VerbalCheck

Data Processing Addendum

Choice Pursuits Technologies LLC

Version 1.1 • Effective Date: May 16, 2026 • Last Updated: May 16, 2026 • Institutional Review Document

Important Notice. This Data Processing Addendum is provided for institutional review. It does not create authorization to use VerbalCheck with Student Data unless accepted by an authorized institutional representative or incorporated into a written agreement, purchase order, pilot approval, or other authorized institutional arrangement. This DPA is designed to satisfy GDPR Article 28(3), CCPA / CPRA service provider requirements, FERPA school official requirements, and the supplemental information requirements of New York Education Law § 2-d / 8 NYCRR Part 121.

1. Purpose and Relationship to Primary Agreement

This Data Processing Addendum ("DPA" or "Addendum") applies to the processing of Personal Data and Student Data by Choice Pursuits Technologies LLC ("Choice Pursuits") in connection with the VerbalCheck platform. This document is intended to support review by an institution, legal department, procurement office, privacy officer, information technology office, accessibility office, or other authorized reviewer.

If VerbalCheck is used under a separate written agreement, pilot authorization, purchase order, institutional approval, or other written arrangement, this Addendum supplements that arrangement. If no separate written institutional arrangement exists, this Addendum applies only to the extent it has been accepted by an authorized representative of the institution or other Authorized Customer.

This Addendum does not create institutional approval for use of VerbalCheck where institutional approval, procurement review, data privacy review, security review, accessibility review, or legal review is required.

2. Parties and Roles

Controller / Processor. The institution or Authorized Customer is the Controller of institutional Personal Data and student Education Records. Choice Pursuits Technologies LLC is the Processor when it processes such data through VerbalCheck on behalf of the Controller.

Service Provider / Processor (U.S.). For purposes of the California Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA), Colorado Privacy Act, Connecticut Data Privacy Act, Virginia Consumer Data Protection Act, Utah Consumer Privacy Act, Oregon Consumer Privacy Act, Texas Data Privacy and Security Act, Tennessee Information Protection Act, Montana Consumer Data Privacy Act, and analogous

statutes, Choice Pursuits acts as a “service provider,” “processor,” or analogous role on behalf of the Controller.

School Official (FERPA). When VerbalCheck processes Education Records for a participating institution, Choice Pursuits is designated as a school official with a legitimate educational interest under 34 C.F.R. § 99.31(a)(1)(i)(B), subject to the institution’s direct control.

Responsibility. The institution remains responsible for determining whether VerbalCheck may be used with Student Data, what data may be submitted, how long data may be retained, and what decisions may be made using the Services. Choice Pursuits will process data only as needed to provide the Services and only according to the Controller’s written instructions, the applicable agreement, this Addendum, and applicable law. Choice Pursuits is responsible for the acts and omissions of its Subprocessors with respect to data protection obligations under this Addendum as if they were its own.

3. Key Definitions

For consistency, defined terms used in this Addendum, the Privacy Policy, and the Terms of Service share the meanings below.

- **Authorized Customer** means an institution, school district, or other organization that has accepted these terms or executed an institutional agreement, purchase order, or pilot authorization permitting use of VerbalCheck.
- **Controller** means the institution or Authorized Customer that determines the purpose and means of processing Personal Data.
- **Processor** means Choice Pursuits Technologies LLC when processing Personal Data on behalf of the Controller.
- **Personal Data** means information that identifies, relates to, describes, or can reasonably be linked to an individual.
- **Student Data** means Personal Data connected to a student, course, assignment, submission, recording, interview, evaluation, or Education Record.
- **Education Records** means has the meaning given in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(a)(4), and applicable implementing regulations at 34 C.F.R. Part 99.
- **Institutional Data** means records, files, content, settings, course information, user data, Student Data, assignment data, or related information submitted by or on behalf of the institution.
- **Services** means the VerbalCheck platform, including standalone access, assignment workflows, academic integrity support, AI-assisted review, reporting, file storage, audio services, administrative features, and related support.
- **Subprocessor** means a service provider engaged by Choice Pursuits to process Personal Data in support of VerbalCheck, including any sub-subprocessor engaged by a Subprocessor.

- **De-Identified Data** means data that has been processed to remove or modify direct and indirect identifiers so that the data can no longer reasonably be linked to an individual, consistent with reasonable de-identification standards (such as NIST Special Publication 800-188 or analogous standards) and the legal standards in the CCPA/CPRA and similar state laws.
- **Aggregated Data** means De-Identified Data that has been combined or summarized so that individual data points cannot reasonably be associated with an identifiable individual.
- **Reportable Security Incident** means a confirmed event of unauthorized access to, acquisition of, disclosure of, alteration of, loss of, or destruction of Personal Data processed by VerbalCheck. Unsuccessful attempts that do not result in confirmed unauthorized access (including routine port scans, login failures, denial-of-service activity that does not compromise data, and similar events) are not Reportable Security Incidents.
- **AI-Assisted Output** means AI-generated or AI-supported indicators, summaries, scoring support, authorship support, flags, comments, transcripts, retrieval results, or other decision-support information produced through the platform.
- **Business Purpose** means for the avoidance of doubt under U.S. state privacy laws, the operational purposes set forth in this Addendum and the applicable agreement, including providing, securing, supporting, and improving the Services.

