

7.2. Any such notices shall be in accordance with federal and Louisiana state law.

7.3. Follett will use its best efforts to mitigate any negative consequences caused to Customer or a student of Customer as a result of a Data Breach and will use its best efforts to implement procedures to prevent the recurrence of a similar event.


8. Follett certifies that student information shall not be retained or available to Follett upon completion of the terms of Agreement and shall be deleted from all Follett-hosted systems. Customer may export their library catalog data from the Platform. Certification of deletion shall be provided in writing upon request by Customer.

9. Follett shall regularly assess its hosted data operations against Follett's Cyber Security framework using third-party assessors who are experienced in education security requirements. Follett's Cyber Security framework incorporates industry standard practices, for data security and privacy of student information. In accordance with applicable law, Follett agrees that it shall permit Customer auditors to perform privacy and security audits related to the Customer's use of the Platform. Customer auditors who perform such privacy and security audits shall be selected by the Customer. Audits shall be performed at the expense of the Customer under the direction of the superintendent. Follett agrees that it shall make its records available to such Customer auditors during normal business hours upon 7 days prior notice and to cooperate with and provide reasonable assistance with access to information requested by the auditors.

10. Except as specifically amended by this Addendum, the Agreement shall continue in full force and effect in all respects.

IN WITNESS WHEREOF, the parties execute this Addendum on the dates set forth below.

VIDALIA LOWER ELEMENTARY SCHOOL

By: 
Name: Paul Nelson
Title: Superintendent
Date: 10-19-95

FOLLETT SCHOOL SOLUTIONS, INC.

By: _____
Name: _____
Title: _____
Date: _____

**ADDENDUM TO AGREEMENTS WITH DESTINY CUSTOMERS IN
LOUISIANA**

This addendum, dated October 14, 2015 (this "Addendum") is by and between Vidalia Lower Elementary School ("Customer") and Follett School Solutions, Inc. ("Follett") in connection with the certain agreement for Follett's Destiny or other product(s) (the "Platform") dated August 7, 2012 (the "Agreement") and is intended to comply with Louisiana student data privacy laws ("Act 677 and Act 837"). All capitalized terms used in this Addendum but not otherwise defined shall have the meaning ascribed to them in the Agreement.

Customer and Follett hereby agree as follows:

1. This Addendum shall be incorporated by reference into the Agreement.
2. The term of this Addendum shall expire on the termination date stated in the Agreement, as the same may be amended.
3. Follett and Customer agree to work together to comply with the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) and Louisiana state laws related to the privacy and security of student information accessed and stored within the Platform by Follett and Customer.
 - 3.1. Follett agrees to protect and maintain the security of Customer's student Personally Identifiable Information ("PII") with commercially reasonable security measures in accordance with industry practices, utilizing appropriate administrative, physical and technical safeguards to secure student records from unauthorized access, disclosure and use.
 - 3.2. Follett's Code of Conduct provides an overview of the standards of behavior for business dealings applicable to Follett employees of. By completing a course and signing the Code of Conduct, Follett employees annually acknowledge their obligation to protect the confidentiality and proprietary information of Follett customers, to not disclose this information to unauthorized persons, and to not engage in illegal activities.
4. Follett shall not use student information for any purpose other than those required or specifically permitted in the Agreement
5. Follett shall not give access to, or release of student information to any person or entity except as specified in the Agreement or in this Addendum.
 - 5.1. Access to the Platform is limited to Follett associates, authorized subcontractors, and auditors with a need to access the Platform for specific functions related to performing a service on behalf of the customer, the Customer and its authorized users, including its Students.
 - 5.2. Access and authentication methods include the assignment of a single login and password shared across the school or through the assignment of unique ID's and passwords for individual students. Customer may choose method of access at their sole discretion. When a single login is shared across a school, no PII or student information is stored by the platform.

- 5.3. When individual student IDs are used, PII that the Customer may store within the Platform may include Student ID, Barcode ID, Student Name, Nickname, email address, Gender, Graduation Year, Address, Phone Numbers, Picture, and Homeroom, plus up to 5 variable fields which may be assigned at the discretion of the Customer. It is the Customer's responsibility to assign and maintain identifying data entered in the platform and to ensure that identifying data complies with federal and state laws.
 - 5.4. ID's may be created through an entry form by a Customer-authorized administrative user, imported by a Customer-authorized administrative user from Customer's Student Information System or other authoritative system, or be validated and authenticated through a secure socket connection from an external library system using the SIP2 protocol. The method of access and authorization is selected by the customer at their sole discretion.
 - 5.5. The Platform supports pass-through and export of limited student information to other external applications that have been authorized by the Customer to provide a service to the Customer, including fines and fee payment and access to ebooks. Customer may enable and disable pass-through of student data at their sole discretion through the platform administrative controls which can be accessed by Customer authorized administrative users. A limited export for fines and fee data is accessible to administrative users authorized by the Customer. Customer is responsible for ensuring that all external applications which receive data from the Platform meet their data privacy and security requirements.
6. Follett has implemented policies and procedures to address storage, retention and disposition of all Customer data which is under Follett's control when Customer chooses to have Follett host the Platform.
 - 6.1. Follett shall perform regular backups of Customer data and shall retain backup copies for a commercially reasonable period of time, or for such period of time as may be required by federal or state law.
 - 6.2. Follett shall maintain and store backup copies of Customer data at a secure offsite storage or offsite disaster recovery facility.
 - 6.3. Storage, retention and disposition policies for data stored on the platform locally by the Customer on Customer-hosted systems are the responsibility of the Customer.
7. Follett has implemented policies and procedures addressing unauthorized disclosure of confidential Customer information and maintains a corporate Data Security Incident Response Plan.
 - 7.1. In the event of unauthorized disclosure of any student information, Follett will follow its corporate data security incident response plan, which includes notifying affected Customer in a timely and efficient manner in coordination with Follett's internal legal counsel. It is expected that most notifications will occur within 24 hours of authorization by Follett's General Counsel. Follett will provide appropriate data to assist Customer in their efforts to notify affected eligible Students their Parents and Legal Guardians in the case of unauthorized disclosure.