SignalVine

Signal Vine's Platform Security and Privacy

The Signal Vine platform is 100% compliant with federal communications and data privacy regulations. It's designed to protect your student data from threats by applying industry-standard security controls at every step. The platform meets the Family Educational Rights and Privacy Act (FERPA) standards and is used by the US Department of Education, the military, and hundreds of higher education institutions. Your data is safe with Signal Vine.

TCPA

The FCC enacted the Telephone Consumer Protection Act (TCPA) to crack down on unsolicited marketing messages. The Signal Vine Text Messaging Platform was designed from the beginning to fully comply with TCPA regulations.

An important clause from the policy for most of our customers is, "For non-commercial, informational texts (such as those sent by or on behalf of tax-exempt non-profit organizations, those for political purposes, and other noncommercial purposes, such as school closings), your consent may be oral." Text messages must include information about the following:

- Who is sending the message: Simply identify yourself and your organization in your first message to students to fulfill this requirement.
- A physical address: Signal Vine provides your organization with local long-form phone numbers, which comply with this requirement.
- A method to "unsubscribe": Any student who texts back "stop" or "cancel" will automatically be opted out of future text messages.

Ask your Customer Success Representative for help crafting opt-in or opt-out language.

FERPA

The Signal Vine Text Messaging Platform is fully compliant with the US Department of Education's Family Education Rights and Privacy Act (FERPA). The platform logs all message history, encrypts communications, and securely protects all data. Most organizations that use the text messaging platform only include "directory" information in their text messages, such as students' names. It is important to note that this directory information does not require consent to adhere to FERPA laws. Signal Vine provides controls to ensure that this protected information is only available to the appropriate users.

COPPA

The Federal Trade Commission's Children's Online Privacy Protection Rule (COPPA) requires parental consent before communicating with students under the age of 13. Most of Signal Vine's customers do not work with or communicate with students under the age of 13. For those who wish to communicate with students younger than 13, proof of written parental consent is required. Your Customer Success Representative can help you draft language for a parental consent form if needed.

Higher Ed compliant

The Signal Vine platform is 100% compliant with federal communications and data privacy regulations. It is designed to protect your student data from threats by applying industry-standard security controls at every step. Built upon HIPAA compliance, the platform meets FERPA standards and is used by the US Department of Education, the military, and hundreds of higher education institutions. Your data is safe with Signal Vine.

Privacy and Security Details

Application Infrastructure

The Text Messaging Platform is a distributed, fault-tolerant (i.e., if one component fails, back-up equipment will ensure the platform still operates), cloud-based application that can scale vertically and horizontally based on the amount of demand, giving you the performance you need during peak times. Only message content and the recipient phone number are shared with our SMS providers. No other customer data is accessible outside of the platform. The platform only allows HTTPS, which is a secure connection from users. It's a client of our REST API (our programmer's toolkit) and provides a user interface for reading and writing program data.

The platform is hosted on a virtual private cloud (VPC) in Amazon Web Services (AWS). None of the servers running the platform are directly accessible to the internet and are protected by a Bastion Host that serves as a "locked door" to protect our VPC. When employees need access to servers, they use private key encryption to tunnel through the Bastion Host to reach the servers behind them.

Signal Vine relies on AWS elastic load balancers and elastic IP to provide high availability to the platform. They work by redirecting requests to multiple servers to provide a lag-free experience. Amazon Route 53 provides Domain Name Services (DNS).

The platform is protected by AWS Shield Standard, which is a managed Distributed Denial of Service Attacks (DDoS) protection service that safeguards the Signal Vine web application from malicious activity.

AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and lag that would affect users who are trying to access our service. The platform is stored in five data centers distributed throughout North America.

All services (web servers, database, search) have redundancies (duplicate hardware and software) for high availability.

The platform is accessed over Secure Socket Layer (SSL) with 128-bit encryption and authentication. The platform servers do not accept non-encrypted requests.

SignalVine

Encryption

All data is encrypted both at rest and in transit. Different encryption schemes are used for different types of data, depending on the need. For example, passwords are encrypted using a Bcrypt algorithm and SHA-256 encryption. Additionally, data is only sent using 128-bit authentication. All data is encrypted and delivered by HTTPS. Signal Vine does not support insecure connections to the platform.

Data Security

All data is partitioned by account and program, which provides row-level security to authorized users. This means that each account and application is isolated from all others. The design of the platform enforces restricted access levels and does not allow unauthorized access to data. Each user is assigned a partition key and can only access data in the partition to which they are assigned.

User passwords are encrypted using a Bcrypt hashing function and a single-use salt, which is not stored. This means that encrypted passwords are extremely secure. The platform backs up data nightly and ships transaction logs to allow for a point in time recovery to within 15 minutes of when the database goes down. The database is not accessible directly via the internet. It is only accessible via a private network interface connected to the data center.