4. Privacy Law Coverage, FERPA, and Service Provider Status

General. Choice Pursuits will process Personal Data in accordance with applicable privacy and data protection laws, including FERPA, the Children's Online Privacy Protection Act (COPPA) where applicable, the Protection of Pupil Rights Amendment (PPRA), and other applicable United States federal or state privacy laws. Where applicable, the parties may separately agree to additional regional or international privacy requirements, including obligations under the EU and UK General Data Protection Regulation (GDPR), Quebec Law 25, and Brazil LGPD.

FERPA School Official. When VerbalCheck processes Education Records for a participating institution, Choice Pursuits is designated as a school official with a legitimate educational interest under 34 C.F.R. § 99.31(a)(1)(i)(B), subject to the institution's direct control with respect to the use and maintenance of Education Records. Choice Pursuits will (a) use Education Records only to perform institutional services for which it would otherwise use employees, (b) not redisclose Education Records except as permitted under 34 C.F.R. § 99.33(a) or as directed by the institution, and (c) use Student Data only to provide the Services, support academic integrity and instructional workflows, maintain security, provide support, satisfy legal obligations, and perform activities authorized by the institution.

CCPA / CPRA Service Provider. With respect to Personal Data subject to the CCPA/CPRA, Choice Pursuits, as a service provider, is prohibited from and will not:

- Sell or share Personal Data within the meaning of the CCPA/CPRA.

- Retain, use, or disclose Personal Data for any purpose other than the specific Business Purposes described in this Addendum and the applicable agreement, including not retaining, using, or disclosing Personal Data outside the direct business relationship between the parties.
- Retain, use, or disclose Personal Data for the service provider's own commercial purposes.
- Combine Personal Data received from or on behalf of the Controller with Personal Data the service provider receives from or on behalf of another person, or collects from its own interaction with the consumer, except as expressly permitted by applicable regulation.

Choice Pursuits certifies that it understands these restrictions and will comply with them. Choice Pursuits will notify the Controller if it determines it can no longer meet its obligations under the CCPA/CPRA, and will, on reasonable notice, allow the Controller to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Data. Choice Pursuits will assist the Controller in responding to verifiable consumer requests for access, deletion, correction, opt-out, and limit-use-of-sensitive-personal-information rights as further described in Section 20.

Other U.S. State Privacy Laws. With respect to Personal Data subject to the Colorado Privacy Act, Connecticut Data Privacy Act, Virginia Consumer Data Protection Act, Utah Consumer Privacy Act, Oregon Consumer Privacy Act, Texas Data Privacy and Security Act, Tennessee Information Protection Act, Montana Consumer Data Privacy Act, or analogous statutes, Choice Pursuits, as processor, will (a) process Personal Data only on the documented instructions of the Controller, (b) ensure persons authorized to process Personal Data are subject to a duty of confidentiality, (c) implement appropriate technical and organizational measures as set forth in Section 12, (d) engage Subprocessors only as set forth in Section 14, (e) assist the Controller with consumer rights requests and data protection assessments, and (f) return or delete Personal Data as set forth in Section 16.

No Sale; No Cross-Context Behavioral Advertising; No Training on Student Data. Choice Pursuits will not (i) sell Personal Data or Student Data, (ii) use Student Data for advertising, cross-context behavioral advertising, or behavioral marketing, (iii) use Student Data to create unrelated consumer profiles, (iv) use customer Student Data to train, fine-tune, or otherwise improve generally available models, or (v) intentionally redisclose Student Data except as necessary to provide the Services through approved Subprocessors, as directed by the institution, as required by law, or as otherwise authorized in writing by the institution.

5. Institutional Permission and Standalone Faculty Use

If VerbalCheck is used as a standalone application by faculty or other users, those users are responsible for confirming that such use is permitted by their institution before uploading Student Data or Education Records. Choice Pursuits may restrict, suspend, or deny use when it reasonably believes the use is not authorized, creates a privacy risk, or conflicts with applicable institutional requirements.

Faculty users should not upload Education Records, student assignment submissions, audio files, transcripts, course records, or related Institutional Data unless such use is permitted by their institution and consistent with applicable law and institutional policy.

