PRIVACY POLICY
Literacy Resources, LLC (operating as Heggerty)
This version was last updated on October 14th, 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), when you use our mobile applications (including the Sparks (Bridge to Kindergarten) app for teachers), and when you or your students use the myHeggerty application at my.heggerty.org, including the Vera voice-enabled phonemic awareness assessment. It also tells 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. Consent by use does not apply to children: personal information collected from students under 13 through the myHeggerty application is collected only under the school authorization consent model described in Section 1 and the agreement in effect for the Institution's account, not on the basis of this paragraph.
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. Security Incident Notification
- 8. Data Retention
- 9. Your Rights
- 10. Rights of Parents and Students
- 11. State Biometric Privacy Laws
- 12. California Residents' Privacy Rights
- 13. Third Party Disclosures
- 14. Retention Policy and Auditing
- 15. Persistent Identifier Disclosure
- 16. Data Minimization
- 17. Audit Logging and FERPA Compliance
- 18. Notice of Changes and Contact Information
- 19. 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 this Website, including any data you may provide through this Website when you sign up to our newsletter, or purchase a product or subscribe to a service.

Children under Age 13

Heggerty operates several online services, and they relate to children differently.
Our marketing and e-commerce websites — heggerty.org and shop.heggerty.org — and our mobile applications, which are built for teachers, 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 through those sites or applications 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 them.

The myHeggerty application is different. Most of myHeggerty (my.heggerty.org) is an educator application, used by teachers and administrators. Two parts of it — the Heggerty library and the Vera voice-enabled phonemic awareness assessment — are intended for direct 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 — including audio recordings collected through the Vera voice-enabled phonemic awareness assessment — is governed by Sections 2.1, 2.2, 8, 10, 11, 13, 14 and 15 of this Policy and by the Data Privacy Agreement in effect between Heggerty and the applicable Institution (or, for accounts without a negotiated agreement, the Service Terms accepted by the Institution's administrator).

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 privacy@heggerty.org.

The school authorization model addresses COPPA only. In certain states, biometric privacy laws require direct written informed consent from a parent or legal guardian before voice recordings of a child may be collected, and the school authorization model alone does not satisfy that requirement. Where applicable, your school or district is responsible for obtaining that direct parental consent in addition to the school authorization described in this Section 1. See Section 11.

Parents may contact their Institution to refuse or limit data collection for their child before Services are activated. With respect to Vera specifically, parents may decline the collection of voice recordings for their child on a per-student basis. A refusal communicated to the Institution will be honored by excluding the affected student from Vera, and a parent may withdraw a child from Vera at any time after it is in use. See Section 10.

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 — including any Audio Recordings — 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.

The Vera Voice-Enabled Phonemic Awareness Assessment

Vera is a voice-enabled phonemic awareness assessment within myHeggerty that records a student’s voice while the student completes phonemic awareness assessment tasks. It is designed for students in PreKindergarten, Kindergarten and first grade — most of whom are between three and seven years old, and most of whom are pre-readers.

Vera is not part of myHeggerty by default. It is available only to Institutions that have licensed it, either as a standalone product or as part of a bundled product. Within a licensing Institution, Vera reaches students through the Institution’s own administration: an Institution administrator assigns Vera seats to individual staff members for a specific grade, and Vera becomes available to the students in those staff members’ classes. Heggerty does not enable Vera for any student or class on its own. Before Vera can be used in an account, an administrator of the Institution must also complete an authorization step within the application: the administrator identifies themselves and the Institution, confirms their authority to act for it, and accepts the school authorization consent model and the Institution’s parental notice obligations. Heggerty records who completed this step, when, and the version of the text accepted, and voice recording cannot occur in an account until it has been completed. Voice recording occurs only while a student is completing an assessment that has been assigned to them, and a parent may decline Vera for their child, or withdraw their child from it, at any time — a refusal is recorded against that individual student and prevents any further collection, as described in Section 10.

With Vera, students use myHeggerty directly. A student’s access is limited to completing an assessment that has been assigned to them; students have no other access to myHeggerty and cannot reach the educator-facing application.

