

GARDEN CITY UNION FREE SCHOOL DISTRICT

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and ParentSquare, Inc. (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the GARDEN CITY UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

"Personally identifiable information" from the records of the District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of

Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER:

BY: Brian Rowse **DATED:** June 3, 2025
Brian Rowse, Chief Information Officer

Return to:

Lauren Maguire
Director of Information Technology
Garden City Union Free School District
56 Cathedral Avenue
Garden City, NY 11530
maguirel@gcufsd.net

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

ParentSquare Privacy Policy

Last Updated: February 10, 2025

Overview

ParentSquare is a provider of digital family and community engagement solutions for K-12 institutions. School districts and other users rely on ParentSquare's subscription services, including ParentSquare Engage, Smart Sites, Remind Hub and Remind Chat (collectively, the "Subscription Services").

Commitment to Your Privacy

ParentSquare understands that privacy is extremely important to users of the Subscription Services, the district, school or organization that registers for the Subscription Services (your "District"), and the students, their parents and other users whose information ParentSquare may access on behalf of your District.

ParentSquare's goal is to be transparent in our practices regarding collection and data usage. This Privacy Policy covers all products and services delivered by ParentSquare.

Data Covered and Written Agreements

In this Privacy Policy, "Personal Data" means any information about an identifiable individual or information that can be used to identify an individual, and includes "personal data" as that term is defined under the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR"). This Privacy Policy explains how ParentSquare collects, processes, uses and discloses information from you and other users who access or use the Subscription Services, including our treatment of Personal Data. This includes Personal Data (i) provided to ParentSquare as a service provider by your District pursuant to the ParentSquare School Agreement and/or a separate written agreement between ParentSquare and your District (in either case, the "Agreement"); (ii) collected by ParentSquare as a service provider at the direction of your District; or (iii) provided by an individual account user. This Privacy Policy along with the Agreement and applicable laws govern ParentSquare's handling of Personal Data gathered in its capacity as a service provider.

If this Privacy Policy expressly contradicts the Agreement as to the data privacy and security, the Agreement will govern to the extent of the contradiction.

This Privacy Policy does not apply to websites, services or practices of companies that ParentSquare does not own or control, even if they help ParentSquare operate the Subscription Services. Third party providers who help ParentSquare operate the Subscription Services must adhere to privacy and security obligations in a manner consistent with and at least as protective of Personal Data as are ParentSquare's policies and practices.

Please make sure that you read the ParentSquare Terms of Use to understand additional terms and conditions that apply to the use of the Subscription Services and website.

Information ParentSquare Collects

ParentSquare collects three types of information: Personal Data that your District knowingly chooses to disclose that is collected on an individual basis; information you or your parent or legal guardian may knowingly enter on the Subscription Services; and website usage information collected on an aggregate basis as you and others browse our website.

Information Your District May Provide to ParentSquare

ParentSquare may collect information (including Personal Data) when your District requests integration to receive the Subscription Services. ParentSquare collects that information at the direction of your District, from your District's Student Information/Management System ("SIS/SMS"), or other District systems such as payroll systems, nutrition systems, fee systems or similar systems through a District-requested integration. Information collected from District-provided data may include but is not limited to: name, ID number, title, phone number, email address, home/ mailing address, group memberships, extracurricular activities, enrolled courses, classes, section, grade level, bus route, preferred communication language, emergency contact information, family relationships, school memberships and district memberships.

Information You Provide to ParentSquare

ParentSquare receives and stores any information you knowingly enter on the Subscription Services, including information you may be able to upload, import, or sync to the Subscription Services from your mobile device (for example, contact information from your address book).

This information may include but is not limited to Personal Data such as your name, phone numbers, email addresses, photographs and, in certain circumstances, your school and/or district, class, group, grades and report card, attachments that may contain your voice and image, club, team or organization affiliation. This information may be used to validate your account or to provide you with notifications via the Subscription Services from a teacher, school and/or district, class, group, club, team or affiliated organization, or any other information necessary for ParentSquare to provide the Subscription Services.

