

## **Vendor Statement of Compliance Data Privacy and Protection**

This agreement is entered into between the Roseville City School District ("LEA" or "District") and \_\_\_\_\_ ("Service Provider") on \_\_\_\_\_ ("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

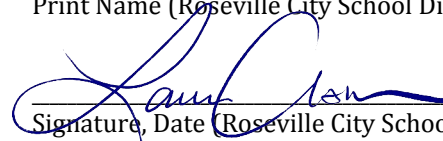
As an authorized representative of my organization, I accept the conditions listed in this document.

Print Name



Signature, Date

Print Name (Roseville City School District)

 10/13/2022  
Signature, Date (Roseville City School District)

## **EXHIBITS**

### **Section 1.6: External Security**

### **Section 1.7: Internal Security**

### **Section II.2: Exporting of Student-Created Content**

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

## **EXHIBITS**

**Section II.5: Securing Student Data**

**Section II.6: Disclosure Notification**

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

**Section III.5: How Student Data is Protected:**

**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?**

The Winsor Learning system is hosted in a Virtual Private Network in aws (Amazon Web Services). The overall structure of aws is based on the concept of Least Privilege. All data is housed in a non-routable, non-public-facing, RDS based Microsoft SQL Server with both encryption during transit (TLS 1.3) and at rest. There are only three methods for accessing the data stored within. The first via the software interfaces we've built for customer-facing users such as your School, the second is via the Right and Role based, non-public-facing, restricted user interface used by the Winsor Learning staff, and finally, there is developer/database administrator access to this database by our networking, security, and development partner, Mindframe, Inc. (hereafter, "Vendor") Security policies such as port-restriction, non-routable ips, web security groups, and in-software username/password/right/role restrictions are in place to protect this RDS instance from both internal and external attacks. All data within is password protected with Least Privilege using non-reversible SHA256-based hashed passwords. Passwords are rotated per our security schedule.

Vendor access to the data is done on an as-needed basis and never at the individual record level. Our Vendor provides maintenance, optimization, backups, disaster recovery, and other related tasks on the database as a whole, not on individual records. Vendor access is restricted to the two DBA/Network Administrators they have on staff, and we have a binding non-disclosure agreement and contract with this Vendor.

District/School data may not be uploaded to the Winsor Learning Digital platform (hereafter, "System"). Administrative or Teacher users are the only user types that have access to add/edit/remove Students from the system. They do this via a web-form on an individual record level. As such, there is no file transfer issue, no file storage issue, or retention policy on upload files as there is not functionality to support uploads. Data entry by these two user types is done via the end-user-facing user interface mentioned above that requires a username(email) and password to access. Additionally, the user must have been proactively granted access to the District/School via a "Kit" or "Seat" for a given product for the purchased term. Once that Kit or Seat expires, access to the student data is revoked. That data is owned at the District/School level, not the user level.

Access to the Administrator/Teacher entered or created data is restricted to only the Administrator user(s) associated with the District/School, and the Teacher for whom the particular Kit or Seat the student is assigned to, while that Kit/Seat is active and valid. Winsor Learning users who have been granted access to support Districts and/or Schools may also access this data if and when they have been requested by the District/School for support. Winsor Learning employees with this access are trained and certify their training to protect the confidentiality of this data at all times.

Backups of the database are performed in an automated fashion on a periodic-basis as per industry standard with a retention period of 7 days. Access to these backups is restricted to our Vendor, and are automatically removed when expired. If and when a District/School requests a purge of their data from our systems, that data will exist in backups for a duration of 7 days past live system deletion, then they will no longer exist in the backups.

Winsor Learning does not print confidential data, unless specifically requested by the District/School for transfer to that school. Physical copies if not sent for some reason, would be shredded as per our internal policy.

Regarding access to our system, no Students have login access, user accounts, or any method to add/edit/delete any data in our system. The 'Login with Google' functionality requires a Teacher or Administrator account be setup in our system before it can be used for SSO (single sign-on). Our SSO follows industry standard OAuth type 2 for SSO and is optional for a given District/School.



Winsor Learning, Inc.  
Data Breach Policy and Communications Plan  
Last Updated Jan 3, 2021

In this policy Winsor Learning is referred to as the "Company". Their customer is referred to as the "Client". In the event of an unauthorized release, disclosure or acquisition of Data that compromises the security, confidentiality or integrity of the Data maintained by the Company the Company shall provide notification to Client of confirmation of the incident, unless notification would disrupt investigation of the incident by law enforcement.

