

Privacy Policy

This version was last updated on July 30th, 2026.

INTRODUCTION

We respect your privacy and are committed to protecting your personal data. This Privacy Policy will inform you as to how we look after your personal data when you visit our Website (regardless of where you visit it from) or use our mobile applications (including the Sparks (Bridge to Kindergarten) app for teachers) (the Website and the mobile application, collectively or individually, the “Services”) and tell you about your privacy rights.

By using our Services, you consent to the data practices described in this Privacy Policy and the Website Terms of Use. If you do not agree with the data practices described in this Privacy Policy or if you do not agree to the Terms of Use agreement, you should not use our Services.

Table of Contents:

1. IMPORTANT INFORMATION AND WHO WE ARE
2. THE DATA WE COLLECT ABOUT YOU
3. HOW WE COLLECT YOUR PERSONAL DATA
4. HOW WE USE YOUR PERSONAL DATA
5. DISCLOSURES OF YOUR PERSONAL DATA
6. DATA SECURITY
7. DATA RETENTION
8. YOUR RIGHTS
9. CALIFORNIA RESIDENT’S PRIVACY RIGHTS
10. THIRD PARTY DISCLOSURES
11. RIGHTS OF PARENTS AND STUDENTS
12. RETENTION POLICY AND AUDITING
13. PERSISTENT IDENTIFIERS DISCLOSURE
14. DATA MINIMIZATION
15. DOCUMENT CHANGELOG

1. IMPORTANT INFORMATION AND WHO WE ARE

The mission of Literacy Resources is to equip teachers with effective and engaging products and professional learning opportunities that help prepare and empower all students to become lifelong readers.

Purpose of this Privacy Policy

This Privacy Policy aims to give you information on how we collect and process your personal data through your use of the Services, including any data you may provide through the Services when you sign up to our newsletter, or purchase a product or subscribe to a service.

Children under Age 13

The Services are not intended for children and we do not knowingly collect data relating to children consistent with the U.S. Children’s Online Privacy Protection Act. If we learn that we have received information directly from a child under age 13 without the parent or legal guardian’s verified consent, we will use that information only to respond to the child/parent/guardian to inform the child that he or she may not use the Services. Heggerty’s myHeggerty application (my.heggerty.org) is intentionally designed for use by students, including children under 13, under the authorization and supervision of their school or district. The myHeggerty application is subject to COPPA and the school authorization consent model described in this Privacy Policy. Data collected through my.heggerty.org from students under 13 is governed by Sections 2.1, 10, 11, and 12 of this Policy and by the Data Privacy Agreement in effect between Heggerty and the applicable Institution.

Under the school authorization consent model, Institution acts as agent for parents and authorizes Heggerty to collect, use, and retain personal information from students under 13 solely for educational purposes. Before enabling student access to myHeggerty — and before authorizing Heggerty to collect personal information from children under 13 — Institution is required to notify parents of Heggerty’s data collection practices, including the categories of data collected, the purposes for collection, Heggerty’s data retention practices, and the existence of the school authorization consent model. This notification obligation is a condition of Institution’s authorization under the Data Privacy Agreement in effect between Heggerty and the applicable Institution, consistent with COPPA §312.4(c) and §312.5(a). Parents who have not received such notice from their school or district, or who have questions about how their child’s data is being used, should contact their school or district administrator or reach Heggerty directly at hello@heggerty.org.

Parents may contact their Institution to refuse or limit data collection for their child before Services are activated.

Access to student data within myHeggerty is governed by a role-based permission structure administered by each Institution. For purposes of this Policy, "Authorized Educator" means a teacher, instructional specialist, or other school-based staff member who has been individually assigned by Institution’s designated administrator to a specific class or student group within the Services. Access to Student Data is limited to the Authorized Educator’s assigned students only — an Authorized Educator cannot access data belonging to students outside their assigned class or group. The designation and revocation of Authorized Educator status is the sole responsibility of Institution’s administrator through the role-based access controls available within the Services; Heggerty does not assign or expand Authorized Educator access unilaterally. Parents who have questions about which staff members have been designated as Authorized Educators for their child should contact their school or district administrator.

Literacy Resources Contact Information

Privacy Officer

Email: hello@heggerty.org

Postal address: 805 Lake St. #293, Oak Park, IL 60301

Changes to this Privacy Policy: We will notify you via email or at log in of any material changes to this Privacy Policy.

Third-Party Links: The Services may include links to third-party websites, plug-ins and applications. We do not control these third-party websites and are not responsible for their privacy statements.