6. Processing Purposes

Choice Pursuits processes Personal Data only for the following purposes (each a Business Purpose):

- Academic integrity support, authorship review, assignment workflow support, interview workflows, instructor review, and related instructional support.
- Creation, storage, processing, transcription, scoring support, and reporting of assignment submissions, interview responses, audio files, transcripts, and related review materials.
- Administrative account management, authentication, course or class management, user support, troubleshooting, service improvement, and product security.
- Internal application analytics based on platform data, such as class activity, assignment activity, usage trends, administrative dashboards, and operational reporting.
- Compliance, legal review support, incident investigation, audit response, enforcement of terms, and enforcement of acceptable use requirements.

7. Categories of Data

- User account information, including name, email address, role, institution, authentication information, and account activity.
- Student identifiers and enrollment context, including student name, student email, course information, class information, instructor information, assignment names, submission identifiers, and related academic context.
- Assignment content, including uploaded documents, text responses, interview answers, written reflections, drafts, faculty questions, rubrics, prompts, feedback, and related coursework data.
- Audio, speech, transcription, and interview data where those features are used, including audio files, speech-to-text output, text-to-speech output, interview recordings, and related processing metadata.
- AI-Assisted Output, including retrieval results, authorship support information, generated summaries, scoring support, flags, comments, and instructor review aids.
- System metadata and logs, including IP address, browser information, device information, timestamps, authentication events, security logs, upload history, error logs, and usage records.
- Support communications and administrative records submitted by users, faculty, institutional contacts, or support personnel.

8. Student and Institutional Data Ownership

The institution retains ownership and control of institutional records, student records, assignment submissions, educational data, transcripts, audio files, and related institutional content processed through VerbalCheck.

Choice Pursuits receives only the limited rights necessary to process such data for purposes authorized by the institution and described in the applicable agreement, this Addendum, and any applicable written institutional instructions.

Nothing in this Addendum transfers ownership of Institutional Data, Student Data, Education Records, assignment content, or related institutional records to Choice Pursuits.

9. Data Use Limits

- Choice Pursuits will not sell Personal Data or Student Data.
- Choice Pursuits will not use Student Data for advertising or behavioral marketing.
- Choice Pursuits will not use Student Data to create unrelated consumer profiles.
- Choice Pursuits will not disclose Student Data to unauthorized third parties.
- Choice Pursuits will not use customer Student Data to train, fine-tune, or otherwise improve models owned, controlled, or hosted by Choice Pursuits, and will not authorize Subprocessors to use customer Student Data to train or fine-tune their generally available models. AI Subprocessors are configured to disable training use of customer data as further described in Section 10.
- Choice Pursuits will use Institutional Data only to provide, secure, support, maintain, improve, or legally protect the Services, unless otherwise authorized by the institution in writing.

De-Identified and Aggregated Data. Choice Pursuits may create and use De-Identified Data and Aggregated Data derived from Institutional Data to operate, secure, troubleshoot, evaluate, and improve the Services. Choice Pursuits will:

- Apply reasonable de-identification techniques consistent with recognized standards (such as NIST SP 800-188) and the legal standards in the CCPA/CPRA and similar state laws.
- Implement administrative and technical controls reasonably designed to prevent re-identification.
- Publicly commit not to attempt re-identification of De-Identified Data and contractually prohibit recipients from doing so.
- Not publish De-Identified Data in a manner that identifies the institution without prior written consent.
- Not use De-Identified Data or Aggregated Data derived from customer Student Data to train Choice Pursuits owned or controlled generally available models.

10. AI Processing, OpenAI Zero Data Retention, and AI Output Disclaimer

VerbalCheck uses OpenAI as the active AI service provider for AI help, retrieval, speech-to-text, text-to-speech, audio services, and related AI-assisted features. Choice Pursuits has enabled OpenAI's Zero Data Retention (ZDR) configuration for the API endpoints used by VerbalCheck. Under ZDR, OpenAI does not retain prompt or completion content sent through covered API endpoints after the request is processed, and customer content sent through these endpoints is not used to train OpenAI models.

AI Subprocessor Review. Choice Pursuits reviews the privacy, security, and data-handling practices of its AI Subprocessors at least annually and again whenever a material change to the Subprocessor's data-handling terms is announced. Material changes affecting institutional Student Data will be reflected in the Subprocessor Register and handled under Section 14.

If Choice Pursuits engages additional AI service providers in the future, it will use commercially available configurations intended to prevent customer Student Data from being used for generalized model training and will update the Subprocessor Register accordingly.

AI-Assisted Output is probabilistic in nature and may contain inaccuracies, incomplete information, false positives, or false negatives. AI-generated indicators, scoring assistance, authorship analysis, summaries, transcripts, retrieval results, comments, or flags are intended solely as decision-support tools and must not be treated as conclusive evidence of misconduct, authorship, grading outcomes, or disciplinary violations.

The institution, faculty member, or other authorized educational decision maker remains responsible for reviewing AI-Assisted Output, considering context, following institutional policy, and making any final decision involving grading, academic integrity, student discipline, or student rights.

