Remind

Security Overview

Remind is built to enhance educational attainment and advance communication between teachers, students, parents, and administrators. Effective learning involves educators, students, and parents—a support network that's built on a foundation of trust and accountability.

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 school and district administrators, third-party auditors, penetration testing firms, and expert policy advisors to continually strengthen our investments across all aspects of security.

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 complies with all applicable privacy laws. Remind has obtained iKeepSafe certification for the FERPA Assessment, COPPA Safe Harbor Program, and California Student Privacy Badge. Remind is a certified signatory of Privacy Shield, administered by the US Department of Commerce, which allows Remind to lawfully transfer the data of European Union residents to the United States. 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 are only visible to school administrators and not exposed to teachers, parents or student users. 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.

Remind

Overview

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

- Corporate governance
- Logical security
- Physical security
- Environmental security
- Software security
- Privacy principles
- Regulatory compliance

Each of these components are described in more detail below.

Corporate governance

Remind works with industry-leading advisors to review and guide our policies and procedures, including the NIST Cybersecurity Framework.

- Remind adapted our practices to meet the criteria set forth in the ISO/IEC 27001 framework, which advances our ability to safeguard sensitive information.
- All Remind employees are scrutinized by mandatory background checks.
- All employees receive privacy and security training at least annually.
- 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.
- Information security controls are measured, monitored, and tested for their effectiveness to support continuous improvement.

Logical security

Remind implements technical controls to prevent the inadvertent exposure of user information.

- Network security controls include protecting the perimeter boundary with a firewall, ensuring public-facing web servers are in a DMZ and applying further segmentation to isolate internal subnets hosting sensitive resources.
- Sensitive information is protected at rest and in transit across untrusted networks using strong encryption.
- Access to Remind systems requires the use of a VPN protected by multi-factor authentication (MFA). VPN access is required for many services, including remote access (through SSH) to production servers and management tools.
- Logging into a sensitive system requires time-limited SSH keys generated by classified users. All SSH requests are logged for accountability purposes.
- All devices issued to Remind personnel are centrally managed to enforce a secure configuration, including full disk encryption, antivirus software and strong authentication requirements.
- Remind employs a host-based intrusion detection system to detect unauthorized access to production hosts.
- Employees are required to enable two-factor authentication in every internal and external service where two-factor authentication is made available and practical.

Physical security

Remind applies layered physical access controls to safeguard employees and protect systems that access, store, transmit or process user information.

- Remind is hosted in a data center facility with rigorous physical security controls including a non-descript location, security staff, layered electronic access controls from all building ingress points to interior zones, intrusion detection, and surveillance monitoring.

Physical security (cont.)

- Geographically distributed backup locations prevent information loss in the event of hardware damage.
- All devices issued to Remind personnel can be remotely locked or wiped if lost or stolen.

Environmental security

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

- AWS's environmental protections reduce the risks associated with fire, loss of power, flood, humidity, and temperature changes in their facilities.
- Data center facilities are strategically located in regions that are less commonly affected by natural disasters.
- Cloud-based information storage is protected from environmental threats using fault-tolerance and redundancy.
- The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best practices, including HIPAA, 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, CMMC, NIST, and MPAA.

Learn more about Amazon's security and environmental protection policies here.

Software security

Remind's software is delivered using industry-tested technology with privacy, end user safety, and security in mind.

- Penetration tests are performed against our application routinely by independent third-party firms using trusted methodologies.
- Remind maintains a private program for security researchers of varied disciplines and expertise to perform ongoing security assessments of our applications.

Software security (cont.)

- Vulnerabilities discovered in our applications are prioritized and remediated swiftly.
- Low-level auditing software is used to record potentially malicious actions or abuse of the service.
- All Remind clients use TLS/SSL when communicating with our servers.
- Remind follows an industry standard secure development process that considers privacy by design and aims to avoid common security exposures.

Privacy principles

Remind has adopted modern practices with respect to handling personal information.

- Remind maintains a Privacy Notice in a clear and conspicuous location on our website to inform consumers about how personal information is used, collected, and shared.
- The processing of personal information is limited to the purposes identified by a commercial agreement and never repurposed.
- Remind does not disclose personal information to any third party without authorization unless that disclosure is necessary in order to comply with the law or a valid request from public authorities.
- Remind will never sell, trade, barter, or exchange for value consumers' personally identifiable information or personal data.
- In the case of a security incident resulting in a data breach or the unauthorized disclosure of personal information, as defined by a state, federal or other regulation, Remind will promptly notify impacted parties and authorities.

Remind has designated a Security Incident Response Manager, Kevin McIntire, who is responsible for coordinating the response to consumer data breaches with members of our executive leadership, security, and legal teams. The Security Incident Response Team can be reached at security@remind.com.

Regulatory compliance

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

- Remind meets COPPA and TCPA legislative requirements.
- Remind helps schools comply with federal FERPA regulations.
- Remind has prepared for and adopted additional practices to comply with jurisdiction-specific privacy regulations such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).

Additional information

Remind's approach to security was developed to help schools and districts remain confident in the integrity and security of their data, so they can focus on helping educators and families support student success. You can find more information and resources on our Trust and Safety page.

Remind