2. THE DATA WE COLLECT ABOUT YOU

Personal data, or personal information, means any information about an individual from which that person can be identified. We or our service providers may collect, use, store and transfer different kinds of personal data about you:

- Identity Data – first name, last name (can just be an initial), username, email, and school role.
- Technical Data – IP address, login data, browser type, time zone, operating system and platform. In our educator-facing mobile applications, this also includes a device or analytics identifier — a randomly generated, app-specific identifier that is not linked to your name or email and is not an advertising identifier.
- Usage Data – information about how you use our Services, products and services.
- Marketing and Communications Data – preferences in receiving marketing and communication preferences.
- Diagnostics and Performance Data – crash reports, error logs, and performance measurements from our educator-facing mobile applications, used to keep the app stable and fast.

2.1 THE DATA WE COLLECT ABOUT CHILDREN

- Name and Student Identifier - (created by school admins during CSV uploads from or direct input by teachers)

- Assessment and Educational Data — student assessment results, performance scores, and related educational records.
- Session identifiers associated with assessment activity

3. HOW WE COLLECT YOUR PERSONAL DATA

Direct interactions – You may give us personal data by filling in forms or corresponding with us when you:

- Apply for our products or services
- Create an account through our Services
- Subscribe to our service or publications
- Request marketing to be sent to you
- Conduct a survey or give us feedback

Third-party sources – We may receive personal data from third-party service providers who perform functions on our behalf such as storing and analyzing data, providing search results and customer service.

Cookies and Automatically Collected Information – We automatically collect certain types of data when you use our Services including your IP address, web browser type, pages visited, and dates/times of visits.

International Visitors – Literacy Resources is located in the United States. If you reside outside the U.S., your data will be transferred to, stored in, and processed in the U.S. By using the Services, you consent to such processing and transfer.

4. HOW WE USE YOUR PERSONAL DATA

We use your personal data in the following ways:

- To register you as a new guest
- To manage our relationship with you
- To enable you to complete a survey, digital student assessment, or report
- To administer and protect our Services
- To deliver relevant Services content and advertisements to you
- To use data analytics to improve our Services, products/services, and marketing
- To make suggestions and recommendations about goods or services

Opting Out: You can ask us to stop sending you marketing messages at any time by replying with “unsubscribe” in the subject line, clicking “unsubscribe” in the email, or contacting us directly.

Children’s and Student Data Excluded from Marketing Uses. The advertising, marketing, recommendation, and marketing-analytics uses described in this Section 4 do not apply to personal information collected from children under 13 or to Student Data collected through the myHeggerty application. Heggerty does not use Student Data for targeted advertising, to build student profiles for any non-educational purpose, or to market or recommend products or services, consistent with COPPA and applicable state student-privacy laws.

5. DISCLOSURES OF YOUR PERSONAL DATA

We do not sell, trade, or otherwise transfer to outside parties your personally identifiable information. Trusted third-party partners who assist in operating our site may:

- Provide you and members with various services
- Provide database maintenance and security
- Help us manage transactions
- Help us process and fulfill orders or requests

We may also release your information when we believe release is appropriate to comply with the law, enforce our site policies, or protect ours or others’ rights, property, or safety.

6. DATA SECURITY

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. We limit access to your personal data to those with a business need to know. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator where legally required.

Heggerty distinguishes between security events and security incidents as follows:

Security event: A suspicious activity that deviates from normal behavior but does not appear to compromise any system resources. Security events include phishing emails, changes in login permissions, spikes in incoming traffic, and similar situations.

Security incident: A suspicious or malicious activity that compromises a system resource and is being used for unauthorized purposes. Security incidents include data breaches, a successful distributed denial-of-service (DDOS) attack, or similar situations.

7. DATA RETENTION

We will only retain your personal data for as long as necessary to fulfill the purposes we collected it for, including for satisfying any legal, accounting, or reporting requirements. We consider the amount, nature, and sensitivity of the data, the potential risk of harm from unauthorized use, and the applicable legal requirements when determining retention periods.

Retention period and Audit Trail:

Student data is retained in order to measure literacy growth across years. Below outlines how that data is subsequently deleted in regards to assessment data (e.g. scores).

Student data is held up to 7 years, or when the account is deleted – whichever occurs first.

If an account becomes inactive (e.g. the district stops the relationship with the Institution), then the student data will be deleted 2 years later.

- Within one year of an inactive account, the student data is still accessible to export.
- Within the second year of an inactive account, the data cannot be exported unless the school reaches out to Heggerty.
- At the end of the second year of an inactive account, all student data is deleted.