For certain Services, you may also choose to provide ParentSquare with additional information about yourself in your user profile, such as your profession, talent, interests and abilities. All information you provide voluntarily may be made accessible to users in your District.

You may choose not to provide ParentSquare with certain information, but then you may not be able to take advantage of many of the features of the Subscription Services.

Information ParentSquare Collects From You

ParentSquare receives and stores certain types of information whenever you use the Subscription Services. For example:

- a. Website Activity Information: ParentSquare monitors some of the actions you perform on the Subscription Services. For example, if you make a comment on a post, ParentSquare both logs the fact that you added a comment as well as stores the actual comment itself.

- b. Notification Activity Information: ParentSquare monitors email delivery, text delivery, app downloads, and engagement through clicks in order to understand your interaction with the Subscription Services and improve your experience with ParentSquare. ParentSquare may include clear gifs in the HTML-based emails ParentSquare sends to your District in order to track which emails are being opened and which links are being clicked on by recipients.
- c. Access Device and Browser Information: When you access the Subscription Services from a computer, mobile phone or other device, ParentSquare collects information from that device such as your browser type, operating system, unique device identifier, Internet Protocol (IP) address, the date and time of visits, and the time spent at ParentSquare's websites.
- d. Cookie Information: ParentSquare may send one or more cookies to be stored on your computer, mobile phone or other device in order to personalize your experience with ParentSquare and make the Subscription Services easier to use. A cookie is a small text file containing a string of alphanumeric characters that allows ParentSquare to uniquely identify your browser and allows you to log in automatically whenever you return to ParentSquare. ParentSquare also uses cookies to identify and maintain your logged in status as well as enhance your navigation through the website. You can remove or block cookies using the technical settings of your browser though you may not be able to do so on certain browsers or mobile devices. Note that disabling cookies may impact your ability to use the Subscription Services fully, so ParentSquare recommends that you leave them enabled for the quality of your experience.

How is Children's Personal Data Treated?

ParentSquare complies fully with the Children's Online Privacy Protection Act ("COPPA").

Due to ParentSquare's commitment to protect the privacy of children, ParentSquare also participates in the iKeepSafe Safe Harbor Program. ParentSquare has been awarded the iKeepSafe COPPA Safe Harbor Seal signifying ParentSquare's website and apps have been reviewed and approved for having policies and practices surrounding the collection, use, maintenance and disclosure of Personal Data from children consistent with the iKeepSafe COPPA Safe Harbor Program guidelines. iKeepSafe's mission, as an independent certification organization, is to give parents, educators, and policymakers the information and tools which empower them to teach children the safe and healthy use of technology and the internet. The iKeepSafe program only covers information collected through the Subscription Services. If you are not satisfied with ParentSquare's response, you can contact the iKeepSafe Safe Harbor Program's dedicated consumer complaint department at: coppaprivacy@ikeepsafe.org or see ikeepsafe.org/about-us/contact-us/.

Pursuant to COPPA, ParentSquare typically relies on your District's consent on behalf of parents in order to allow those under 13 years of age to use the Subscription Services.

For users of Remind Chat, pursuant to COPPA, ParentSquare may collect an under-13 user's name (first and last name), date of birth, email address and/or telephone number in order to operate and provide the Subscription Services, and ParentSquare may collect the under-13 user's parent's (or legal guardian's) email address in order to provide notice to the child's parent or guardian that ParentSquare may contact the under-13 user for the purpose of allowing access to and use of the Subscription Services.

If ParentSquare does not receive the parent's email address within a reasonable time period, the under-13 Remind Chat user will not be able to send or receive any messages and their Personal Data will be deleted. If an under-13 user's Remind Chat account has not sent or received a message through the Subscription Services for at least twelve months, ParentSquare's policy is to delete the Personal Data.

