Remind's approach to data security

REMIND IS BUILT FOR EDUCATION, and the security of personally identifiable information and other data is one of our top priorities. Effective learning involves educators, students, and parents—a support network that's built on a foundation of trust and accountability.

At the school and district levels, this requires complying with regulations like **FERPA** and **COPPA**. As part of our commitment to privacy in the school environment, Remind has obtained iKeepSafe certification for the FERPA Assessment, COPPA Safe Harbor Program, and California Student Privacy Badge. To meet these program guidelines as well as our own rigorous standards, Remind employs two kinds of security features: those that are user-facing, and those that are embedded in the service.

Users can receive messages via text message, smartphone app, or email, but **contact information like phone numbers and email addresses stays private**. Instead, Remind uses third-party phone numbers to protect users' privacy. We've also adopted advanced cloud computing practices and strict internal policies to ensure the integrity of the data we manage.

> "I see a lot more communication now because of Remind. Teachers don't have to worry about giving out their emails."
>
> **P.A. WHITE**
> *Principal, ABC Unified School District, CA*

Remind's approach to security is guided by three principles:

Control
Users own their data and control their experiences.

Collaboration
We actively work with our users to keep the Remind community safe.

Commitment
Remind consistently audits, tests, improves, and shares our practices to protect personal information.

This white paper provides a current overview of the policies and practices that comprise our security approach. Along with the practices outlined below, Remind works with administrators, third-party auditors, penetration testing firms, and policy advisors to continually strengthen our investments across all aspects of security.

Overview

Educators and families trust Remind with important and sensitive information. Our security approach consists of five critical components that allow us to maintain data security and integrity for entry, transfer, storage, and access.

- Corporate governance
- Physical security
- Environmental security
- Software security
- Regulatory compliance

Each of these will be described in more detail.

> "Remind has paved the way for other technology resources in the classroom."
>
> **JUSTIN SANDERS**
> *Teacher, Birmingham City Schools, AL*

Corporate governance

Remind works with industry-leading auditors to review and guide our policies and procedures, including the NIST Cybersecurity Framework Gap Analysis with NCC Group.

- All Remind employees and contractors sign agreements that require them to preserve and protect the confidentiality of sensitive information they may access while doing their jobs.
- All Remind employees are scrutinized by mandatory background checks.
- Employees are required to enable two-factor authentication in every internal and external service where two-factor authentication is made available and practical.
- All computers and mobile devices issued by Remind, as well as any software that runs on those machines, are password-protected and encrypted where possible.
- All employees receive privacy and security training at least annually.

Physical security

Remind strictly controls physical access to user information.

- All Remind premises require keycard entry.
- The on-site storage of personally identifiable information (cloud-based storage) is not required.
- All work computers and laptops provided to Remind personnel have encrypted disks.

Environmental security

Remind uses Amazon Web Services (AWS) and other third-party services in the AWS environment to host and operate our databases.

AWS is an industry-leading cloud service platform that provides nondescript facilities, professional security staff, controlled access, video surveillance, intrusion detection, and other security features. All data is separated from outside connections, and access is limited to select members of the current Remind team.

- Remind stores its data within an AWS region that is FedRAMP compliant.
- Remind's main database and all backups are encrypted at rest.
- The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best practices, including HIPPA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP and FISMA, ITAR, FIPS 140-2, CSA, and MPAA.

Learn more about Amazon's security policies.

Software security

Remind's infrastructure is built on industry-tested technology and security practices.

- Remind uses encryption, firewall, and network security software.
- Remind uses single sign-on (SSO) and two-factor authentication (TFA).
- Any VPN access to Remind systems requires SSO and TFA. VPN access is required for many services, including remote access (through SSH) to production servers and management tools.
- Logging into confidential parts of company systems requires time-limited SSH keys generated by classified users. All SSH requests are logged for auditing.
- Low-level auditing software is run on all systems to record potentially malicious actions that may take place.
- Remind runs periodic penetration tests, then logs and resolves discovered issues.
- All Remind clients use TLS/SSL when communicating with our servers.

- Remind has a host-based intrusion detection system to detect unauthorized access to production hosts.
- Audit logs are sent to a central location for storage and analysis. Access to production servers and interaction with production systems is audited and logged.

Remind's designated Incident Response Manager, Jason Fischl (VP of Engineering), is responsible for handling the response to data breaches. The Incident Response Team can be reached at security@remindhq.com.

Regulatory compliance

Remind works with policy advisors to ensure that our product and practices remain compliant with relevant mandates and regulations.

- Remind meets COPPA and TCPA legislative requirements.
- Remind helps schools comply with federal FERPA regulations.

Learn more

At Remind, we understand the importance of protecting personal information. Our approach to security was developed to help schools and districts remain confident in the integrity and security of their data—and focus on helping educators and families support student success.

> "I thought this was going to be too much for me because I'm older and almost never start using new tech tools, but it's so easy."
>
> NECHAMA BLISKO
>
> *Teacher, NYC Public Schools, NY*

To learn more about what this could look like at your district, contact our team at districts@remindhq.com.