

Privacy Policy

Last updated: May 2026

Pebble N’ Pond Inc. (“**Pebble N’ Pond**”, “**we**”, “**our**”, or “**us**”) respects your privacy and is committed to protecting it through our compliance with this policy. This policy describes how we collect, process, retain, and disclose personal data when providing services to you through our websites, applications, and related services that link to this policy (our “**Services**”) and our practices for using, maintaining, protecting, and disclosing that information.

This policy applies only to information we collect:

- Through the Services.
- In communications, including email, text, chat, and other electronic messages, between you and the Services.
- Through other communications between you and us, such as support requests and demo request forms.
- When you interact with our applications (including mobile apps) on third-party websites and services, if those applications include links to this policy.

It does not apply to information collected by:

- Us through any other means, including on any other website operated by Pebble N’ Pond or any third party that does not link to or reference this policy; or
- Any third party, including through any application or content that may link to or be accessible from or through the Services.

We may provide additional or different privacy policies that are specific to certain features, services, or activities.

Please read this policy carefully to understand our policies and practices regarding your information and how we treat it. By interacting with our Services or providing us with your information, you agree to the collection, use, and sharing of your information as described in this privacy policy. This policy may change from time to time (see [Changes to Our Privacy Policy](#)). Your continued use of the Services after we make changes as described here is deemed to be acceptance of those changes, so please check the policy periodically for updates.

The Personal Data That We Collect or Process

The types and categories of personal data we collect or process include:

- Account and contact information, including name, home address, email address, phone number, username, role, and school or district association and other contact information you provide us.
- School and school district (“**Education Agency**” or “**EA**”)-provided or EA-authorized information (such as personally identifiable information about students (“**Student Data**”)), including student information system data integrated at EA direction (e.g., roster and related education records, academic performance data, attendance data, and student

behavioral data) and data generated within the Services as part of providing them (including student risk assessment reports and student-to-staff communications via active data sharing [stress, mood, sleep rating] or messaging).

- Payment information, including credit card or debit card information and information about the payment methods and services (such as PayPal or Venmo) you use in connection with the Services.
- Demographic information, including your age, gender, or family or marital status, if you have consented to such information collection.
- Location information, including general geographic location such as country, state or province, or city and precise geolocation, if you have enabled and consented to location information collection.
- Device information, including your IP address, browser type and settings, operating system and version, and other device information.
- Content and information you elect to provide, such as support requests, communications, and information submitted through forms (e.g., demo requests).
- Identity document information, such as Social Security and driver's license numbers, if you have consented to such information collection.
- Biometric information, such as fingerprints, faceprints, and voiceprints, iris or retina scans, keystroke, gait, or other physical patterns, and sleep, health, or exercise data, if you have consented to such information collection.

Some of the information identified above, including identification document information, and precise geolocation information may be considered sensitive data under certain laws. If required under applicable law, we will collect and process sensitive personal data only with your consent. If you choose not to provide or allow us to collect some information, we may not be able to provide you with requested features, services, or information.

We also collect:

- **Statistics or aggregated information.** Statistical or aggregated data does not directly identify a specific person, but we may derive non-personal statistical or aggregated data from personal data. For example, we may aggregate personal data to calculate the percentage of users accessing a specific Services feature.
- **Technical information.** Technical information includes information about your internet connection and usage details about your interactions with the Services, such as clickstream information to, through, and from our Services (including date and time), products that you view or search for; page response times, download errors, length of your visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), or methods used to browse away from a page.

If we combine or connect non-personal statistical or technical data with personal data so that it directly or indirectly identifies an individual, we treat the combined information as personal information.

How We Collect Your Personal and Other Data

You Provide Information to Us

We collect information about you when you interact with our Services, such as when you create or update an account, submit a support request, complete a demo request form, or communicate with us.