Students Signing In

Where an Institution has licensed Vera, students sign in to complete an assigned assessment. They do so using credentials that myHeggerty generates automatically for each student within their school's account — a printed QR code badge, or a password. No setup by the school is required to create them. Students do not create accounts, choose their own username or password, or provide any information about themselves in order to sign in. A student's password can be regenerated at any time, after which the previous password can no longer be used to sign in. Students are not asked for an email address, a phone number, or any contact information at any point, and Heggerty does not send marketing communications to students. Scanning a QR code badge uses the camera on the student's device to read the code. Because the students using Vera are pre-readers, the student-facing experience is designed to be operated without reading. Notice of Heggerty's data practices is therefore directed to parents and guardians through their school or district, as described in this Section 1 and Section 10, rather than to the student.

Literacy Resources Contact Information

Privacy Officer
Email: privacy@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: This Website 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.
- **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.
- **Usage Data** – information about how you use our Website, products and services.
- **Marketing and Communications Data** – preferences in receiving marketing and communication preferences.

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, including phonemic awareness performance scores generated from Vera assessments.
- Session identifiers associated with assessment activity
- **Student Sign-In Credentials** — where an Institution has licensed Vera, the means by which a student signs in to complete an assigned assessment: a printed QR code badge, and a password generated by Heggerty for that individual student. Students do not choose their credentials, and no username is used. A student's password can be regenerated at any time, after which the previous password can no longer be used to sign in. Credentials contain no contact information.
- **Audio Recordings** — where an Institution has licensed Vera, digital recordings of a student's voice captured during phonemic awareness assessment tasks. Collected only while the student is completing an assessment item.
- **ASR Transcripts** — internal automated speech recognition transcripts generated by Heggerty's own systems from Audio Recordings. Used to produce assessment scores. Not shared with third parties as a separate data element.
- **Intermediate ASR Processing Artifacts** — phoneme-level features, spectral embeddings, or speaker-diarization artifacts generated during ASR transcription. Treated as Biometric PII under amended COPPA §312.2 and deleted on the same schedule as the underlying Audio Recording. Not retained as a separate data category and not shared with any third party.

2.2 Voice Recordings as Biometric PII Under COPPA

Under amended COPPA §312.2 (effective April 22, 2026), "personal information" includes voiceprints and other biometric identifiers that can be used for the automated or semi-automated recognition of an individual. Audio Recordings collected through Vera fall within this definition because they contain voice characteristics capable of supporting speaker recognition, regardless of whether Heggerty actively extracts such characteristics. Heggerty does not use Audio Recordings to identify or authenticate any individual, does not create voiceprints for that purpose, and does not permit any third party to do so. Automated speech recognition is used solely to score assessment responses.

Heggerty treats all Audio Recordings as Biometric PII. This means:

- Audio Recordings are subject to the most protective data handling controls available within Heggerty's systems.
- Audio Recordings are stored separately from general assessment data, in a private AWS S3 bucket with server-side encryption (SSE-S3), accessible only via time-limited presigned URLs.
- Audio Recordings are subject to a shorter retention period than other student data. See Section 8.
- Voiceprint embeddings or speaker-identification artifacts generated internally by Heggerty's ASR system are treated as Biometric PII and deleted on the same schedule as the underlying Audio Recording.
- All intermediate ASR processing artifacts — including phoneme-level features, spectral embeddings, and speaker-diarization data generated during transcription — are also treated as Biometric PII and deleted on the same schedule, regardless of whether Heggerty actively uses them for speaker recognition purposes.

- Voiceprint embeddings are never shared with any third party.

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 on our Website
- Subscribe to our service or publications
- Request marketing to be sent to you
- Conduct a survey or give us feedback

Student assessment activity – Where an Institution has licensed Vera, we collect audio recordings of a student's voice directly from the student while the student completes an assigned assessment. Recording occurs only during an active assessment item.

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 site 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 this Website, 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 Website
- To deliver relevant Website content and advertisements to you
- To use data analytics to improve our Website, products/services, and marketing
- To make suggestions and recommendations about goods or services

Vera assessment scoring. Audio Recordings collected through Vera are processed by Heggerty's own automated speech recognition systems to produce phonemic awareness assessment scores, which are delivered to Authorized Educators through the myHeggerty dashboard. Recordings are also available to Authorized Educators for review of scored items.