In order for an under-13 user to gain access to additional ParentSquare features or products, ParentSquare may employ one or more methods approved by the Federal Trade Commission for verifying parental consent.

If ParentSquare learns that it had collected Personal Data from a child under age 13 other than pursuant to the above, or if ParentSquare learns that a child under 13 has provided it Personal Data beyond what was requested from them, ParentSquare will delete that information as quickly as possible after it has been notified internally or by impacted customers.

If you have questions about modifying or deleting Personal Data of a student on ParentSquare or Remind Hub, please contact your District directly.

How ParentSquare Uses Information

Your privacy and your child's privacy is extremely important to ParentSquare. ParentSquare uses the Personal Data it receives about you to provide you with the Subscription Services and also for purposes such as:

To Manage the Service

ParentSquare uses the information it collects to provide the Subscription Services and features to you and provide you with customer support. In addition, ParentSquare uses the information it collects to analyze how you use the Subscription Services and features so that it can measure and improve the Subscription Services and features.

To Contact You

ParentSquare may contact you with Subscription Services-related announcements from time to time. This includes contacting you for any school or district related activities. ParentSquare may include content you see on the Subscription Services in the emails it sends to you. ParentSquare may also contact you in order to notify you about important changes to the Subscription Services.

To Provide Relevant Information To Your District

ParentSquare uses the information it collects to report usage levels to your District. This allows your District to monitor how successful their communications are so that they can improve their use of the Subscription Services.

And most importantly, authenticating your identity, protecting our users, and working toward making sure the Subscription Services are safer and more secure.

Email and Text Message Communications

If ParentSquare has your email address or phone number, it may send you administrative messages (such as updates, notifications, newsletters and other news) relating to the Subscription Services or to respond to communications from you. ParentSquare may also send you urgent messages when it is directed to do so by a teacher, school, district or government agency.

By maintaining a ParentSquare account and/or not opting out of receiving information from ParentSquare, you acknowledge and agree that you may receive e-mail or SMS text messages on your phone or mobile device from other ParentSquare users, from ParentSquare and/or its third-party service providers and other individuals or companies if you choose to use applicable services or products that they offer. Receiving these messages may cause you to incur usage charges or other fees or costs in accordance with your wireless or data service plan. Any and all such charges, fees or costs are your sole responsibility. You should consult with your wireless carrier to determine what rates, charges, fees or costs may apply. ParentSquare may receive a confirmation when you open an email from us if your computer supports this type of program. Communications of this type are also sent to under-13 users and the parental consent to use this service also covers these messages. If you no longer wish to receive administrative email messages from ParentSquare, you may opt-out by following the unsubscribe link located at the bottom of each message or by contacting us at privacy@parentsquare.com.

To permanently cease receiving SMS text messages, please text @STOP in reply to any SMS message from that class, group or school.

If you are located in Canada, you may opt out of receiving marketing messages (including text messages and emails); however, you may still receive text message and email communications that are necessary for the Subscription Services or otherwise exempt from anti-spam laws.

Mobile Application

When users use ParentSquare's mobile applications, it automatically collects the IP address, device ID, device type, and what operating system (OS) the user is running.

ParentSquare collects users' IP addresses whenever they use ParentSquare's mobile applications, which provides it with a coarse approximation of the user's location at the city level in order for ParentSquare to, for example:

- provide organizers with a geo-specific long-code (i.e., generic phone number with a local area code),

- support features such as school selection, and
- enable other internal measurement and Subscription Services features.

ParentSquare also may, with your express consent, request more specific location information in order to provide you with more relevant information (such as nearby classes or relevant groups that you may subscribe to). ParentSquare will not store or track your device location on an ongoing basis or without your permission. ParentSquare may also collect location-based information from users as part of providing the Subscription Services, or in order to comply with applicable laws and regulations for the user's jurisdiction.

If the under-13 user has signed up for the Subscription Services through SMS and then downloaded Remind Chat's mobile application, ParentSquare will have and may use the under-13 user's phone number:

- to merge the under-13 user's accounts,
- to continue SMS delivery services, and/or
- as a back-up method of notification.