Automatically Through Our Services

As you navigate through and interact with our Services, we may use automatic data collection technologies to collect information that may include personal data. Information collected automatically may include usage details, IP addresses, operating system, browser type, pages viewed, timestamps, and information collected through cookies and other tracking technologies including details of your interactions with our Services, such as traffic data, location data, logs, and other communication data, and which resources and Services features that you access and use.

Using automatic collection technologies helps us to improve our Services and to deliver a better and more personalized experience.

The technologies we use for this automatic data collection may include:

- **Cookies.** A cookie is a small file placed on your device when you interact with the Services. You may refuse to accept or disable cookies by activating the appropriate setting on your browser or device. However, if you select this setting, you may be unable to access certain features of the Services.
- **Web Beacons.** Some parts of the Services and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit Pebble N' Pond, for example, to count users who have visited those parts or opened an email and for other related statistics (for example, recording the popularity of certain content and verifying system and server integrity).
- **Administrative Access.** Aggregate data is collected for the purpose of providing intended use of the platform to users, with monitoring for errors that negatively impact the user experience or access to the services.

Pebble N' Pond does not use automated technologies for personal data sales, targeted advertising, or profiling.

When you interact with the Services, there are third parties that may use automatic collection technologies to collect information about you or your device. These third parties may include:

- Analytics companies (e.g., Google Analytics on our public marketing website).
- [Your device manufacturer.]
- [Your internet or mobile service provider.]

These third parties may use tracking technologies to collect information about you when you use the Services. The information they collect may be associated with your personal data or they may collect information, including personal data, about your online activities over time and across different websites, apps, platforms, and other online services. We do not use Google Analytics to target advertising to students.

We do not control these third parties' tracking technologies or how they may be used. If you have any questions about an advertisement or other targeted content, you should contact the responsible provider directly.

How We Use Your Information

We use information that we collect about you or that you provide to us, including any personal data, to:

- Provide, operate, maintain, and secure the Services.
- Perform EA-authorized workflows and communications.
- Provide customer support and service communications.
- [Improve the reliability, performance, usability, and security of our Services, including by analyzing your information and creating de-identified or aggregated data derived from your information for internal purposes such as product improvement, analytics, service performance, security, and research. We maintain such information in de-identified form, do not attempt to re-identify any individual, and do not disclose it in a manner that could reasonably identify an individual. We do not use Student Data or PII data to train generalized AI/ML models.]
- Carry out our obligations and enforce our rights arising from any contracts entered into between you and us.
- Notify you when Services updates are available and about changes to any products or services we offer or provide through them.
- In any other way we may describe when you provide the information.
- For any other purpose with your consent.

The usage information we collect, whether connected to your personal data or not, helps us improve our Services and deliver a better and more personalized experience by enabling us to:

- Estimate our audience sizes and usage patterns.
- Store information about your preferences, allowing us to customize the Services according to your individual needs and interests.
- Speed up your searches.
- Recognize you when you return to our Services.

We use location information we collect to provide access to location-based services, or in support of emergency services.

Who We Disclose Your Information To

We may disclose aggregated or de-identified information about our users that does not identify any individual, without restriction. We do not sell Student Data and do not use Student Data for targeted advertising. Student-facing experiences are not designed to serve pop-up ads or advertisements directed to children.

We may also disclose personal data that we collect or you provide as described in this privacy policy:

- To the EA and authorized users, as configured by the EA.
- To subprocessors that help us provide the Services (such as Google Cloud Platform, Vercel, Neon, and Google Analytics), who are bound by written obligations to protect such data consistent with Pebble N' Pond's commitments.
- To students' parents and guardians where required or permissible under applicable data protection laws.
- To a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of Pebble N' Pond Inc.'s assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by Pebble N' Pond Inc. is among the assets transferred, with appropriate safeguards.
- To fulfill the purpose for which you provide it.
- For any other purpose disclosed by us when you provide the information.
- With your consent.

We may also disclose your personal data:

- To comply with any court order, law, or legal process, including to respond to any government or regulatory request. If we receive such a request for Student Data, we will promptly notify the EA unless legally prohibited, and respond only to the extent required by law or as directed/authorized by the EA.
- To enforce or apply our [terms of service](#) and other agreements.