In such an event, notification shall be made within a reasonable time after the incident. Company shall follow the following process:

1. The security breach notification described above shall include, at a minimum, the following information to the extent known by the Company and as it becomes available:
  - a. The name and contact information of the reporting Client subject to this section.
  - b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
  - c. If the information is possible to determine at the time the notice is provided, then either
    - i. the date of the breach,
    - ii. the estimated date of the breach, or
    - iii. the date range within which the breach occurred. The notification shall also include the date of the notice.
    - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
    - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
2. Company agrees to adhere to all federal and state requirements with respect to a data breach related to the Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
3. Company further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Data or any portion thereof, including personally identifiable information and agrees to provide Client, upon request, with a summary of said written incident response plan.
4. Client shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
5. In the event of a breach originating from Client's use of the Service, Company shall cooperate with Client to the extent necessary to expeditiously secure Data.

[Winsor Privacy Notice and Policy](#)

## **Winsor Learning Privacy Policy**

Last Updated December 2<sup>nd</sup>, 2020

This privacy notice and policy applies to the use of the WINSOR LEARNING® web platform (the “Platform”) and the Content, tools and features found here. The Platform is owned by Winsor Learning, Inc., and by using the Platform, you agree to our Privacy Policy as explained below. In summary,

- We do not collect personally identifiable information about you unless you choose to provide that information to us.
- Information you provide us with in connection with your use of the Platform is stored, collected, and used in connection with your and your organization’s use of the Platform.
- Any personal information you provide is protected by reasonable security measures.
- Non-personal information on how you use the Platform may be automatically collected and stored.
- Unless you authorize us in advance, we do not disclose, give, sell, or transfer any personal information to any third party unless required by law.

We do not disclose personal information to third parties for their direct marketing purposes.

### **PERSONAL INFORMATION VOLUNTARILY SUBMITTED**

If you choose to provide us with personal information, we may use that information to provide with the services associated with the Platform, respond to you, and/or get you the help, information, feedback, or services you requested. We retain the information you voluntarily provide to us only for as long as necessary to provide you with the Platform services and/or respond to your question or request, in most cases no longer than three months, or in the case of access to the Platform, as long as needed to provide you with access to and use of the Platform.

### **INFORMATION AUTOMATICALLY COLLECTED AND STORED**

When you use the Platform, we use analytics tools to gather and temporarily store a variety of information about your use. The basic information we collect during your visit includes:

- The name of the domain you use to access the Internet
- The location, date and time of your use of the Platform
- The content and features you have used on the Platform
- The type and version of your Web browser and operating system

We may aggregate this data in order to improve the Platform. The aggregate data is available only to our designated team members who require this information to perform their duties. It is retained only for as long as needed for proper analysis.

### **HOW WE MAY SHARE YOUR INFORMATION**

We may share your personal and other information in the following ways:

- With your employer or contractor who has a paid for use of the Platform

- With our team members who need access to such information to carry out work on our behalf
- If needed to protect rights, property and/or safety, or if needed to respond to the request of law enforcement in cases where we believe disclosure is required and/or in accordance with law
- As requested or directed by you

## **CHILDREN'S INFORMATION**

The Platform may only be used only by educators that have obtained and verified all required parental consent. It cannot be used by children under the age of 18, other than in connection with a teacher's authorized use of the Platform. Teachers who use the Platform have the option to enter, store, and use the first and last name, and student ID (not SSN), of their students who may be under the age of 13. This information is entered only by authorized teacher users of the Platform, and not collected directly by us. We do not disclose any such personal information to any third parties, or use it other than in connection with a teacher's authorized use of the Platform. If you are the parent or guardian of a child under 13 and would like to request that this personal information regarding your child be updated or deleted, or if you'd like to prevent further use of that information on the Platform, please contact us at: 800-321-7585 or at [www.winsorlearning.com](http://www.winsorlearning.com). We will respond to such a request within 30 days of our receipt of the request.

## **WEBSITE SECURITY**

We take reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, and disclosure. For Platform security purposes, we use software to monitor traffic to identify unauthorized use. In the event of law enforcement investigations and as part of any required legal process, information from these sources may be used to help identify an individual.

## **CHANGES TO THIS POLICY**

We may update this policy from time to time. When we do, we revise the "Last Updated" date at the top of this page. We encourage you to check this page periodically for any changes. You acknowledge and agree that it is your responsibility to review this policy periodically and become aware of modifications.

## **CONTACTING US**

If you have any questions about this policy, or your experience with the Platform, or want to notify us of anything, please contact us at: 800-321-7585 or at [www.winsorlearning.com](http://www.winsorlearning.com)

From <<https://www.winsorlearning.com/privacy>>