Push Notifications

ParentSquare sends notices to you for various reasons directly relating to your use of the Subscription Services or at the request of your District, for example when an organizer of your class or group has posted something new to your class or group, you are sent a message, or when ParentSquare needs to inform you of something. If you no longer wish to receive such communications, you may turn them off at the device level for applicable services or contact your District. If you are a parent of an under-13 Remind Chat user, you always have the choice to no longer allow your child to receive such communications by contacting ParentSquare at privacy@parentsquare.com.

How ParentSquare Shares Information

ParentSquare uses the data received from your District for the sole purpose of delivering products and services to your District. ParentSquare does not rent, trade, sell or otherwise distribute your information to any third parties, and will only disclose information when allowed by the Family Educational Rights and Privacy Act ("FERPA") and required: a) by applicable laws or government orders, such as a law enforcement or court order; b) to maintain and operate the Subscription Services; c) to enforce or apply the ParentSquare Terms of Use and other agreements; d) to protect the rights, property or safety of ParentSquare, its employees, its users or others; or e) when authorized by your District.

How Does ParentSquare Work with Third Party Service Providers?

ParentSquare works with a number of third party service providers and contractors to maintain and operate the Subscription Services. For example, but not limited to, ParentSquare uses third party service providers:

- For secure credit card transaction processing for supporting payments in ParentSquare.
- To provide customer support communication to users.
- To analyze use of the ParentSquare website and app.
- For the ParentSquare blog and to facilitate social sharing on its blog.
- To send emails, texts, phone calls, and push notifications.
- For hosting the Subscription Services and databases.
- To provide additional services to your District such as mailing services, background checks for volunteers, lesson plans, newsletters and other optional features.
- To provide solutions for logging into the Subscription Services using Google, Clever, SIS/SMS or a district-managed single sign-on (“SSO”) integration.

Before ParentSquare engages with a third party where ParentSquare may share Personal Data, it ensures that their privacy policy is at least as protective of your Personal Data as is ParentSquare’s.

ParentSquare will not provide any Personal Data to any person, party or organization ineligible to receive student records or student record data and information protected by FERPA, federal regulation, state law or regulation, or who is otherwise prohibited from receiving District data.

ParentSquare also may provide to its third-party partners aggregated information derived from automatically collected information about how users, collectively, use the Subscription Services. ParentSquare may share this type of non-personally identifiable, aggregated statistical data so that its partners also understand how often people use their services as well as ParentSquare’s.

A list of the third-party partners’ services ParentSquare currently uses, the data that is shared, as well as links to their privacy policies, can be found [here](#).

No Advertising

ParentSquare does not use student or user records or data collected for purposes of targeted advertising, and no student profile is built by ParentSquare for reasons other than for the District’s purposes.

ParentSquare provides links to external websites for purposes which are intended solely to support your District’s day-to-day operations.

Your District or its users may post links within ParentSquare to external websites for which ParentSquare has no control. Before interacting with those third-party websites and their owners’ services or features, ParentSquare recommends you familiarize yourself with their owners’ privacy policies and practices as ParentSquare cannot control the data practices of these third parties.

Corporate Restructuring

In the case of a corporate event such as a sale of assets, an acquisition, or a merger of ParentSquare with another organization, ParentSquare may transfer your Personal Data. However, ParentSquare will provide you with notice and an opportunity to opt-out of the transfer of Personal Data.

With Your Consent

You will be notified when your Personal Data may be shared with agents or companies other than ParentSquare, and you will be given the option to prevent the sharing of this information unless ParentSquare determines that not disclosing this to you prior to your information being shared is necessary to comply with applicable laws or legal processes or ParentSquare is prohibited by law or legal processes from informing you in advance.