Heggerty maintains durable access logs for all interactions with student PII, including assessment record views, report generation, and roster access. These logs record who accessed the data, when, and for what purpose, in accordance with FERPA §99.32. Access logs are retained for a minimum of 3 years and are available to districts upon written request. Heggerty will provide access to logs within 30 days of receiving a written request. Audit log entries persist independently of student data — they are not deleted when student records are deleted.

8. YOUR RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data:

- Request access to your personal data
- Request correction of your personal data
- Request erasure of your personal data
- Object to processing of your personal data
- Request restriction of processing your personal data
- Request transfer of your personal data
- Right to withdraw consent to us processing your personal data

To exercise any of these rights, contact your school or district administrator as your first point of contact if you feel that one of your rights (e.g. Request access to your personal data) has been infringed. For revocation of consent to

Heggerty's collection of a child's personal information, parents may also contact Heggerty directly at hello@heggerty.org; Heggerty will honor direct parental revocation requests within 2 business days of a verified written request, consistent with COPPA §312.5(b) and §312.6, and will provide concurrent written notice to Institution of the revocation and deletion. For all other rights requests — including review, correction, and non-revocation deletion requests — Heggerty will refer individuals who contact Heggerty directly to their Institution in the first instance. Institutions may submit verified written deletion requests on behalf of students to hello@heggerty.org; Heggerty will fulfill such requests within 2 business days.

9. CALIFORNIA RESIDENT'S PRIVACY RIGHTS

In addition to the rights in Section 8, California residents have additional privacy protections. We do not respond to Do Not Track (DNT) signals.

California's "Shine the Light" law permits individual California residents to request certain information regarding our disclosure of Personal Information to third parties for direct marketing purposes. To make such a request (no more than once per calendar year), contact us at hello@heggerty.org.

10. THIRD PARTY DISCLOSURES

The following third parties receive children's personal information in connection with Heggerty's provision of the Services, as required by COPPA §312.4(c)(1)(iv) and §312.5(a)(2). These parties act as processors under binding agreements and are prohibited from using personal data for any purpose other than providing their contracted services to Heggerty.

Integral disclosures. The following disclosure is integral to the Services because the core educational service cannot function without it:

Service Provider	Amazon Web Services, Inc. (AWS)
Purpose	Infrastructure hosting, encrypted database storage, and transactional email delivery (SES). Assessment report CSVs containing student names and scores are delivered to authorized teachers and administrators via AWS SES as presigned S3 links; student data is not transmitted in the email body.
Children's PII disclosed?	Yes. Assessment performance data is processed by AWS as a delivery processor. Because this disclosure is necessary to provide the core literacy assessment service, the school or district must authorize use of these services on behalf of parents consistent with COPPA.
Written assurances	On file, consistent with COPPA §312.8(c).
Opt-out	Parents and schools cannot opt out of AWS hosting, as it is necessary to deliver the educational service. Parents who wish to revoke consent should contact their school or district administrator in the first instance, or contact Heggerty directly at hello@heggerty.org . Withdrawal of consent may result in the student's inability to use the assessment platform.

Nature of the data interaction (AWS SES). Assessment report CSVs containing student performance data are uploaded to a private S3 bucket. AWS SES delivers an email to the requesting teacher or administrator containing a presigned link to the CSV. Student data is not transmitted in the email body itself. AWS acts as a delivery processor only.

Non-integral disclosures. As of the effective date of this Policy, Heggerty makes no non-integral third-party disclosures of children's personal information in connection with the Services. Heggerty will not engage in any non-integral disclosure without: (a) updating this Policy and Exhibit C of the applicable Data Privacy Agreement; (b) providing Institution with 30 days' prior written notice; and (c) obtaining verifiable parental consent as required by amended COPPA §312.5(a)(2).

Mobile-application analytics & diagnostics — no children's data

The processor below supports Heggerty’s educator-facing mobile applications and is listed here for transparency. It does NOT receive children’s personal information, and the COPPA children’s-data requirements described above do not apply to it. The device or analytics identifier and the Diagnostics and Performance Data described in Section 2 are shared with:

