RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Follett School Solutions, Inc. ("Service Provider") on 06/23/2021 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ● No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ● No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ● No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ● No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ● No ○

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ● No ○

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ● No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ● No ○

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ● No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ● No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ● No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ● No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ● No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ● No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ● No ○

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

	Laura Assem
Print Name	Print Name (Roseville City School District)
06-24-2021 10:47:36 GMT	Laura Assem
Signature, Date	Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

See attached

Section 1.7: Internal Security

See attached

Section II.2: Exporting of Student-Created Content

More can be provided upon request. This is an option with the software and follows all guidelines in the attached document.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Follett does not have direct access to the data. The local school administrator would be responsible for making any corrections or updates.

EXHIBITS

Section II.5: Securing Student Data

See attached

Section II.6: Disclosure Notification

Follett follows all state and national regulations in regards to notification.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

See attached

Section III.5: How Student Data is Protected:

See attached

Follett Data Security

Follett is committed to data security and supporting our customers' data privacy needs. As student data collection evolves, Follett continues to provide and enhance the necessary levels of security to ensure your student information is secure and private in our learning management and educational systems.

Protection of individual sensitive and personally identifiable information (i.e. PII) is a priority for Follett. To ensure compliance with all applicable privacy legislation Follett has established policies and processes that focus on the protection of all potentially sensitive customer data. Follett has invested in technologies that support the protection and provide security of data while in transit or at-rest.

Follett's Pledge of Student Privacy

Follett is proud to be one of the first signers of the national Student Privacy Pledge (https://studentprivacypledge.org) regarding the collection, maintenance, and use of student personal information. The pledge states: "School service providers take responsibility to both support the effective use of student information and safeguard student privacy and information security." Follett takes the signing of Student Privacy Pledge seriously and strives to go above and beyond the privacy constructs defined within.

Aspen

Aspen provides several levels of security that control access to your system from people external to your organization, internal to your organization, and even among other Follett products that you are using.

Aspen was architected with security in mind

We built Aspen to include security as a core component of it's design. This design includes a strict adherence to the separation of different layers within the application. Users interact with a presentation layer that is strictly HTML. All business logic operates on the application server in a business layer that is isolated from both the presentation and the database access. Finally, all database access is handled by a third and isolated persistence layer. Thus, between the end user and the actual storage of sensitive data, there are three independent layers in the Aspen application that all play important roles in ensuring only the appropriate data gets to the each user.

The Aspen data model consists of a single database, meaning that data does not need to be replicated to other data stores. Security rules are applied universally to each database instance when it is created, and the database is not accessible from outside the data center firewall. Each Aspen customer has a separate logical database, and each Aspen instance only has the user account of the database for that instance.

Our approach to security at the design level means that typical hacking techniques such as SQL injection and Cross-Site Scripting (XSS) are blocked, not by patches and fixes to vulnerabilities that come out on a periodic basis, but by the basic design of the application and encapsulation of each layer.

Security and penetration tests are routinely run on Aspen to verify that our security is intact. This testing allows us to verify that the security measures we've developed—such as the cross-site scripting protection layer that prevents database access via SQL injection—are working to prevent known attack vectors.

Aspen has multiple levels of data security

All access to the database is managed through the application, and the data is only visible to users with specific rights and permissions. To accomplish this you can apply your data security in a number of ways including; field-level, component-level, record-level or scoping, and navigation security.

User Group Profile and Maintenance

Aspen provides role-based security. Roles are defined and granted privileges to create, read, update, delete, or mass-update (CRUD-M) records in a particular table. There are also business privileges for special operations like archiving a student or accessing teachers' grade books. Roles are then assigned to users. Aspen allows users to be associated with multiple roles and with multiple schools. A user gets the cumulative privileges allowed by those roles.

Audit Reporting of System and Application Access

Aspen has auditing abilities that allow you to review and confirm that your policies are working the way you intended. Aspen includes an audit trail component that can be enabled for any table and field in the Data Dictionary. For each record modified, the audit trail shows who made the change, what was changed (both the original and new values), and when the change was made. Only users with the appropriate privileges to view a record's audit trail history can do so. Aspen also makes use of security roles to restrict users from intentionally deleting data, alerts and prompts to prevent users from accidentally deleting data, and the audit trail to record what data may have been lost.

Aspen complies with FERPA guidelines

The Family Educational Rights and Privacy Act (FERPA) business rules are built into system so that guidelines (for example, teachers can only access student data for students that they teach) is automatically enforced. System-wide searches only show directory info that is within the FERPA guidelines and can be disabled at the discretion of the district. The comparable Canadian privacy act, Freedom of Information and Protection of Privacy Act (FOIPPA), is also supported.

Student-identifiable information is not shared or uploaded to any other systems from Aspen—including other Follett Software Solutions. The ability to share patron data with Destiny exists, but must be explicitly and proactively configured. Student-identifiable information that would not otherwise be stored in Destiny is not shared.

Destiny

Destiny shares many of the same security attributes as Aspen.

The data model consists of a single database; data does not need to be replicated to other data stores.

Each Destiny district has a separate physical database file.

Security rules are applied universally to each database instance.

The database is not accessible from outside the data center firewall in case the Destiny product is housed at the Follett-managed data center.

The database is not directly accessible via the public internet.

All access to the database is managed through the application, and data is only visible to users with specific rights and permissions.

Destiny is routinely tested against attacks using automated acceptance testing, such as exercises and sample data intended to uncover SQL injection vulnerabilities. Authentication methods are exercised through automated unit tests to validate that data access is restricted to users with the appropriate permissions.

Destiny also has multiple levels of supported data security

Follett eBooks and Security

Data Security

All data is securely transmitted over the HTTPS protocol. This includes page content, images, fonts, and user data. All data is then stored into an encrypted data store on the local machine, inside a directory that only that user (and root) has access to. The encryption key to unlock the data is generated locally at the time of the data store creation and stored in the system user's encrypted local store (ELS). Only a combination of our application and that user has access to the encryption key in the ELS. Each book's data is contained in its own secure data store, separate from the main encrypted data store, with its own encryption key stored in the ELS. When the book is removed by the user via Follett Digital reader, its data store is deleted from the local file system, which includes all content, imagery, and fonts.

DRM

We encrypt each book with 128bit AES encryption, and every book has its own unique key. In addition to encrypting the book, we have a voucher mechanism that is also encrypted using 128bit AES encryption and ensures the content is locked to the specific machine it was downloaded to.

Follett eReader

Follett uses a proprietary conversion and encryption process that our Follett readers have been designed specifically to utilize.

About Our Data Center

The Data Center where Follett houses and manages its servers is an approximately 3,000 square-foot, raised-floor facility. Physical access to the data center is controlled by a card proximity reader. Only individuals with a role that requires access to the data center are permitted in the raised floor area. Access to the mechanical space is similarly controlled. A camera system has been installed at the doors to the data center to record entrance and exit to the raised floor and mechanical space. Procedures are in place to log the access to the data center.

Data Center contained server access is similarly controlled with secured access by Follett employees as well as approved designated third party vendors / systems (i.e. development consultants, hardware vendors, SIF agents).

Contact Us

Follett is committed to helping our customers demonstrate the privacy and security of their student data. Our security features are designed to provide physical and digital security and empower districts to develop, enact, and enforce their privacy policies. For more information about our data security, please contact us.