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, Executive 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 Appointlet LLC ("Service Provider") on 9/28/2022 ("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 ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Executive 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, Executive 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 ○

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Executive 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.

Jared Morse
_____
Print Name

_____
Signature, Date

Laura Assem
_____
Print Name (Roseville City School District)

9/29/2022
_____
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, Executive Director of Technology

EXHIBITS

Section 1.6: External Security

Learn more here: https://www.appointlet.com/security-measures

Section 1.7: Internal Security

Learn more here: https://www.appointlet.com/security-measures

Section II.2: Exporting of Student-Created Content

You can reach out to our support about any data export needs. We also have a feature that allows you to export all meeting data here. Learn more here: http://kb.appointlet.help/en/articles/4220737-export-booking-data-as-a-spreadsheet

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

Users can correct information using the email in they receive after scheduling, or an admin can update their information in the dashboard UI.

ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

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

Laura Assem, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data

https://www.appointlet.com/privacy-policy
https://www.appointlet.com/security-measures

Section II.6: Disclosure Notification

Our current policy dictates that we will notify you of any data breach and we will assist you in notifying your meeting participants if desired, but we don't reach out directly to them.

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

Our privacy policy dictates we will only release information to you, the account holder, after which you can release that information as needed.

Section III.5: How Student Data is Protected:

https://www.appointlet.com/privacy-policy
https://www.appointlet.com/security-measures

Reset Form

Appointlet

Privacy Policy

Last Updated: May 21, 2020

At Appointlet ("Service") we take privacy and the security of your data very seriously, so we'd like to be transparent with you about how we collect, utilize and protect it.

A lot of what you'll read in this document is designed to address various laws and regulations such as the GDPR and CCPA. That said, we'd like to take a moment to share a few philosophies that guide how we treat data and privacy here at Appointlet now and going forward:

- Data you provide us, or that is collected on your behalf, is owned entirely by you and will be available to you on demand as well as removed on demand.
- We consider data a liability and only collect and share the minimum amount required to provide you with a great service.

We've made an effort to make this document as clear and easy to understand as we can, but if you have any questions, please don't hesitate to reach out.

If you do not agree with this policy, please do not access or use our Service.

Who this policy applies to

- Our Customers who have signed up for our Service

- End-Users of our Customers who interact with our Service

What this policy covers

The goal of this policy is to help you understand:

- What data we collect from you
- What data we collect automatically
- How we use data we collect
- How we share data we collect
- How we store and secure data we collect
- How you can access and manage your data
- Other important privacy information

What data we collect from you

We collect data about you when you provide it to us by using our Service, as described below.

- Account and profile information – We collect information about you when you register for the Service, such as name and email address, as well as other various settings and contact information.
- Content you provide through our Service – When using our Service we collect various information about your company and the Services you provide to your customers.
- Information you provide through our support channels – If you elect to use our customer support, we will collect any information you choose to share with us.
- Payment information – If you decide to upgrade to one of our premium plans, we will collect payment information such as credit card details.

What data we collect automatically

By using the Service there is some information we get from you automatically.

- Your use of the Service – When you use the Service we track certain information to help us

better understand how you're using the Service, such as what features you use and how frequently.

- Device and connection information – We collect various pieces of information about your network connection, such as IP address, so that we can protect the Service against abuse. We also collect information about your device such as what type it is (laptop, tablet, etc) and what browser you're running so that we can improve the quality of the Service, as well as resolve any issues you may encounter.
- Cookies and other tracking technologies – Our Service uses cookies so that we can recognize you after you sign in. They also help us identify you when resolving issues.

How we use data we collect

How we use your data depends on how you utilize the Service. These are the purposes for which we use your data.

- To provide the Service and customize your experience – We use your information to provide the Service and tailor it to your needs.
- For product development and research – To improve our Service, we will often look at our customer data to better understand what it is you're using the Service for. For example, if we find that customers are using certain web conference providers, we will use that information to develop integrations with those services.
- For customer support – We use your information to resolve technical issues and to respond to requests for assistance.
- For safety and security – We use information about you to verify your account and to monitor for suspicious or fraudulent behavior.

How we share data we collect

Our Service inherently requires sharing some of your data with other Service users and some third parties in order to function.

Sharing with other Service users

- For scheduling – We must share some of your data with them so that they know what they're scheduling and with whom.