What Can Other ParentSquare Users See

You are responsible for any content you provide in connection with the Subscription Services. ParentSquare cannot control the actions of anyone with whom you or any other ParentSquare users may choose to share information. Therefore, ParentSquare cannot and does not guarantee that content you or any user posts on the Subscription Services will not be viewed by unauthorized persons. Although ParentSquare may allow its users to set privacy options that limit access to certain parts of the Subscription Services, please be aware that no security measures are perfect or impenetrable and that ParentSquare is not responsible for circumvention of any security measures contained on the Subscription Services. ParentSquare does not encourage you to make any Personal Data public other than what is necessary for you to use the Subscription Services. You understand and acknowledge that, even after removal, copies of content may remain viewable in cached pages, archives and storage backups or if other users have received, copied or stored your content. ParentSquare will make efforts to remove the content under our control that is not part of another user's account.

Notwithstanding the foregoing, your District may choose to share some ParentSquare posts and associated pictures on social websites, such as but not necessarily limited to Facebook, Reddit, TikTok, YouTube, X, etc. If done via an integration, ParentSquare will require your District to confirm that it has prior permission before doing so. Sharing posts and pictures on social websites will make the posts and pictures viewable by users outside of ParentSquare, and ParentSquare's Privacy Policy will no longer apply to those posts and pictures.

Your District's administrators may have access to user accounts via methods such as, but not limited to, SSO options, integrations with their SIS/SMS, or ParentSquare product enhancements. These options allow verified administrators or employees to access and utilize the accounts of members of their school or district communities. Administrators may do this to remediate account issues, or to implement quality or safety controls. If your District chooses to use those login features, ParentSquare requires administration to give notice to all users in your District in advance, collect evidence of their consent, and have in place an acceptable use policy for technologies used within your District.

Your contact information, i.e., your email, phone and home/mailling address, may be made available to other registered parents at your district or school as part of an online school directory according to your District's discretion.

How ParentSquare Protects Information

ParentSquare complies with, or works with your District to jointly ensure compliance with, FERPA and all other applicable confidentiality and privacy laws and rules, and requires its employees, consultants, and subcontractors to similarly comply. Each ParentSquare user plays an important role in securing their account.

Security

ParentSquare takes great measures in keeping your Personal Data safe and secure. ParentSquare encrypts Personal Data during transfer and at rest. ParentSquare stores and protects your account information on a secured server behind a firewall. ParentSquare utilizes encryption/security software to safeguard the confidentiality of Personal Data it collects.

Data Breach Policy

If ParentSquare becomes aware of a data breach of its users' Personal Data, ParentSquare will comply with applicable law, the Agreement, and notify your District as well as the affected users if asked to do so by your District or as required by applicable laws.

In the event of a data breach, as that term is defined in law or by the Agreement, the goal is to provide notice to your District within 72 hours (or sooner if required by law or the Agreement) after ParentSquare has confirmed the data breach.

If there are actions required on the part of your District related to the breach, ParentSquare will provide detailed instructions and assist in remediation.

Choices About Your Information

Managing Your Account

You may review, update and correct the information in your account by logging into ParentSquare or, in many cases, from your SIS/SMS portal. Your District may not allow you to update your account information directly in ParentSquare. In such an event, an alternate District contact or instructions will be provided for you to update your ParentSquare contact information or you may be able to update in the SIS/SMS portal. You are able to adjust your notification settings within ParentSquare so that you receive instant or digest notifications for app notifications, emails and texts, or you may opt out of ParentSquare communications and receive no notifications at all. If you choose not to receive notifications from ParentSquare this will not stop you from receiving urgent notifications, for example those regarding school closure, threats, etc.

Deleting Your Account

If you or your child graduates from your District or leaves your District and you are no longer associated with your District, your District may delete your account, i.e., you will no longer be able to access your information on ParentSquare and no other ParentSquare user will be able to access your Personal Data either, including your District, unless for legal reasons. ParentSquare will retain and use your information as necessary in order to comply with its legal obligations, resolve disputes, prevent abuse and enforce its agreements. In case of accidental deletion, ParentSquare will be able to restore the account on request if a request is made within thirty (30) days of deletion.