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.

Heggerty maintains a written Information Security Program (ISP) that complies with amended COPPA §312.8. Technical safeguards applicable to student data, including Vera audio, include:

- Audio Recordings stored in a private AWS S3 bucket with server-side encryption (SSE-S3); no public bucket policy.
- Access to Audio Recordings controlled via IAM roles; accessible only via time-limited presigned URLs generated by Heggerty's application.
- AWS CloudTrail enabled on the student recordings S3 bucket; access events logged to CloudWatch.
- Student database encrypted at rest using AES-256 encryption.
- All data in transit encrypted using TLS 1.2 or higher.
- Access to Student Data governed by role-based access controls and least-privilege principles.
- Multi-factor authentication required for all Heggerty employees with access to production systems.
- Presigned S3 URLs expire automatically; report CSVs not transmitted in email bodies.
- Analytics tools suppressed during authenticated student assessment sessions.
- Student sign-in credentials are generated by Heggerty and provided to students through the Institution. A password can be regenerated at any time by staff with access to that class within the Services, after which the previous password can no longer be used to sign in.

Heggerty's ISP is available to Institution upon written request. Heggerty conducts annual risk assessments and annual tabletop exercises to test its Incident Response program.

7. SECURITY INCIDENT NOTIFICATION

In the event of a Security Incident affecting Student Data — including Audio Recordings — Heggerty will notify Institution in writing within 48 hours of discovering the incident. This timeline applies regardless of whether the full scope of the incident has been determined, and is not conditioned on completion of an internal investigation.
A Security Incident includes any actual or reasonably suspected: unauthorized access to or acquisition of Student Data; loss or theft of devices containing Student Data; ransomware or malware affecting systems that contain Student Data; or unauthorized use or disclosure by an employee, contractor, or subprocessor.
Within 10 business days of the initial notice, Heggerty will provide a follow-up notice describing remediation steps, assessment of harm, and any changes to security procedures. Heggerty will cooperate with Institution in preparing any required notifications to parents, students, or regulatory authorities.

8. 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.

Audio Recordings are retained on a shorter schedule than other student data. They are automatically and permanently deleted one year from the date of the assessment, enforced by an automated storage lifecycle rule. Earlier deletion is triggered by: (a) an Institution's written deletion request, fulfilled within 2 business days; (b) termination of the Service Agreement; or (c) revocation of school authorization.

Data Category	Retention Period
Audio Recordings (Biometric PII)	One year from the date of the assessment, enforced by an automated storage lifecycle rule. Earlier deletion on written Institution request (2 business days), termination, or revocation of authorization.
Intermediate ASR Artifacts (Biometric PII)	Deleted on the same schedule as the underlying Audio Recording. Not retained

	separately.
ASR Transcripts (internal)	Retained with standard assessment data — up to 7 years on active accounts, hard-deleted 2 years post-closure.
Student Sign-In Credentials	Retained with the student's record and deleted on the same schedule as other Student Data. A password can be regenerated at any time, after which the previous password can no longer be used to sign in. A student's credentials stop working once a parent has declined Vera for that student, or the Institution has withdrawn that student from Vera.
Assessment Results & Scores	Up to 7 years on active accounts; 2-year post-closure lifecycle as described above. On-demand deletion fulfilled within 2 business days at any point.
Audit Logs (FERPA §99.32)	Minimum 3 years from date of access event. Not deleted when student records are deleted.
Teacher / Admin Credentials	Same 2-year post-closure lifecycle as student data. On-demand deletion within 2 business days.
Application and infrastructure logs	Request logs for myHeggerty and the educator-facing mobile applications, including client IP address, are retained in Heggerty's AWS environment for 2 years from collection, then automatically deleted.
Mobile app analytics and diagnostics	Retained by Datadog for 30 days, then deleted or retained only in aggregated, de-identified form. See Section 13.

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.