- For administration – For certain kinds of accounts we will share your information with the administrator(s) of the account. For example your name and email are shared with your account administrator.

Sharing with third parties

Third parties that we share data with do so under direct instruction from us, and abide by policies designed to protect your information.

- Service providers – We work with a few third-party service providers to enable customer support, hosting/development, payment processing and communications.
- Integration partners – If you choose to take advantage of our various integrations, we will share the minimum amount of data with them to perform the desired task.
- Legal / law enforcement – In exceptional circumstances we may share information about you with a third party if we believe sharing is necessary to comply with applicable laws, regulations or governmental requests.

How we store and secure data we collect

We use extreme care when handling your data and always use industry standards where applicable.

How we store and transmit data

- We store your data in a Amazon Web Services data centers located in the United States. You can read more about their physical security here.
- We always use secure connections (TLS/SSL) to transmit data in between Service users and third parties.
- We encrypt all data stored in our databases at rest.
- Payment data is stored with our billing provider, which is PCI-DSS compliant
- Access to our database is limited to a select group of employees.

We make an effort to protect your data through a number of security measures, however please remember that no system is 100% secure.

How long we keep data

We keep user data for varying lengths of time, depending on the type of data and how you've configured our Service.

- Account data – We retain account data for the lifetime of the account, as it's mandatory to use the Service. We also retain any data necessary to comply with legal obligations and resolve disputes.
- Content you provide – If your account is deactivated, we retain some of your content so that other Service users that you have collaborated with will be able to continue using the Service in an expected manner.
- Booking data – By default we retain booking data for the lifetime of the account. However you can configure our Service to automatically delete booking data a certain period of time after it is no longer useful to you.
- Payment data – We retain payment data for the lifetime of the account as it's mandatory in order to use our Service.

Notification of security breach

We will notify you within 72 hours of becoming aware of a security breach or configuration weakness which could have allowed your data to be exposed.

How you can access and manage your data

We strongly believe in giving you access to export or delete your data at will.

Your rights

You have several rights that can be exercised at any time:

- The right to request a copy of your data in a structured, electronic format
- The right to object to our use of your data
- The right to request deletion of your data ("Right to be forgotten")

In some cases we may not be able to comply with requests, such as a situation where compliance would result in another user's personal data being exposed, or where we are prohibited by law.

In situations where you have asked us to share your data with a third party, you may need to contact those parties to have your request fulfilled.

If you have unresolved concerns or feel your rights were infringed, you may have the right to complain to a data protection authority in your country of residence.

How to make a data request

In some cases we have automated tools to help you obtain or delete your data, and in other cases you'll need to make a data request to our customer support team.

To make a data request, please login to your account and use the customer support tools. Alternatively, you can send us an email from the address you used to create the account.

In some situations we may ask for additional proof of identity so we can ensure the privacy of our other customers.

How to access and update your data

Our Service allows you to access and update your information from within the Service. For example, you can access your profile information from your account, as well as booking data and other content you had previously supplied us.

How to delete your data

If you would like to have account data deleted, please make a data request. Please note that we may need to retain certain data within your profile for record keeping purposes or to comply with our legal obligations.

Opt out of communications

You may opt out of receiving promotional communications from us by using the unsubscribe link at the bottom of each email. Even after you opt out of promotional emails, you will continue to receive transactional emails from us.

Data portability

Data portability is the ability to obtain some of your data in a format you can move from one Service to another. Should you request it, we will provide you with an electronic file of your account data.

Other important privacy information

Our policy towards children

Our Service is not designed for individuals under 16 years of age, and we do not knowingly collect personal information from them.

Changes to this policy

We may change this policy from time to time. Any changes will be posted to this page, and if they are significant, we will notify you via email and within the Service. We will also keep previous versions of this policy which are available upon request. You are advised to review this policy periodically for any changes.

If you disagree with any changes to this policy, you will need to stop using the Service.

Contact Us

If you have any questions, concerns, or data requests, please reach out by logging in to our Service and using the customer support tool there, or by emailing us at help+privacy@appointlet.com.

English

General

Teams

Features

Pricing

Login

Start free

Use cases

Sales

Customer Success

Education

Interviews & HR

Company

About

Blog

Support

Affiliate Program

Partnerships

Integrations

Google Calendar

Office 365

Zoom

View All

Privacy Policy Terms of Service

Security Disclosure Policy

Last Updated: December 18, 2021

Data security is a top priority for Appointlet, and we believe in working with skilled security researchers to identify any potential weaknesses in our technologies.