If you are a member of ParentSquare school or district and cease to agree with the ParentSquare Terms of Use and Privacy Policy at some point in the future or if you no longer desire the Subscription Services, please contact your District directly to delete your account.

Remind Chat users may request deletion of your Remind account by accessing your account online or contacting us at privacy@parentsquare.com.

Note, if you are a member of a ParentSquare school or district and you request to delete your account, ParentSquare may notify the organization and the organizer(s) of the classes and/or groups you are affiliated with of your deletion request.

Please note that certain information may remain in ParentSquare's records, server logs and archives after deletion of your account. ParentSquare retains this information for purposes such as diagnosing problems with the Subscription Services, to comply with various states' open records laws or similar contractual commitments to a District, and for auditing legal investigations. ParentSquare reserves the right to delete this information in accordance with its standard business practices in effect from time to time. Information and other content you have provided, however, may remain visible elsewhere to the extent such content was copied or stored by other users.

If your or your child's Personal Data changes, you no longer desire to use the Subscription Services, or you would like to rescind permission for ParentSquare's Remind Chat services to further contact your child, you may review, correct, update, delete inaccuracies, request deletion of your child's information, or amend it by logging into your account and making those changes or contacting us at privacy@parentsquare.com.

If you are a Remind Hub or ParentSquare user, ParentSquare will get in touch with your District to honor your request and respond within a reasonable time not exceeding thirty (30) days. ParentSquare will retain your information for as long as your account is active or as needed to provide services to you and your District.

HIPAA

ParentSquare is not a healthcare organization and is not certified as compliant with the Health Information Portability and Accountability Act ("HIPAA").

European Union Residents

ParentSquare's computer systems are currently based in the United States, so your Personal Data entered in the Subscription Services or related to your use of the Subscription Services will be stored in the United States. By using the Subscription Services you: (a) agree to and accept the terms stated in this Privacy Policy, and, (b) expressly consent to the processing of your Personal Data on equipment and by service providers outside the European Economic Area. If you reside in the European Union and ParentSquare does not seek your explicit consent to process your Personal Data, ParentSquare is relying on the legitimate commercial interest of ParentSquare in providing the Subscription Services to you and other customers and the need to process your Personal Data as previously described in order to accomplish that legitimate interest. You also have the right to withdraw consent and request that ParentSquare halts processing of your Personal Data at any time. This withdrawal of consent does not invalidate the consent-based processing that occurred prior to withdrawal. As an EU resident, you also have the following rights under the General Data Protection Regulation:

- Right to access your Personal Data
- Right to rectification of Personal Data held where it is incorrect or incomplete
- Right to erasure of Personal Data ("right to be forgotten") if certain grounds are met
- Right to restrict/suspend processing of Personal Data
- Right to complain to a supervisory authority
- Right to object to processing
- Right to object to processing of Personal Data for direct marketing purposes
- Right to receive your Personal Data in a standard electronic format (data portability)

Remind Chat complies with all applicable laws regarding your privacy. Individuals from the European Union ("EU"), European Economic Area ("EEA") or United Kingdom ("UK") may only use the Subscription Services after providing your freely given, informed consent for ParentSquare to collect, transfer, store, and share your Personal Data, as that term is defined in the EU's General Data Protection Regulation. EU, EEA or UK residents may grant that consent directly to ParentSquare.

You may withdraw this consent or exercise any of the foregoing rights applicable to you by contacting the Privacy Officer at the address below or notifying us at privacy@parentsquare.com.

How may I exercise my privacy rights as a resident of the EU, EEA, Switzerland or the UK who uses Remind Chat?