Service Provider	Datadog, Inc.
Purpose	Product analytics, crash/error reporting, and performance monitoring for Heggerty’s educator-facing mobile applications.
Children’s PII disclosed?	No. Datadog receives only educator app-usage, diagnostics, and non-identifying device/analytics identifiers. No student data and no teacher name or email are sent to Datadog.
Nature of data	Anonymous app-usage events, crash/performance data, a randomly generated app-specific device/analytics identifier, and device model + operating-system version. A client IP address is transmitted with these requests and retained for operational logging — approximately 30 days in Datadog, and 2 years in the log copies retained in Heggerty’s AWS environment, after which it is automatically deleted. It is not used to derive your location and is not linked to your account identity. No geolocation, GPS, or precise location is collected; not used for advertising or cross-app tracking.
Retention	Analytics and diagnostics data is retained by Datadog for 30 days, after which it is deleted or retained only in aggregated, de-identified form. Copies of these logs are retained in Heggerty’s AWS environment for 2 years from collection, after which they are automatically deleted.
Written assurances	Datadog’s published Data Processing Addendum applies; Datadog acts solely as a processor on Heggerty’s behalf, not for advertising or tracking.

11. RIGHTS OF PARENTS AND STUDENTS

Parents and eligible students have the following rights with respect to Student Data collected through the Services:

- Review: Request access to the personal information Heggerty has collected from your child.
- Correction: Request correction of inaccurate information.
- Deletion: Request deletion of your child’s personal information.
- Right to File a Complaint: File a complaint with the U.S. Federal Trade Commission ([ftc.gov](https://www.ftc.gov)), your state Attorney General, or — where applicable — the regulator administering your state biometric privacy law.

To exercise these rights, contact your school or district administrator or contact Heggerty directly at hello@heggerty.org. Institutions may submit written deletion requests to Heggerty at hello@heggerty.org; Heggerty will fulfill student data deletion requests within 2 business days of a verified written request.

12. RETENTION POLICY AND AUDITING

Service Provider	Amazon Web Services, Inc. (S3 + SES)
Retention Period	Student identity, enrollment, and assessment records: Duration of Service Agreement + 2 years post-closure, then hard-deleted. Audit logs (FERPA §99.32): 3 years from date of access event. Teacher/admin credentials: Deleted upon request.
Audit Logging	Audit logs are stored in a secured S3 environment (Parquet format, queryable via Amazon Athena) with access restricted to authorized Heggerty personnel. Logs are protected against unauthorized access or modification.

13. PERSISTENT IDENTIFIERS DISCLOSURE

Safeguards (AWS S3 + SES)	S3: Private bucket with server-side encryption (SSE-S3); access controlled via IAM roles; no public bucket policy. SES: Report CSVs not transmitted in email body; presigned S3 URLs expire in 7 days; emails sent only to verified teacher or administrator recipients; student email addresses explicitly excluded from all notification services.
----------------------------------	--

Session identifiers / cookies (students). Heggerty uses session identifiers (server-side session tokens) solely to maintain authenticated state during an active assessment session. These identifiers are not used for behavioral advertising, cross-site tracking, or building profiles of child users. Session tokens expire at the end of each authenticated session. No persistent device-level identifiers are written to student devices, and analytics tools are suppressed for authenticated student sessions. The foregoing applies to student sessions in the myHeggerty application. In Heggerty’s educator-facing mobile applications, a randomly generated, app-specific analytics identifier (described in the Technical Data category in Section 2) is used for product analytics and diagnostics; it is not linked to a teacher’s name or email, is not an advertising identifier, and is not used for cross-app tracking or profiling.

14. DATA MINIMIZATION

Heggerty collects only the data necessary to provide the Services. Specifically:

- Heggerty does not use Student Data to train, fine-tune, or develop general-purpose machine learning models whose outputs are used outside the provision of Services to Institution.
- De-identified data may be used for internal product improvement, consistent with FERPA 34 C.F.R. §99.31(b). Heggerty will not attempt to re-identify de-identified data.

15. DOCUMENT CHANGELOG

May 27, 2026 — Chris Dugan	§2.1 added student data categories; §7 retention table restructured; §8 added FTC/AG complaint right + tiered contact routing; §10 adopted integral/non-integral framework; added Data Minimization and Document Changelog sections. (See prior published version for full detail.)
July 30, 2026 — Steve Dumais	Mobile applications (minimal update): Introduction and §1 scope/consent extended to cover mobile applications; §2 added a device/analytics identifier to Technical Data and a new Diagnostics and Performance Data category (both scoped to the educator-facing app); §10 added a demarcated "no children’s data" subsection disclosing Datadog as an educator-app analytics/diagnostics processor (30-day Datadog retention; log copies retained 2 years in AWS); §13 scoped the student-session identifier language and disclosed the educator-app anonymous analytics identifier. Existing §2 Identity/Technical/Usage language relied on for account, OS/platform, and app-usage data. Basis: App Store / Google Play privacy-disclosure requirements.