If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of our organization, our users, or others. The categories of personal data we may disclose to such parties include:

- Account and contact information.
- Payment information.
- Demographic information.
- Location information, including general geographic location and precise geolocation.
- Device information.
- Content and information you elect to provide to us.
- Identity document information.
- Biometric information.
- EA-provided or EA-authorized information (Student Data).
- Self-reported information

Your Rights and Choices About Your Information

This section describes mechanisms you can use to control certain uses and disclosures of your information and rights you may have under state law, depending on where you live.

Cookies and other tracking technologies choices:

- **Cookies and Other Tracking Technologies.** You can set your browser to refuse all or some browser cookies or other tracking technology files, or to alert you when these files are being sent. If you disable or refuse cookies or similar tracking files, some Services features may be inaccessible or not function properly. Some browsers include a “Do Not Track” (DNT) setting that can send a signal to the online services you visit indicating you do not wish to be tracked.

Location data choices:

- **Location Data.** You can choose whether or not to allow the Services to collect and use real-time information about your device’s location through the device’s privacy settings or through the privacy settings of the Services. If you block the use of location information, some Services features may become inaccessible or not function properly.

Your State Privacy Rights

Depending on your state of residency, you may have certain rights related to your personal data, including:

- **Access and Data Portability.** You may confirm whether we process your personal data and access a copy of the personal data we process. To the extent feasible and required by state law, depending on your state, data will be provided in a portable format. Depending on your state, you may have the right to receive additional information and it will be included in the response to your access request.
- **Correction.** You may request that we correct inaccuracies in your personal data that we maintain, taking into account the information’s nature and processing purpose.
- **Deletion.** You may request that we delete personal data about you that we maintain, subject to certain exception under applicable law.
- **Opt Out of Using Personal Data for Targeted Advertising, Profiling, and Sales.** You may request that we do not use your personal data for these purposes.

Important: The exact scope of these rights vary by state. There are also several exceptions where we may not have an obligation to fulfill your request.

To exercise any of these rights, please contact us at Scott.Pearlman@pebblespond.org. To appeal a decision regarding a consumer rights request, please contact us at the same email address.

Some browsers and browser extensions support the Global Privacy Control (“GPC”) that can send a signal to process your request to opt out from certain types of data processing, including data “sales” as defined under certain laws. When we detect such a signal, we will make reasonable efforts to respect your choices indicated by a GPC setting as required by applicable law.

Children’s and Minors’ Data

Our Services are primarily intended for use by Education Agencies and their authorized users, including district staff, counselors, administrators, and students and their legal guardians. Where students under 13 use the Services, student access is enabled by the EA for educational purposes, and EA authorization and consent mechanisms govern access as required under the Children’s

Online Privacy Protection Act (COPPA). We do not require students to provide more personal information than is reasonably necessary to participate in an educational activity supported by the Services. If we learn we have collected or received personal data from a child without the requisite EA authorization or parental consent, we will delete that information.

Student Data Privacy (Family Educational Rights & Privacy Act (“FERPA”) and NY Education Law 2-d)

This section provides additional detail about how Pebble N’ Pond handles Student Data when providing Services to EA and the steps we take to ensure our processing of Student Data complies with applicable legal requirements. Where an EA’s written agreement with Pebble N’ Pond provides more specific or different requirements, the EA agreement controls for that EA’s use.

FERPA (School Official / Legitimate Educational Interest)

The Services are designed to support EA’s educational and administrative functions. When we process Student Data provided by (or at the direction of) an EA, we act as a “school official” or service provider, as applicable under FERPA, performing institutional services or functions for which the EA would otherwise use its own employees. EA users may access Student Data only as authorized by the EA, and we limit internal access to Student Data to personnel with a legitimate need to know for operating, maintaining, securing, and supporting the Services. We do not redisclose Student Data except as directed by the EA, as required by law, or as otherwise permitted under applicable education privacy requirements.