11. Voice, Audio, and Biometric Data

VerbalCheck may collect, store, and process audio recordings, interview responses, speech input, speech output, transcripts, and related audio processing metadata when voice-based features are used. VerbalCheck uses this information to support assignment workflows, interview workflows, transcription, instructor review, academic integrity review, accessibility support, and related educational purposes.

No Biometric Identifiers. VerbalCheck does not intentionally create, enroll, store, or use voiceprints, speaker identification templates, speaker verification profiles, faceprints, or other biometric identifiers or biometric information for the purpose of identifying or authenticating any individual. VerbalCheck does not generate biometric identifiers within the meaning of the Illinois Biometric Information Privacy Act (740 ILCS 14/), the Texas Capture or Use of Biometric Identifier Act (Tex. Bus. & Com. Code § 503.001), the Washington biometric identifiers statute (RCW 19.375), the New York City biometric identifier law (NYC Admin. Code § 22-1201 et seq.), or analogous state laws, and does not perform automated speaker recognition.

Future Features. If a future feature would create or use biometric identifiers, biometric information, or speaker-recognition templates, Choice Pursuits will (a) update this Addendum and the Privacy Policy, (b) require the institution's written authorization before enabling the feature for that institution, and (c) implement notice, consent, retention, destruction, and disclosure controls required by applicable biometric privacy laws.

Other Designations. Audio recordings, transcripts, and related materials may still constitute Education Records, sensitive personal information, or regulated information under applicable state law depending on how they are used, stored, or processed. Where applicable law or institutional policy requires notice, consent, written authorization, or additional terms before collecting or processing voice-related data, the institution and Choice Pursuits will work through the applicable institutional approval process before such use.

Choice Pursuits will not sell, lease, disclose, or use voice-related data for advertising, unrelated profiling, unrelated biometric identification, or unrelated authentication.

12. Security Safeguards

Choice Pursuits maintains administrative, technical, and organizational safeguards designed to protect Personal Data against unauthorized access, misuse, alteration, disclosure, loss, or destruction, with the objective of protecting the confidentiality, integrity, and availability of Personal Data (the "CIA Triad"). The security program is aligned with the NIST Cybersecurity Framework. Choice Pursuits is working toward SOC 2 Type II attestation. Safeguards are appropriate to the risk of the processing in light of the state of the art, costs of implementation, and the nature, scope, context, and purposes of processing, consistent with GDPR Article 32(2).

- Encryption in transit using Transport Layer Security (TLS) version 1.2 or higher for communications between users, the application, and Subprocessors.
- Encryption at rest using AES-256 (or substantially equivalent algorithms supported by hosting, database, and storage Subprocessors) for stored Personal Data.
- Encryption key management consistent with industry practice (such as use of provider-managed key management services with documented key rotation, access controls, and audit logging).
- Multi-factor authentication for administrative access, production access, and access to Subprocessor consoles handling Personal Data.
- Role-based access controls and least-privilege access for administrative functions, with periodic access reviews (at least quarterly for production access).
- Administrative access limited to personnel or contractors with a legitimate business need.
- Written confidentiality obligations for personnel or contractors who may access Personal Data.

- Background screening, where permitted by law, for personnel with access to production environments containing Student Data, including criminal history and employment verification appropriate to the role.
- Annual privacy and security awareness training for personnel with access to Personal Data, covering FERPA, COPPA where applicable, biometric and voice data, AI/ML privacy considerations, incident response, and social engineering awareness, with role-specific training for engineering personnel.
- Audit logging, security logging, and monitoring appropriate to the operational stage of the platform, with logs retained for a period appropriate to the security needs and applicable law.
- Secure software development practices, code review where practical, dependency and vulnerability scanning, secure credential management, environment variable protection, and separation of production and non-production environments.
- Vulnerability management practices, including periodic dependency review, vulnerability scanning, and patching of known security vulnerabilities within risk-based timelines.
- Annual penetration testing or vulnerability assessment by an independent qualified third party once the platform reaches production scale, with executive summaries available to institutional reviewers under NDA.
- Backup, recovery, and deletion practices consistent with platform capabilities and agreed institutional requirements.
- Documented incident response procedures supporting investigation, mitigation, documentation, institutional cooperation, and required notifications.
- A coordinated vulnerability disclosure channel at security@choicepursuits.com for good-faith security researchers.

Privacy by Design. Choice Pursuits considers data protection principles, including data minimization, purpose limitation, and security, in the design and modification of the Services.

13. Confidentiality

Each party agrees to protect confidential information disclosed by the other party using reasonable administrative, technical, and organizational safeguards and not to disclose such information except as required to provide the Services, comply with law, fulfill institutional obligations, respond to lawful requests, or perform obligations under the applicable agreement.

Confidential information includes nonpublic business information, institutional records, Student Data, system configurations, security-related information, proprietary materials, and other information reasonably understood to be confidential based on the nature of the information or the circumstances of disclosure.

