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 MobyMax ("Service Provider") on 09/19/2019 ("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 ○

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

**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 ○

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

**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 ○

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

**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.

**John Jennings**
Print Name

9.19.19
Signature, Date

Laura Assem, 9/19/19
Print Name (Roseville City School District)

Signature, Date (Roseville City School District)

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

# EXHIBITS

**Section 1.6: External Security**

All exhibits are attached in a separate document.

**Section 1.7: Internal Security**

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

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

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

# 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:**



Reset Form

# MOBYMAX TECHNICAL OVERVIEW

## HOSTING AND UPTIME

MobyMax uses a hybrid hosting model, featuring dedicated database servers in a private network managed by Rackspace. Concurrently, web servers free of user-related data are hosted in the Rackspace cloud using RackConnect v3.0. With this approach, we can scale web servers according to traffic on daily basis, while keeping user data on secure, dedicated machines.

### PHYSICAL DATA CENTER

The Rackspace data center where your data will be hosted is located just outside of Chicago. It meets critical requirements of Tier 3 ratings, with N+1 redundancy or greater across all major infrastructure systems, including generators, UPSs, chillers, and air handlers. Single points of failure are minimized, and proper floor loading is maintained.

Perhaps more importantly, Rackspace adheres tightly to its own internally developed technical change management processes in order to maintain a commitment to 100% uptime. Rackspace has routinely delivered a service level of 99.999% globally, compared to the Tier 3 requirement of only 99.982%. Rackspace has earned the following industry compliance certifications:

- ISO/ IEC 27001
- ISO 14001
- ISO 18001
- ISO 9001
- SOC 1 (SSAE 18)
- SOC 2
- SOC 3
- PCI DSS Level 1
- FedRAMP JAB P-ATO
- NIST 800-53
- FISMA
- NIST 800-171 (“DFARS”)
- CJIS
- ITAR
- FIPS 140-2
- HITRUST

### UPTIME

- In 2018, MobyMax customers were subject to less than one total hour of unplanned, partial service disruption.
- You will experience planned downtime for 12 hours overnight on July 31-August 1 each year for the purpose of resetting the school year. You will be notified several times in advance of this reset.
- In addition to the school year reset, we may have additional planned maintenance over the weekend lasting less than one hour. This happened twice in 2018.

MobyMax
Fix learning gaps.

## BACK-UP PROCESS

One of the big worries of any online solution is the potential for data loss. With MobyMax, this need not be a concern. Here are the safeguards in place to keep you protected:

### REAL-TIME REPLICATION TO PHYSICAL SERVERS

All database servers are replicated in a master/slave configuration to identical dedicated servers. In the event of hardware failure, the system can promote backup server to a “master” role and switch over without any data loss.

### REAL-TIME REPLICATION TO CLOUD

Data is replicated in real time to cloud servers. In case of loss of all dedicated servers, these cloud servers will retain the latest updated data.

### DAILY BACKUPS

A full snapshot of all database servers is taken on a daily basis. This snapshot remains in a ready-to-use state and can be attached to a cloud server for loading in minutes. This is supplemented with a compressed, encrypted daily snapshot of all databases retained for one week. SQL format data backups are used for selected critical data to be accessed and restored in less than 10 minutes in the event of data loss. MySQL logs are backed up on a daily basis and can be used for point-in-time recovery.

### EXTERNAL BACKUPS

As part of our disaster recovery strategy, the SQL format critical data backup is uploaded to the Amazon cloud twice weekly and retained for six months, while the weekly compressed snapshot is retained on Amazon S3 within private buckets for six months.

# DATA SECURITY

Through the course of finding and fixing learning gaps, your teachers and students will be spending a significant amount of time on our website. It stands to reason that you should go to great lengths to ensure you don't have to worry about security risk while that is happening. Here's what we will do to keep your learning community safe:

## SESSION SECURITY AND ACCESS

All network traffic, including data uploads, happens over encrypted channels (SFTP or HTTPS). The private keys for encryption/decryption are password-protected and accessible only to a very limited number of systems engineers. User passwords are encrypted in storage. MobyMax staff will only access data in support of the contract as requested by school or district staff.

## SERVERS

For database servers, the Rackspace engineering team automatically applies the latest security patches provided by the RedHat Enterprise Security Team. On the web server side, security patches are applied weekly using CentOS package update repositories, which provide updated security patches for all relevant operating system tools and applications. The hardware firewall and load balancer are firmware-patched and updated regularly by Rackspace as required by their security maintenance protocols.

## TESTING AND AUDITING

The MobyMax Quality Assurance team regularly tests all functionality, especially authentication, for potential security vulnerabilities. In addition, our development team conducts regular code reviews to find security vulnerabilities such as, but not limited to, SQL injections and cross-site scripting attacks. We conduct similar tests on all third-party software used in the development process prior to integration.

Every new release is tested against the most recent versions of common browsers and operating systems, including desktop and mobile versions.

## DATA RETENTION

At the end of each school year, all data from the previous year is archived in a read-only format for an additional year. After that time, the database is deleted, with all nodes overwritten and permanently cleared.

MobyMax
Fix learning gaps.

## PRIVACY POLICY

Student privacy is just as important to us as it is to you. Our security starts with the data you enter into our program. Only the most basic personal information (name and grade level) is entered into MobyMax.