Remind Chat complies with the EU GDPR and the UK Information Protection Act 2018 and makes it easy for EU, EEA, Swiss or UK residents to exercise their rights described in that regulation. The purposes for which ParentSquare collects your Personal Data, the categories and specific types of Personal Data ParentSquare collects, and ParentSquare's practices and policies regarding your Personal Data are described in this Privacy Policy. As discussed throughout this Privacy Policy, ParentSquare makes it easy for you to access, correct, delete or demand deletion of your Personal Data. You may object to our processing of your Personal Data by emailing us, although if you prohibit our processing, it may make some of the Subscription Services either impossible to offer or less useful. Any of those requests should be sent to privacy@parentsquare.com. Should you ever wish to leave Remind Chat and take an electronic copy of the Personal Data and information ParentSquare has collected about you, you may make that request at privacy@parentsquare.com. In addition to contacting our Privacy Officer (who also serves as our Data Protection Officer) or the Better Business Bureau, EU individuals may contact the Data Protection Authority of Ireland by email at info@dataprotection.ie, and UK individuals may contact the Information Commissioners Office by live chat at <https://ico.org.uk/global/contact-us/> to raise concerns about our implementation of GDPR, the UK Information Protection Act 2018, or our facilitation of the exercising of your privacy rights.

How does Remind Chat protect my privacy rights as a European Union, European Economic Area, Swiss or United Kingdom Individual?

Remind Chat complies with the EU-U.S. Data Privacy Framework program (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework program (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. Remind Hub and Remind Chat has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of Personal Data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Remind has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework program Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view the ParentSquare certification, please visit <https://www.dataprivacyframework.gov/>.

In compliance with the EU-US Data Privacy Framework Principles, ParentSquare commits to resolve complaints about your privacy and its collection or use of your Personal Data transferred to the United States pursuant to the DPF Principles. European Union, Swiss and United Kingdom individuals with DPF inquiries or complaints should first contact us.

ParentSquare has further committed to refer unresolved privacy complaints under the DPF Principles to an independent dispute resolution mechanism, Data Privacy Framework Services, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit

<https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers> for more information and to file a complaint. This service is provided free of charge to you.

If your DPF complaint cannot be resolved through the above channels, under certain conditions, you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms.

See <https://www.dataprivacyframework.gov/s/article/G-Arbitration-Procedures-dpf?tabset-35584=2>

Changes to Privacy Policy

ParentSquare reserves the right to change, modify, add or remove portions of this Privacy Policy. ParentSquare will notify District administrators in writing or via email of material changes to this Privacy Policy, including practices around new or additional data collection, or practices that may lessen the previously noted protections around student data privacy.

If you have any questions or would like further clarification about ParentSquare or this Privacy Notice, please e-mail ParentSquare at privacy@parentsquare.com.

How to Contact ParentSquare

If you have questions or concerns pertaining to your information, your registration, your account, or unsubscribing from Remind Hub or ParentSquare, please contact your District directly. Otherwise, if you have questions about this Privacy Policy or ParentSquare, you may contact ParentSquare at privacy@parentsquare.com.

You can also direct inquiries via phone at 888-496-3168 or in writing to:

ParentSquare Privacy Officer
ParentSquare, Inc.
6144 Calle Real, #200A, Goleta, CA 93117

Change Log

Last Updated: February 10, 2025

- Combined principles of ParentSquare and former Remind101 privacy policies, keeping more robust portions of each

August 19, 2022

- Addition of “Data Covered and Written Agreements” paragraph
- Change title from “No Disclosure to Third Parties” to “Sharing and Disclosure of Information”

March 4, 2022

- Under “Access Device and Browser Information” we have updated the device and browser information we collect as part of a security enhancement regarding session management
- Updated our list of third-party service providers referenced in the section “How do we work with Third Party Service Providers?”

June 15, 2021

- External review for compliance with applicable laws & guidelines
- Improved transparency regarding how we use your personal information and with which service providers we share this information
- Added details about our data breach policy
- Addition of California privacy information
- Addition of a “Change Log” to provide additional historical information about ongoing changes to our Privacy Policy.