These confidentiality obligations survive termination of the Services to the extent needed to protect confidential information and comply with applicable law.

14. Subprocessors and Subprocessor Register

Use of Subprocessors. Choice Pursuits may use Subprocessors to provide, host, secure, store, transmit, process, analyze, or support VerbalCheck.

Flow-Down Obligations. Choice Pursuits will require Subprocessors, by written contract, to (a) process Personal Data only as needed to support VerbalCheck and only for the Business Purposes described in this Addendum, (b) be bound by confidentiality, privacy, and security obligations no less protective than those in this Addendum, including the CCPA/CPRA service provider restrictions in Section 4, and (c) impose the same obligations on any sub-subprocessor engaged to process Personal Data on the Subprocessor's behalf.

Liability for Subprocessors. Choice Pursuits remains liable to the Controller for the acts and omissions of its Subprocessors with respect to the data protection obligations under this Addendum as if such acts and omissions were Choice Pursuits' own.

Subprocessor Register. The current Subprocessor Register is maintained at https://verbalcheck.com/subprocessors and is incorporated into this Addendum by reference. The Subprocessor Register identifies the provider, the service or system provided, the purpose of the processing, and the deployment status of each Subprocessor.

Notice and Objection Procedure. Choice Pursuits will provide at least thirty (30) days' advance notice before adding or replacing a material Subprocessor that processes Student Data, by updating the Subprocessor Register and (where the institution has subscribed to update notifications) sending notice to the designated institutional contact. The Controller may object to a new material Subprocessor within fifteen (15) days of notice based on reasonable data protection, security, legal, or institutional policy concerns. The parties will work in good faith to resolve the objection. If the parties cannot resolve the objection, the Controller may terminate the Services with respect to the affected processing without penalty, subject to obligations regarding return or deletion of data.

Disposition Upon Subprocessor Replacement. When a Subprocessor is replaced, Choice Pursuits will use commercially reasonable efforts to ensure that Personal Data is migrated to the replacement provider and securely deleted from the prior provider in accordance with that provider's standard deletion processes.

Institutions may subscribe to Subprocessor change notifications by contacting privacy@choicepursuits.com.

15. Data Residency and International Transfers

Default Residency. Personal Data processed through VerbalCheck is stored and processed within the United States using approved Subprocessors identified in the Subprocessor Register. Cross-border data transfers, if any, will be handled in accordance with applicable law and institutional requirements.

Transfer Mechanisms. For institutions or data subjects in the European Economic Area, the United Kingdom, or Switzerland, Choice Pursuits will, on reasonable written request, support lawful cross-border transfers through one or more of the following mechanisms (as applicable and as updated by competent authorities):

- The European Commission Standard Contractual Clauses (SCCs), Module 2 (Controller-to-Processor) (and Module 3 (Processor-to-Processor) where Choice Pursuits engages a non-EU Subprocessor).
- The United Kingdom International Data Transfer Addendum to the SCCs (UK IDTA) or the UK International Data Transfer Agreement.
- Where Choice Pursuits is self-certified, the EU–U.S. Data Privacy Framework, the UK Extension to the EU–U.S. Data Privacy Framework, and the Swiss–U.S. Data Privacy Framework, in each case where the recipient is also self-certified.
- Other transfer mechanisms recognized as adequate by competent authorities, including successor mechanisms to the SCCs or DPFs.

Transfer Impact Assessment. Where required under applicable law, Choice Pursuits will conduct or cooperate with a transfer impact assessment evaluating the laws of the recipient country and any supplementary measures applied to protect transferred Personal Data.

Specific Residency Requirements. If the institution requires specific data residency terms (such as in-state hosting), regional processing limitations, or additional transfer safeguards, those requirements should be stated in the applicable institutional agreement or written instructions accepted by Choice Pursuits.

16. Retention, Return, and Deletion

Unless a different period is set by the institution or required by law, VerbalCheck retains student submissions, interview responses, audio files, transcripts, AI-Assisted Output, and related assignment records only for as long as reasonably necessary to provide the Services, support academic review, address disputes, maintain security, and comply with applicable obligations.

Recommended Default. A recommended default retention period for institutional review is 180 days after the end of the applicable course, pilot, or assignment review period, unless the institution directs a shorter or longer period.

Backups. Backup copies may remain for a limited period according to provider backup cycles and operational needs before scheduled deletion, generally not exceeding 35 days after deletion from

production systems. Choice Pursuits does not restore deleted Personal Data from backups except as required to respond to a security incident, legal obligation, or documented institutional request.

Termination Assistance Period. For sixty (60) days following termination of the applicable agreement (or such other period as the parties agree in writing), Choice Pursuits will, on written request from an authorized institutional representative, make Institutional Data available for export in a documented machine-readable format (such as CSV or JSON) appropriate to the data category. Following the Termination Assistance Period, Choice Pursuits will return or delete Institutional Data according to the institution's instructions, subject to legal obligations, security requirements, backup limitations, and reasonable technical constraints.