If you believe that you've found a security vulnerability in Appointlet's service, please notify us by emailing any and all information about the issue to security@appointlet.com, and we will work to resolve the issue promptly. Please allow us one week to acknowledge. We try and resolve critical issues within 1-2 days and less critical issues within 2-3 weeks.

Please refrain from:

- Denial of Service (DoS) attacks
- Spamming
- Social engineering or phishing of Appointlet employees or contractors
- Anything else that impacts the service for our users

Thank you for your help in making Appointlet a safe and secure service.

Appointlet

Security Measures

Last Updated: December 18, 2021

Personnel Security

- **Confidentiality** – Appointlet personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Appointlet's internal policies.
- **Security Education and Awareness Training** – Appointlet personnel are required to attend security and privacy training upon hire and annually thereafter.

Organizational Security

- **Access Controls** – Appointlet implements access provisioning based on the principle of least privilege and access removal controls promptly on termination. These controls are reviewed company-wide twice annually.
- **Multi-factor Authentication (MFA)** – Appointlet employs multi-factor authentication for access across our production environment and internal systems containing Customer Data.
- **Passwords** – Appointlet requires and enforces password complexity requirements where passwords are employed for authentication (e.g., login to workstations). These requirements include restrictions on password reuse and sufficient password strength.
- **Information Security** – Appointlet personnel are required to acknowledge and comply with

Appointlet Information Security policies and standards. Noncompliance is subject to disciplinary action, up to and including termination of employment.

- **Monitoring and Incident Response** – Appointlet maintains incident detection capabilities and a documented incident response program. In the event of an incident, Appointlet will promptly take reasonable steps to minimize harm and secure Customer Data.

Data Hosting & Practices

- **Industry Standard Encryption** – Data in transit is encrypted using TLS 1.2+, and data at rest is encrypted using AES-256. Appointlet hashes user passwords with PBKDF2 before storing them in an encrypted database.
- **Retention and Deletion** – Appointlet maintains backup data for up to 7 days after any data has been deleted by an end user. After that period the data is permanently deleted.
- **Storage** – Appointlet stores data in a multi-tenant environment hosted on AWS servers and logically isolates Customer Data.
- **Data Centers** – Appointlet hosts data on Amazon Web Services (AWS), which maintains internationally recognized world-class compliance certifications and reports. AWS maintains industry-leading security practices, offers state-of-the art environmental and physical protection for the services and infrastructure that comprise Appointlet's operating environment.
- **Backups** – Appointlet conducts periodic database backups. Backups are retained for 7 days during the normal course of operations.
- **Replication** – Appointlet also replicates databases and database backups in alternate availability zones. We perform regular backups and restoration testing.
- **Redundancy** – Appointlet's infrastructure has been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. This design allows Appointlet to perform maintenance and improvements of the infrastructure with minimal impact on the production systems.

Network Protection

- **Firewalls** – Appointlet configures firewalls according to industry best practices and unnecessary ports and protocols are blocked by configuring AWS Security Groups and NACL (Network Access Control Lists). Configurations are regularly monitored using automated cloud

security posture management tools.

- **Monitoring, Logging, and Alerting** – Appointlet logs application logs to monitor for any suspicious activity. This is done using an SIEM (Security Incident and Event Management) tool. All alerts are triaged by Appointlet's Security Team and a security incident is raised after log introspection.

Subprocessors

- **Confidentiality** – Appointlet takes appropriate steps to ensure our security posture is maintained by establishing agreements that require subprocessors and service organizations to adhere to confidentiality commitments.

Security Certifications and Reports

- **Penetration Testing** – Appointlet engages with independent third party firms to conduct application-level and network-level penetration tests at least annually. Results of these tests are shared with senior management, triaged, prioritized, and remediated in a timely manner.
- **Independent Security Disclosure Program** – Appointlet runs a "Bug Bounty" program for independent security auditors designed to allow security professionals to disclose security issues through appropriate channels so that we can resolve them promptly. More information can be found here.