Under FERPA, parents and eligible students (students who are 18 years of age or older) have the right to: (i) inspect and review the student’s education records; (ii) seek amendment of education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student’s privacy rights; (iii) consent to disclosures of personally identifiable information contained in the student’s education records, except to the extent that FERPA authorizes disclosure without consent; and (iv) file a complaint with the U.S. Department of Education concerning alleged failures to comply with FERPA. Complaints may be filed with the Student Privacy Policy Office, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202. To exercise these rights with respect to education records maintained through the Services, parents and eligible students should contact their EA, which controls the education records and the processes for responding to such requests.

NY Education Law 2-d / Part 121 (New York EAs)

For New York EAs, our commitments are designed to align with Education Law 2-d and Part 121 requirements, including:

- Purpose limitation (i.e., use Student Data only to provide the Services).
- Prohibition on sale or commercial marketing use of Student Data.
- Security safeguards consistent with industry standards.
- Subprocessor flow-down protections.
- Breach notification and cooperation.
- Secure deletion and sanitization.

Parents' Bill of Rights Alignment (NY)

Consistent with NY Ed Law 2-d “Parents’ Bill of Rights” principles:

- Student Data is not sold or released for commercial purposes.
- Parents/eligible students may inspect and review education records through the EA’s established processes.
- EAs may request an EA-specific list of Student Data elements processed/configured for that EA deployment.
- State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when Student Data is stored or transferred.
- A complete list of all Student Data elements collected by the state is available for public review at the New York State Education Department website (www.nysed.gov/data-privacy-security) or by writing to: NYSED, 89 Washington Avenue, Albany, NY 12234.
- Complaint pathways are generally handled through the EA; Pebble N’ Pond will cooperate with EA investigations related to unauthorized disclosure.]

How We Protect Your Personal Data

We maintain an information security program aligned to the NIST Cybersecurity Framework (NIST CSF) to manage cybersecurity risk. This includes processes and controls organized around the CSF functions: Identify, Protect, Detect, Respond, and Recover. We use commercially reasonable administrative, physical, and technical measures designed to protect your personal data from accidental loss or destruction and from unauthorized access, use, alteration, and disclosure. However, no website, mobile application, system, electronic storage, or online service is completely secure, and we cannot guarantee the security of your personal data transmitted to, through, using, or in connection with the Services. Any transmission of personal data is at your own risk.

The safety and security of your information also depend on you. You are responsible for taking steps to protect your personal data against unauthorized use, disclosure, and access.

How We Retain Your Personal Data

We keep the categories of personal data described in this policy for as long as reasonably necessary to fulfill the purposes described or for as otherwise legally permitted or required, such as maintaining the Services, operating our organization, complying with our legal obligations, resolving disputes, and for safety, security, and fraud prevention. [Upon termination/expiration of an EA’s Services (or as otherwise specified in the EA agreement), we will support export/return of EA data in an acceptable format and delete Student Data within 60 days. Secure destruction and media sanitization will be performed in a manner aligned to NIST SP 800-88 Rev. 1 where applicable. Upon EA request, we can provide written confirmation that Student Data has been deleted in accordance with the EA agreement.] At the end of the retention period, personal data will be deleted, destroyed, or deidentified.

Changes to Our Privacy Policy

We may update this policy from time to time, and we will provide notice of any such changes to the policy as required by law by making an updated policy available to you via the applicable Services or an alternate channel, as applicable. The date the privacy policy was last updated is identified at the top of the page. We will notify you of changes to this policy by updating the “last updated” date and posting the updated policy on the Services. We may email or otherwise communicate reminders about this policy, but you should check our Services periodically to see the current policy and any changes we have made to it.

Contact Information

To exercise your rights or ask questions or comment about this privacy policy or our privacy practices, contact us at:

Email: Scott.Pearlman@pebblespond.org

Mailing Address: Available upon request.

For requests to access, correct, or delete education records, please contact your EA first. Under FERPA, EAs control education records and the process for responding to these requests.