Certification of Deletion. Choice Pursuits will, on written request from an authorized institutional representative, provide written certification of deletion of Institutional Data from production systems.

17. Security Incident Notification and Cybersecurity Responsibilities

Initial Notice. Choice Pursuits will notify the Controller without undue delay and, where feasible, within seventy-two (72) hours after confirming a Reportable Security Incident involving Personal Data processed through VerbalCheck. The notice will include, to the extent then known: (a) the nature of the incident, (b) the categories and approximate number of data subjects concerned, (c) the categories and approximate number of records concerned, (d) the likely consequences of the incident, (e) the measures taken or proposed to address the incident and mitigate possible adverse effects, and (f) a point of contact for further information.

Follow-Up Report. Within thirty (30) days following the initial notice, or as otherwise agreed by the parties, Choice Pursuits will provide a written follow-up report describing investigation findings, root cause (to the extent then known), remediation steps, and recommended actions for the Controller. Where information is not yet available at the time of the initial notice, Choice Pursuits will provide updates as material new information is confirmed.

Cooperation. Choice Pursuits will cooperate reasonably with the Controller in investigating, mitigating, documenting, and responding to a confirmed Reportable Security Incident, including providing information reasonably needed for the Controller's legal, regulatory, and institutional notification obligations under state breach notification laws, FERPA, COPPA, GDPR Article 33/34, and other applicable laws.

Direct Notification. Where required by applicable law and not in conflict with the Controller's instructions, Choice Pursuits may also provide notice directly to affected individuals or regulators, in coordination with the Controller. Notice may be delayed where law enforcement or applicable law requires delay.

Internal Obligations. Each party remains responsible for its own internal legal obligations, reporting obligations, regulatory responsibilities, and institutional response obligations unless otherwise agreed in writing.

18. Audit, Documentation, and Institutional Review

Documentation. The Controller may request reasonable written responses to security questionnaires, privacy questionnaires, accessibility questionnaires, vendor review forms, procurement forms, or similar documentation. Choice Pursuits will provide commercially reasonable cooperation during institutional review.

On reasonable written request and subject to appropriate confidentiality protections, Choice Pursuits will provide:

- A current response to the Higher Education Community Vendor Assessment Toolkit (HECVAT) or analogous vendor security assessment.
- A current Voluntary Product Accessibility Template (VPAT) describing the platform's alignment with WCAG 2.1 Level AA.
- An executive summary of the most recent annual penetration test or independent security assessment, once such assessments are routinely conducted.
- Documentation describing data processing activities, security safeguards, Subprocessors, privacy practices, accessibility review, and incident response processes.
- Where Choice Pursuits later obtains a SOC 2 Type II report (or analogous independent attestation), a copy of the report or executive summary will be made available subject to confidentiality. Choice Pursuits does not currently maintain a SOC 2 Type II report and will not represent that it does until one is issued by an independent auditor.

On-Site Audits. On-site audits, intrusive penetration tests, or direct inspection of production systems are not required unless mutually agreed in writing and subject to appropriate confidentiality, security, scheduling, and operational limits. Where required by applicable law (including GDPR Article 28(3)(h)), Choice Pursuits will permit and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to the following conditions:

- The Controller will provide at least thirty (30) days' advance written notice of any on-site audit, except in the case of a confirmed Reportable Security Incident requiring immediate investigation.
- Audits will be conducted no more than once per twelve (12) month period, except in the case of a confirmed Reportable Security Incident or where required by a regulator.
- The auditor must execute appropriate confidentiality undertakings before access to information.
- Audits will be scheduled and conducted in a manner that does not unreasonably disrupt operations or compromise the security or confidentiality of other customers' data.

- Each party bears its own costs of routine annual audits. The Controller will reimburse Choice Pursuits' reasonable costs for any additional audits beyond the routine annual audit, except where an audit reveals material noncompliance, in which case Choice Pursuits will bear its own costs.

Records Retention. Choice Pursuits will retain records relevant to demonstrating compliance with this Addendum (including security logs, training records, and Subprocessor documentation) for a period reasonably necessary to support institutional audit and regulatory inquiries.

19. Accessibility Commitment

Choice Pursuits will make commercially reasonable efforts to support accessibility standards, including the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and to cooperate with institutional accessibility review processes. Accessibility improvements, remediation requests, and platform enhancements may be implemented as part of ongoing development efforts.

The institution may request reasonable accessibility documentation, testing information, remediation planning, or accessibility review materials when such information is necessary for institutional approval or continued use. On reasonable request, Choice Pursuits will provide a current Voluntary Product Accessibility Template (VPAT) or substantially similar conformance documentation. Accessibility-related communications may be directed to accessibility@choicepursuits.com.