9. 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 has been infringed. For revocation of consent to Heggerty's collection of a child's personal information, parents may also contact Heggerty directly at privacy@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 privacy@heggerty.org; Heggerty will fulfill such requests within 2 business days.

10. 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, including Audio Recordings.
- **Revocation through Institution:** Revoke school authorization through your school or district administrator, which will trigger deletion of Audio Recordings within 2 business days.
- **Refusal Before Activation:** Decline collection of voice recordings for your child before Vera is activated, by notifying your school or district administrator.
- **Withdrawal After Activation:** Withdraw your child from Vera at any time by notifying your school or district administrator. No further voice recordings will be collected, and existing recordings cannot be played back.
- **Right to File a Complaint:** File a complaint with the U.S. Federal Trade Commission (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 privacy@heggerty.org. Institutions may submit written deletion requests to Heggerty at privacy@heggerty.org; Heggerty will fulfill student data deletion requests within 2 business days of a verified written request.

Individuals who contact Heggerty directly will be referred to their Institution in the first instance. However, Heggerty will also honor direct parental revocation requests as described above, consistent with COPPA §312.5(b) and §312.6. Heggerty responds to Institution requests for Student Data within 15 business days.

11. STATE BIOMETRIC PRIVACY LAWS

In addition to COPPA, collection of voice recordings from students may trigger obligations under state biometric privacy laws, depending on where your school or district is located. Relevant statutes include:

- Illinois Biometric Information Privacy Act (740 ILCS 14) (BIPA)

- Texas Capture or Use of Biometric Identifier Act (Tex. Bus. & Com. Code §503.001)
- Washington My Health My Data Act (RCW 70.372) — includes biometric data provisions applicable to operators collecting biometric information from residents
- New York Education Law §2-d and associated biometric provisions
- Florida's limitation on the collection of student biometric information (Fla. Stat. §1002.222), the Florida Parents' Bill of Rights (Fla. Stat. ch. 1014), and the Florida Student Online Personal Information Protection Act (Fla. Stat. §1006.1494)
- California Student Online Personal Information Protection Act (Cal. Bus. & Prof. Code §22584) and California Consumer Privacy Act (Cal. Civ. Code §1798.100 et seq.)
- Similar statutes in other states where Institution operates

District responsibility. Heggerty's Data Privacy Agreement (or, for accounts without one, the Service Terms accepted for the Institution's account) places responsibility on Institution to comply with applicable state biometric privacy laws before enabling Vera for any student. Heggerty will cooperate with Institution in providing information necessary to fulfill these obligations. As stated in Section 1, the school authorization consent model addresses COPPA only and does not by itself satisfy a state-law requirement for direct written parental consent.

12. CALIFORNIA RESIDENTS' PRIVACY RIGHTS

In addition to the rights in Section 9, 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 privacy@heggerty.org.

13. 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, audio 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. Audio Recordings (Biometric PII) are stored in a

	private AWS S3 bucket. 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.
Nature of interaction	S3: private bucket with SSE-S3 encryption; access controlled via IAM roles; accessible only via time-limited presigned URLs generated by Heggerty's application. AWS acts as a storage processor only and does not access or analyze audio content; its contractual obligations expressly prohibit any analysis, use, or disclosure of audio content beyond infrastructure provision. SES: presigned S3 links to report CSVs delivered to authorized teachers and administrators only.
ASR processing	Automated speech recognition is performed entirely within Heggerty's own AWS infrastructure using Heggerty's proprietary model. It is not a third-party disclosure. AWS does not have access to audio content as part of ASR processing beyond its role as a compute infrastructure provider, and its access is contractually restricted to that role.
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 privacy@heggerty.org. Withdrawal of consent may result in the student's inability to use the assessment platform.

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. The Vera experience does not load Google Analytics, Wistia, advertising scripts, or other non-integral third-party content. 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).

(c) Educator-facing mobile applications. Heggerty's educator-facing mobile applications use one third-party processor for product analytics and diagnostics. No children's personal information is disclosed to this processor and it receives no student data. It is listed here for

transparency and to meet App Store and Google Play disclosure requirements.