English

General

Teams

Features

Pricing

Login

Start free

Use cases

Sales

Customer Success

Education

Interviews & HR

Company

About

Blog

Support

Affiliate Program

Partnerships

Integrations

Google Calendar

Office 365

Zoom

View All

Privacy Policy Terms of Service

Appointlet

Subprocessors

Last Updated: December 18, 2021

Subprocessor	Location	Purpose/Notes
Amazon Web Services	USA	Hosting
Amplitude	USA	Analytics
AppCues	USA	Analytics
Email Octopus	USA	Email Newsletters
Facebook	USA	Advertising
Google	USA	Business Operations, Analytics, Advertising
Heroku	USA	Hosting
Intercom	USA	Customer Support
Logentries	USA	Platform Monitoring
LogRocket	USA	Customer Support, Analytics
Memcachier	USA	Hosting
Netlify	USA	Hosting
New Relic	USA	Platform Monitoring
Notion	USA	Business Operations
Postmark	USA	Transactional Emails
Price Intelligently	USA	Analytics
Redis Cloud	USA	Hosting
Slack	USA	Business Operations
Tapfiliate	Ireland	Affiliate Program
UploadCare	Canada	Hosting

Appointlet

Terms & Conditions

Last Updated: May 15, 2018

Please read these Terms and Conditions ("Terms", "Terms and Conditions") carefully before using the https://www.appointlet.com website (the "Service") operated by Appointlet, LLC ("us", "we", or "our").

Your access to and use of the Service is conditioned on your acceptance of and compliance with these Terms. These Terms apply to all visitors, users and others who access or use the Service.

By accessing or using the Service you agree to be bound by these Terms. If you disagree with any part of the terms then you may not access the Service.

Termination

We may terminate or suspend access to our Service immediately, without prior notice or liability, for any reason whatsoever, including without limitation if you breach the Terms.

All provisions of the Terms which by their nature should survive termination shall survive termination, including, without limitation, ownership provisions, warranty disclaimers, indemnity and limitations of liability.

Links To Other Web Sites

Our Service may contain links to third party web sites or services that are not owned or controlled

by Appointlet, LLC.

Appointlet, LLC has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third-party web sites or services. You further acknowledge and agree that Appointlet, LLC shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods or services available on or through any such web sites or services.

We strongly advise you to read the terms and conditions and privacy policies of any third-party web sites or services that you visit.

Governing Law

These Terms shall be governed and construed in accordance with the laws of the United States of America, without regard to its conflict of law provisions.

Our failure to enforce any right or provision of these Terms will not be considered a waiver of those rights. If any provision of these Terms is held to be invalid or unenforceable by a court, the remaining provisions of these Terms will remain in effect. These Terms constitute the entire agreement between us regarding our Service, and supersede and replace any prior agreements we might have between us regarding the Service.

Billing

Paid Subscription Cancellation Policy

Paid subscriptions will automatically renew for the same subscription period unless cancelled by the account owner before the end of that current subscription period. You have the option to cancel your paid subscription at any time via the in-app billing modal. Alternatively, you can contact customer support in app or by email (help@appointlet.com) with your cancellation request.

When a cancellation is issued, the downgrade from premium to free is scheduled for the time of subscription renewal. Until end of cycle, all premium features will remain active for the organization.

Refund Policy

Organizations are eligible for a full refund on monthly or annual premium paid subscriptions provided that no bookings have been made since the subscription started and the account owner makes that request within 7 days of the current subscription cycle. For annual payment cycles, a

cancellation fee of 10% of the total charge will be assessed, after which the remaining refund will be processed within 1-10 business days.

Legacy Plans

As pricing models change at Appointlet, existing customers will retain their existing subscription cost until they request to move to the current plan or until Appointlet eliminates that plan. If a plan is eliminated, organization owners will receive at least 30 days advanced notice with details regarding the new pricing structure.

Changes

We reserve the right, at our sole discretion, to modify or replace these Terms at any time. If a revision is material we will try to provide at least 30 (change this) days notice prior to any new terms taking effect. What constitutes a material change will be determined at our sole discretion.

By continuing to access or use our Service after those revisions become effective, you agree to be bound by the revised terms. If you do not agree to the new terms, please stop using the Service.

Contact Us

If you have any questions about these Terms, please contact us at help+tos@appointlet.com.

English

General

Teams

Features

Pricing

Login

Start free

Use cases

Sales

Customer Success

Education

Interviews & HR

Company

About

Blog

Support

Affiliate Program

Partnerships

Integrations

Google Calendar

Office 365

Zoom

View All

Privacy Policy Terms of Service