limited to, the use of user names, secure passwords, encryption, security questions, etc. «Vendor»'s network must maintain a high level of electronic protection to ensure the integrity of sensitive information and to prevent unauthorized access in these systems. «Vendor» agrees to perform regular reviews of its protection methods and perform system auditing to maintain protection of its systems. «Vendor» 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 «Vendor» to access personally identifiable student data, «Vendor» shall implement various forms of authentication to identify the specific individual who is accessing the information. «Vendor» must individually determine the appropriate level of security that will provide the necessary level of protection for the student data it maintains. «Vendor» shall not allow any individual or entity unauthenticated access to confidential personally identifiable student records or data at any time.

«Vendor» shall implement appropriate measures to ensure the confidentiality and security of personally identifiable information, protect against any unanticipated access or disclosure of information, and prevent any other action that could result in substantial harm to the School Board or any individual identified by the data.

«Vendor» 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 School Board 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 «Vendor»'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 School Board.

«Vendor» agrees that any and all data obtained from the School Board shall be used expressly and solely for the purposes enumerated in the original Contract. Data shall not be distributed, used, or shared for any other purpose. As required by Federal and State law, «Vendor» further agrees that no data of any kind shall be revealed, transmitted, exchanged or otherwise passed to other «Vendor»'s or interested parties. «Vendor» shall not sell, transfer, share or process any student data for any purposes other than those listed in the Contract, including commercial advertising, marketing, or any other commercial purpose.

«Vendor» shall establish and implement a clear data breach response plan outlining organizational policies and procedures for addressing a potential breach. «Vendor»'s response plan shall require prompt response for minimizing the risk of any further data loss and any negative consequences of the breach, including potential harm to affected individuals. A data breach is any instance in which there is an unauthorized release or access of personally identifiable information or other information not suitable for public release. This definition applies regardless of whether «Vendor» stores and manages the data directly or through a contractor, such as a cloud service provider.

«Vendor» 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. «Vendor» 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.

«Vendor» is permitted to disclose Confidential Information to its employees, authorized subcontractors, agents, consultants and auditors on a need to know basis only, provided that all such subcontractors, agents, consultants, and auditors have written confidentiality obligations to «Vendor» and the School Board. The confidentiality obligations shall survive termination of any agreement with «Vendor» for a period of fifteen (15) years or for so long as the information remains confidential, whichever is longer, and will inure to the benefit of the School Board.

«Vendor» acknowledges and agrees that unauthorized disclosure or use of protected information may irreparably damage the School Board in such a way that adequate compensation could not be obtained solely in monetary damages. Accordingly, the School Board shall have the right to seek injunctive relief restraining the actual or threatened unauthorized disclosure or use of any protected information, in addition to any other remedy otherwise available (including reasonable attorney fees). «Vendor» hereby waives the posting of a bond with respect to any action for injunctive relief. «Vendor» further grants the School Board the right, but not the obligation, to enforce these provisions in «Vendor»'s name against any of «Vendor»'s employees, officers, board members, owners, representatives, agents, contractors, and subcontractors.

«Vendor» 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 of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of «Vendor»'s security obligations or other event requiring notification under applicable law, «Vendor» agrees to notify the School Board immediately and assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the School Board

and its employees from and against any and all claims, damages, or causes of action related to the unauthorized release.

In accordance with applicable state and federal law, «Vendor» agrees that auditors from any state, federal, or other agency, as well as auditors so designated by the School Board, shall have the option to audit «Vendor»'s service. Records pertaining to the service shall be made available to auditors and the School Board when requested.

«Vendor» agrees that if this agreement is terminated or expires, «Vendor» shall return all data to the School Board in a useable electronic format. «Vendor» 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. «Vendor» shall certify in writing that these actions have been completed within 30 days of the termination of the Contract or within seven (7) days from receipt of any request by the School Board, whichever comes first.

The terms of this Addendum shall supplement and supersede any conflicting terms or conditions of the original Contract between the Parties. Subject to the foregoing, the terms of the original Contract shall remain in full force and effect.

«LCIS»

CALCASIEU PARISH SCHOOL BOARD

Theriez  
Authorized Representative (Signature)

Shannon LaFargue  
La Fargue, Phd, Shannon (Signature)

Valerie THERIEZ  
Authorized Representative Name (Print)

Shannon LaFargue  
La Fargue, Phd, Shannon (Print)

President  
Title

Superintendent of Schools  
Title

12-15-2022  
Date

12.8.22  
Date



# Calcasieu Parish School Board

BUILDING FOUNDATIONS FOR THE FUTURE

Shannon LaFargue, PhD, Superintendent

To Whom This May Concern,

This document serves as an official addendum to the Data Sharing Agreement, or MOU, agreed upon between Calcasieu Parish School Board (CPSB) and Louisiana Consortium of Immersion Schools (LCIS) effective December 1, 2022. LPSS agrees that LCIS can and will, on behalf of CPSB students, submit student data required for DELF Diploma testing of French Immersion students to the Minister of Education in France in order to maintain the progress and quality monitoring of our French immersion schools.

Only the LCIS designees and the Ministry of Education in France/France Education International will have access to any student data relevant to this internationally respected diploma program. CPSB will ensure parents understand this agreement and will allow concerned parents to opt out of testing at their discretion.

Sincerely,



Shannon La Fargue, PhD,  
CPSB Superintendent of Schools

12.8.22

Date



Accepted by LCIS Team

12-15-2022

Date

Valerie THERIEZ  
Printed Name of LCIS Representative

*Building Foundations for the Future*