20. Assistance with Rights, DPIAs, and Legal Requests

Data Subject and Consumer Rights. Choice Pursuits will provide reasonable assistance to the Controller in responding to student, parent, data subject, consumer, institutional, legal, or regulatory requests related to Personal Data processed through VerbalCheck, including requests for access, correction, deletion, restriction, portability, opt-out, and limit-use-of-sensitive-personal-information rights under applicable law. When a user contacts Choice Pursuits directly about Student Data controlled by an institution, Choice Pursuits may refer the request to the institution or respond according to institutional direction and applicable law.

DPIAs, TIAs, and Article 30 Records. Where the Controller is required by applicable law to conduct a Data Protection Impact Assessment (GDPR Article 35), Transfer Impact Assessment, data protection assessment under U.S. state laws, FERPA review, or similar evaluation involving Choice Pursuits' processing, Choice Pursuits will provide reasonable cooperation and information needed for the assessment, including descriptions of the nature, scope, context, and purposes of processing, the categories of Personal Data, applicable Subprocessors, security measures, and data transfer mechanisms. On reasonable request, Choice Pursuits will support the Controller's obligations to maintain a record of processing activities under GDPR Article 30 or analogous law.

Regulator Cooperation. Choice Pursuits will, to the extent required by applicable law, cooperate with reasonable inquiries from data protection authorities, attorneys general, educational regulators

(including state education departments), and other competent authorities relating to its processing activities under this Addendum.

Legal Requests. Choice Pursuits may disclose information when required by law, subpoena, court order, government request, or other lawful process, but will use reasonable efforts to notify the Controller when legally permitted and commercially practical, to allow the Controller to seek protective orders or alternative compliance. Choice Pursuits will object to overbroad requests where appropriate.

21. Insurance

Choice Pursuits maintains, or in the case of policies not yet in force will use commercially reasonable efforts to procure as the platform scales, insurance coverage appropriate to the operational scale, risk profile, and deployment stage of the platform, including:

- Cyber liability / technology errors and omissions insurance covering data breach response, privacy liability, and technology professional services.
- Commercial general liability insurance.
- Such other coverage as may be required by an executed institutional agreement.

Proof of Coverage. On reasonable request from an institutional reviewer, and subject to confidentiality, Choice Pursuits will provide a certificate of insurance evidencing the coverage in place at that time. Specific minimum limits, additional-insured requirements, waiver-of-subrogation requirements, and notice-of-cancellation provisions appropriate to the institution's risk profile should be stated in the applicable executed institutional agreement; the parties acknowledge that institutional minimum-limit requirements vary widely and are typically addressed in the master agreement rather than in this DPA.

22. Indemnification

IP Indemnification by Choice Pursuits. Choice Pursuits will defend and indemnify the institution against third-party claims alleging that VerbalCheck, as delivered by Choice Pursuits, directly infringes a valid United States patent, copyright, trademark, or trade secret, except to the extent the claim arises from institution-supplied content, misuse of the Services, unauthorized modifications, or combinations with unapproved systems or data. As remedy for an actual or threatened infringement claim, Choice Pursuits may, at its option, (a) procure the right for the institution to continue using the affected portion of the Services, (b) modify the affected portion to be non-infringing while substantially preserving functionality, or (c) on reasonable notice, terminate the affected portion and refund any prepaid fees applicable to the unused remainder of the term. This Section states Choice Pursuits' sole obligation and the institution's exclusive remedy for any third-party IP infringement claim with respect to the Services.

Indemnification by Institution. The institution will indemnify and hold harmless Choice Pursuits from claims arising from misuse of the platform, unlawful uploads, violations of institutional policy,

unauthorized disclosure of data by institutional users, or use of VerbalCheck in a manner not authorized by the applicable agreement or institutional policy.

Procedure. Indemnification obligations are subject to: (a) prompt written notice of the claim, (b) reasonable cooperation at the indemnifying party's expense, and (c) the indemnifying party's right to control the defense and settlement of the covered claim, provided that no settlement may impose liability, a non-monetary obligation, or an admission of fault on the indemnified party without that party's written consent. The indemnified party may participate in the defense with counsel of its own choosing at its own expense.

Public Institution Carve-Out. The institution's indemnification obligations under this Section apply only to the extent permitted by applicable law and do not require a public institution, school district, state agency, or governmental entity to assume an indemnification obligation prohibited by law.

23. Limitation of Liability

To the maximum extent permitted by law, neither party will be liable for indirect, incidental, consequential, special, punitive, or exemplary damages arising from or related to this Addendum or the use of VerbalCheck, even if advised of the possibility of such damages.

Aggregate Cap. Subject to the carve-outs below, Choice Pursuits Technologies LLC's total aggregate liability under this Addendum will not exceed the greater of (a) the total fees paid by the institution for the Services during the twelve (12) month period preceding the event giving rise to the claim, or (b) the amount specified in an executed institutional agreement. The parties acknowledge that the limitations of liability in this Section are an essential basis of the bargain and would apply even if a remedy fails of its essential purpose.