As noted above, the platform is hosted on a group of separate, secure application servers. All servers can only be accessed using key-based authentication (a 2048-bit RSA key pair). Signal Vine employs access control policies to secure appropriate access and ensure that personally identifiable information (PII) and all data is protected by encryption. Signal Vine employs highly restrictive network access and a rigorous data backup protocol. In addition, an activity log is monitored when data is exported.

Compliance with State and Federal data privacy regulation is ensured through periodic peer review of compliance laws and ops/coding practices, procedures, and implementation.

Application Security and Case Management

Customers control staff access to student profile and message data by assigning security roles to users. There are currently three supported roles:

- **Account Administrator.** Access to view and manage all programs, groups, and students in an account. Account Administrators can invite users to the platform and can view and revoke all account users' access to the platform. They have all permissions available to users at a lower access level.
- **Program Administrator.** Access to view and manage specific programs and their associated students within an account, which is determined by an Account Administrator. Program Administrators can invite users to the platform (with Program Administrator permissions or lower). They can view and revoke access to any user with access to the programs they administer. They have all permissions available to users at a lower access level.
- **Counselor.** Access to one or more groups within one or more programs. Counselors can only view messages and manage the data associated with students belonging to the Counselors' assigned groups.

SignalVine

Signal Vine GDPR Compliance Summary

Our Commitment

Signal Vine is committed to ensuring the security and protection of the personal information that we process and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by strong data protection principles. However, we recognize our obligations in updating and expanding this program to meet the demands of the GDPR.

We are dedicated to safeguarding the personal information under our control and in developing a data protection program that is effective, fit for purpose and demonstrates an understanding of and appreciation for all existing regulations. Our preparation and objectives for GDPR compliance have been summarized in this statement and include the development and implementation of revised data protection policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How We Prepared for the GDPR

Signal Vine, Inc. already has a consistent level of data protection and security across our organization. While our company and our customers are based in the United States, it is our aim to be fully compliant with the GDPR in order to safeguard the information we store. Our preparation has included the following:

- **Information Audit** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- **Policies & Procedures** - revising data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including the following:
    - **Data Protection** – our main policy and internal procedures for data protection have been adjusted to meet the standards and requirements of the GDPR, with a dedicated focus on privacy by design and the rights of individuals.
    - **Data Retention & Erasure** – we have updated our retention policy and schedule to ensure that we meet the 'data minimization' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply, along with any exemptions, response timeframes and notification responsibilities.

  - **Data Breaches** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
  - **Subject Access Request** – we have added new SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.
- **Privacy Policy** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

Data We Store

Signal Vine stores personal and educational data on behalf of our customers, which is used to segment and personalize outgoing text messages from our customer institutions. The data that is stored varies by institution and is governed by agreements between the recipient and that institution.

All records in the Signal Vine database must have a mobile phone number, which is used to send messages to the recipient. Additionally, the following fields are standard fields that most (but not all) customers collect:

- First Name
- Last Name
- Timezone

This information is used to identify the recipient and personalize the messages that the recipient receives.

Additionally, customers may store any additional personal profile information that the deem necessary to segment and personalize their outgoing messages. Signal Vine does not directly control what information is stored, but will ensure that the information is secure. We respect all requests for deletion or update, regardless of the information stored.

Data We Collect

Messaging

As messages are exchanged between our customer institutions and their messaging recipients, Signal Vine collects and stores data related to those transactions, including (but not limited to):

- Mobile phone number
- Mobile phone carrier
- Mobile phone country code
- Message content
- Message direction
- Message delivery status
- Message delivery error code, if present
- Message delivery time

This information is used to ensure that messages are being delivered correctly, to troubleshoot any issues and to display the conversation within our application. Additionally, message content may be analyzed to look for common questions or responses to identify areas that institutions may want to automate or otherwise address. When analyzing in this manner, only the message content is analyzed. Recipient name or personally identifiable information is not used in this analysis.

Usage

Data on usage of the Signal Vine application by customers is collected, including when users access the platform, what they access, what actions they perform and what browser or device they are using. Only users of the Signal Vine platform are included in this collection - this does not extend to recipients of messages.

This data is used to support users, to analyze the platform for performance and to plan additional features. This data is only available to members of the Product, Customer Success and Engineering teams within Signal Vine and is not shared with third-parties.

Marketing

Signal Vine would like to send you information about services and resources of ours that we think you might like. If you have agreed to receive marketing, you may always opt out at a later date.

You have the right at any time to stop Signal Vine from contacting you for marketing purposes. You can opt out by selecting the option in any communication you receive from Signal Vine.