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 and operating-system version. A client IP address is transmitted with these requests; it is filtered at Datadog and is not retained there. The IP address is not used to derive location and is not linked to account identity. No geolocation, GPS, or precise location is collected, and the data is 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 the underlying request 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, consistent with COPPA §312.8(c). Datadog acts solely as a processor on Heggerty's behalf, not for advertising or tracking.

14. RETENTION POLICY AND AUDITING

	AWS (S3 + SES)
Service Provider	Amazon Web Services, Inc.

Retention Period	Student identity, enrollment, and assessment records: duration of Service Agreement + 2 years post-closure, then hard-deleted. Audio Recordings and intermediate ASR artifacts: one year from the date of the assessment, enforced by an automated storage lifecycle rule. Audit logs (FERPA §99.32): 3 years from date of access event. Teacher/admin credentials: 2-year post-closure lifecycle; on-demand deletion within 2 business days. Application and infrastructure request logs: 2 years from collection.
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. Access to Audio Recordings is logged on the same basis as other Student Data access.

15. PERSISTENT IDENTIFIER DISCLOSURE

	AWS (S3 + SES)
Safeguards	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	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. Analytics tools are suppressed for authenticated student sessions.
Mobile application identifier	In Heggerty's educator-facing mobile applications, a randomly generated,

	app-specific analytics identifier is used to group diagnostic and performance events. It is not linked to a name or email address, is not an advertising identifier, and is not used in student-facing experiences.

16. DATA MINIMIZATION

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

- Audio Recordings are collected only during active Vera assessment sessions and only where Institution has licensed Vera.
- Vera is not part of myHeggerty by default; audio is collected only for Institutions that have licensed Vera, and only from students completing an assigned Vera assessment.
- Heggerty does not use Student Data — including Audio Recordings or ASR transcripts — to train, fine-tune, or develop general-purpose machine learning models whose outputs are used outside the provision of Services to Institution. Training of Heggerty's internal ASR systems for the benefit of Institution's Services is permitted, provided such training occurs entirely within Heggerty's AWS infrastructure and de-identified outputs are used consistent with Heggerty's de-identification standards.
- 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.

17. AUDIT LOGGING AND FERPA COMPLIANCE

Heggerty maintains durable audit logs of all access to Student Data, including Audio Recordings, consistent with FERPA §99.32. Each log entry records: the identity of the accessing party, denormalized at write time to remain complete and interpretable independent of any subsequent account deletion or archival; the date and time of access; the category of Student Data accessed; and the legitimate educational interest supporting the access.
Heggerty maintains separate administrative records of internal personnel actions, including access to customer accounts performed via account emulation for support or quality-assurance purposes. These records are available to Institution upon reasonable written request for purposes of compliance review, and not only in connection with a Security Incident investigation. Audit logs are retained for a minimum of 3 years from the date of the access event and are not deleted when student records are deleted. Heggerty will make audit logs available to Institution upon written request within 30 days.

18. NOTICE OF CHANGES AND CONTACT INFORMATION

Heggerty will notify institutions and, where required, parents of any material changes to this Policy via email or at login. This Policy will be updated to reflect any new third-party disclosures, changes to retention periods, or changes to data practices before those changes take effect.

Privacy Officer	privacy@heggerty.org
Postal Address	805 Lake St. #293, Oak Park, IL 60301
Data Deletion Requests	privacy@heggerty.org (fulfilled within 2 business days for student data)
Audit Log Requests	privacy@heggerty.org (fulfilled within 30 days of

	written request)
Parent Inquiries	Parents may contact Heggerty directly for revocation requests at privacy@heggerty.org. For other inquiries, contact your school or district administrator first; Heggerty will refer non-revocation direct inquiries to Institution.

19. DOCUMENT CHANGELOG

Date	Author	Change Summary
October 14, 2026	Steve Dumais	Added coverage of the Vera voice-enabled phonemic awareness assessment.
July 30, 2026	Steve Dumais	Mobile application introduction.
May 27, 2026	Chris Dugan	New sections — Data Minimization; document changelog.

© 2026 Literacy Resources, LLC. All rights reserved. | 805 Lake Street #293, Oak Park, IL 60301 | hello@heggerty.org