We never share your information with third parties, with only one exception: with your explicit permission, we may allow educational researchers to access aggregate class information.

### MobyMax does:

- ✅ Comply with COPPA and FERPA
- ✅ Enable teachers to replace student names with nicknames or aliases
- ✅ Enable parents/guardians to view a student's progress, time spent, and lesson data
- ✅ Constantly monitor the security and integrity of data
- ✅ Allow student accounts to be soft-deleted or permanently deleted

### MobyMax does not:

- 🚫 Collect sensitive student information such as address, social security #, or date of birth
- 🚫 Sell or rent user information
- 🚫 Display commercial advertising

### COPPA AND FERPA

We are committed to working with our Users to comply with laws, rules, and regulations governing the use and protection of Student Records, including the Children Online Privacy Protection (COPPA) and the Family Educational Rights and Privacy Act (FERPA) and their implementing regulations, applicable state laws, and statues governing Student Records we receive from Users. As such, MobyMax is committed to protecting the security, confidentiality,

and integrity of Student Records that we receive from Users, as well as to protecting against unauthorized access or anticipated threats.

### Personal Identification Information

We may collect personal identification information from Users in a variety of ways, including, but not limited to, when Users visit our Site, subscribe to email alerts, and in connection with other activities, services, features or resources we make available on our Site. Users may be asked for, as appropriate, name, email address, mailing address, and phone number. Teachers or administrators choose which identifying information to include as the students' first name, last name, username, password, and ID. We never collect sensitive information such as student addresses, social security numbers, or dates of birth. We permit teachers or administrators to replace student first and last names with nicknames or aliases. Users may, however, visit our Site anonymously. We will collect personal identification information from Users only if they voluntarily submit such information to us. Users can always refuse to supply personal identification information, except that it may prevent them from engaging in certain Site-related activities. Users can correct any erroneous personal information by emailing support@mobymax.com or calling (888)793-8331.

### Non-Personal Identification Information

We may collect non-personal identification information about Users whenever they interact with our Site. Non-personal identification information may include the browser name, the type of computer and technical information about Users' means of connection to our Site, such as the operating system and the Internet service providers utilized and other similar information.

### Web Browser Cookies

Our Site may use "cookies" to enhance Users' experience. A User's web browser places cookies on their hard drive for record-keeping purposes and sometimes to track information about them. Users may choose to set their web browser to refuse cookies, or to alert them when cookies are being sent, but this may result in some parts of the Site not functioning properly.

### How We use Collected Information

MobyMax may collect and use Users' personal information for improving the User’s experience or sending periodic emails. Students shall not receive email alerts containing any advertising or

product information. We may use information in the aggregate to understand how our Users as a group use the services and resources provided on our Site and so that we may improve our Site. If the User decides to opt-in to our email alerts, they will receive emails that may include company news, updates, related product or service information, etc. If at any time the User would like to unsubscribe from receiving future emails, we include detailed unsubscribe instructions at the bottom of each email.

## Property and Control of Student Data

All student records and data continue to be the property of and under the control of the local educational agency. Students are able to access, print, and otherwise retain any student-generated content by accessing it through various channels in their student accounts. If teachers provide parents or guardians with login instructions, they are able to access basic student MobyMax data like progress, lessons completed, and time spent.

## How We Protect Your Information

We adopt appropriate data collection, storage and processing practices, and security measures to protect against unauthorized access, alteration, disclosure, or destruction of your personal information, username, password, transaction information, and data stored on our Site.

## Sharing Your Personal Information

We do not sell, trade, or rent Users' personal identification information to others. We will not allow unrelated third parties to use your personal information for any reason without your consent. We may share generic aggregated demographic information not linked to any personal identification information regarding visitors, and users with our business partners for the purposes outlined above. We may disclose and share personal information with (1) our group companies or any entity which acquires any part of our business, (2) with our service providers (including, for example, suppliers who develop or host our sites), (3) with single sign-on providers that you use to access our software, (4) roster services that you use to update your student and teacher rosters, and (5) if required or permitted by law with other third parties with your consent.

## Procedure for Unauthorized Records Disclosure

In the event of a breach or unauthorized disclosure of student records that would be subject to disclosure under applicable federal or state law has occurred, MobyMax will take prompt and appropriate steps to mitigate further breach or release of student records, provide notice to the affected User promptly and without reasonable delay, and work with the affected User to provide information and assistance necessary to comply with any notification to parents, legal guardians, or students, as is required by applicable law.

## CONTRACT TERMINATION/COMPLETION

Following expiration or termination of the agreement under which the User purchased access to the MobyMax web-based products or services, and upon receipt of written request from the User, MobyMax will destroy or, if agreed, return to the User, the Student Records in its possession within a commercially reasonable period of time. At any point, teachers or administrators are able to soft-delete or permanently delete student accounts and data. For clarity, data generated by MobyMax or our products that is in aggregate, or that is anonymized (i.e., personally identifiable information has been removed) may be retained by MobyMax and used for product improvement purposes.

## CHANGES TO THIS PRIVACY POLICY

We may update this Privacy Policy at any time. When we do, we will revise the updated date at the bottom of this page. If we change the policy in a material manner, for example, if we seek to use personal information in a materially different way than we had previously, we will provide at least 30 days' notice to you so that you have sufficient time to evaluate the change in practice. Of course, you can always opt out by deleting your account before the changes take effect.