SignalVine

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website of an individual's right to access any personal data that Signal Vine, Inc. processes about them. The individual has the following data subject rights:

- The right to request what personal data we hold about them
- The right to request the purpose(s) of the data processing
- The right to request the categories of personal data concerned
- The right to request to whom the personal data has or will be disclosed to
- The right to request how long the individual's personal data will be stored for
- The right to request the source of the individual's personal data
- The right to request to correct incomplete or inaccurate personal data
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from Signal Vine, Inc. and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organizational Measures

Signal Vine, Inc. takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorized access, alteration, disclosure or destruction and have several layers of security measures.

None of the servers running the Signal Vine platform are directly accessible to the internet. These servers are protected by a Bastion Host that serves as a firewall to protect our Virtual Private Cloud (VPC). When employees need access to servers, they use private key encryption to tunnel through the Bastion Host to reach the servers behind them. The platform is accessed over SSL with 128-bit encryption and authentication. Platform servers do not accept unencrypted requests.

All servers can only be accessed using key-based authentication (a 2048-bit RSA key pair). Signal Vine employs access control policies to secure appropriate access and guarantee that personally identifiable information (PII) and all data is protected by encryption. Signal Vine employs highly restrictive network access and a rigorous data backup protocol.

Signal Vine addresses and tests for the Open Web Application Security Project (OWASP) Top 10.

Cookies

Cookies are text files placed on your computer to collect standard Internet log information and visitor behavior information. When you visit our websites, we may collect information from you automatically through cookies or similar technology. For more information, visit all aboutcookies.org.

Our Company uses cookies to improve your experience on our website, including the following:

- Keeping you signed in
- Understanding how you use our website

Privacy Policies of Other Websites

The Signal Vine website contains links to other websites. Our privacy policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

Changes to Our Privacy Policy

Signal Vine keeps its privacy policy under regular review and places any updates on this webpage. This privacy policy was last updated on January 7, 2020.

SignalVine

Disaster Recovery Business Continuity

Signal Vine has developed and implemented a tested set of processes to ensure any outage or service interruption is managed in a timely manner. This document outlines these procedures.

Disaster Recovery

Signal Vine's Text Messaging Platform is hosted in a secure facility with Amazon Web Services (AWS). The platform is stored in five data centers distributed throughout the Northern Virginia AWS region.

Signal Vine has two database servers with AWS: primary and replica. If anything happens to the primary database, the replica server will take over and become the new primary. Signal Vine's data replication strategy provides a five minute recovery point objective (RPO) and a one hour recovery time objective (RTO). In addition, Signal Vine keeps daily AWS backups in a separate data center and region in case the availability zone is affected and both primary and replica databases are lost (a catastrophic event). The platform will survive this scenario with a 24 hour RPO and an 8 hour RTO. Recovery can take place at any time.

The disaster recovery process ensures that Signal Vine will notify customers as soon as an incident is detected.

Business Continuity

Platform. Signal Vine has a hosted, managed data center that can run without our involvement. Signal Vine's back office systems are all indexed and searchable.

Personnel. Signal Vine's Engineering and DevOps staff provide multiple layers of oversight and redundancy. Oversight roles elevate to the Chief Financial Officer and ultimately the CEO.

Signal Vine, a Delaware corporation, has a board of directors and external investors to help assure that the company remains a going concern.

Insurance. Signal Vine has multiple insurance policies and plans in place to guarantee that the business is covered in the case of unexpected events. These events may include loss of key personnel or an insurance claim that might disrupt the normal operation of the business.

SignalVine

Continuity Test Results

Signal Vine restores backups to a testing environment every day. Signal Vine constantly verifies that the backups used in event of catastrophe are usable. There is tooling in place to create a database from those backups.

Signal Vine can spin up a new environment with its servers and support services within minutes. This capability is tested multiple times per day.

Signal Vine regularly performs vulnerability assessments and penetration tests on the infrastructure and platform. An independent assessment will be performed and the results will be shared if requested by a customer.

Third Party Access to Data

Signal Vine does not disclose data to any third party except where the disclosure is a) required for the sending of an account's text messages, or b) required by law pursuant to a subpoena.

Data is encrypted both at rest and in transit, so Signal Vine's technology providers do not see customer data, unless Signal Vine explicitly grants access.

This encryption also protects against accidental disclosure or malicious attacks.

How to Contact Us

If you have any questions about Signal Vine's privacy policy, the data we hold on you, or you would like to exercise one of your data protection rights, please do not hesitate to contact us.

Email us at contact@signalvine.com

Call us at (703) 480-0278

Or write to us at 811 N. Royal St., Alexandria, VA 22314