Excluded Claims. The cap in the preceding paragraph does NOT apply to, and there is no contractual cap on, liability arising from any of the following:

- Choice Pursuits' breach of its confidentiality obligations under Section 13.
- Choice Pursuits' breach of its data protection obligations under Sections 4 (Privacy Law Coverage, FERPA, and Service Provider Status), 9 (Data Use Limits), 10 (AI Processing), 11 (Voice, Audio, and Biometric Data), 12 (Security Safeguards), 14 (Subprocessors), 15 (Data Residency and International Transfers), and 16 (Retention, Return, and Deletion).
- Choice Pursuits' obligations under Section 17 (Security Incident Notification).
- Choice Pursuits' indemnification obligations under Section 22.
- Liability arising from gross negligence, willful misconduct, fraud, or violation of applicable law.
- Liability that cannot be limited or excluded under applicable law.

Nothing in this Section limits any rights or remedies that cannot be limited under applicable law.

24. New York Education Law § 2-d Commitment

For institutions that are educational agencies under New York Education Law § 2-d and 8 NYCRR Part 121, Choice Pursuits will, on request, execute an addendum that includes:

- The Parents Bill of Rights for Data Privacy and Security required under 8 NYCRR § 121.3.
- Supplemental information required under 8 NYCRR § 121.3(c), including (i) the exclusive purposes for which Student Data and teacher and principal data will be used, (ii) how Choice Pursuits will ensure that Subprocessors and assignees abide by data protection and security requirements, (iii) when the agreement expires and what happens to Student Data on expiration, (iv) procedures by which parents, eligible students, and other authorized persons may challenge the accuracy of Student Data, (v) where Student Data will be stored and the security protections in place, and (vi) how Choice Pursuits will encrypt Student Data while in motion and at rest.
- A representation that Choice Pursuits' data security and privacy plan aligns with the NIST Cybersecurity Framework.

In all events with respect to a New York educational agency, Choice Pursuits will (a) not sell Student Data, (b) not use Student Data for marketing or commercial purposes other than providing the Services, (c) maintain administrative, technical, and physical safeguards aligned with the NIST Cybersecurity Framework, and (d) provide notice and cooperation in the event of an unauthorized release of Student Data as required by § 2-d.

25. Modifications to This Addendum

Choice Pursuits may update this Addendum from time to time as VerbalCheck changes, laws evolve, Subprocessors change, or institutional requirements require clarification. Updated versions will include a new effective date and version number, and material changes will be summarized in the Revision History.

Notice. For material changes that affect institutional Student Data, privacy obligations, security commitments, or Subprocessor arrangements, Choice Pursuits will provide at least thirty (30) days' advance notice before the change takes effect, where reasonably practicable, through the Privacy Policy update process, the Subprocessor Register, email to the institutional contact, or another appropriate method. Some changes may take effect immediately when needed for security, legal compliance, or service protection.

Executed Institutional Agreements. Material changes affecting institutional Student Data under an executed institutional agreement will be handled through the applicable agreement, written amendment, or institutional notice process, and the executed institutional agreement controls to the extent of any conflict.

26. Governing Law and Venue

This Addendum is governed by and construed in accordance with the laws of the State of Oklahoma, without regard to conflict-of-law principles, unless otherwise specified in a fully executed institutional agreement.

Any dispute arising from or related to this Addendum will be resolved in the state or federal courts located in Oklahoma County, Oklahoma, unless the parties agree otherwise in writing or unless a fully executed institutional agreement provides a different venue. Nothing in this Section overrides a mandatory legal requirement applicable to a public institution, school district, state agency, governmental entity, or executed institutional agreement.

27. Conflict with Other Agreements

If this Addendum conflicts with a fully executed institutional agreement, the terms of the executed institutional agreement control for that institution unless the parties agree otherwise in writing. If a conflict exists between this Addendum and the public Terms of Service or Privacy Policy, the more specific institutional data protection term controls for institutional Student Data.

28. Survival

Confidentiality, security, data handling, data return, deletion, limitation on use, legal cooperation, indemnification, limitation of liability, audit cooperation, regulator cooperation, and governing law obligations survive termination of the Services to the extent needed to protect Personal Data, comply with law, and complete return or deletion obligations.

29. Notice and Contact Information

Company	Choice Pursuits Technologies LLC
Product	VerbalCheck
Privacy and Data Protection	privacy@choicepursuits.com
Security and Incident Response	security@choicepursuits.com
Accessibility	accessibility@choicepursuits.com
Legal Notices	legal@choicepursuits.com
Subprocessor Register	https://verbalcheck.com/subprocessors
Subprocessor Change Notices	Subscribe by emailing privacy@choicepursuits.com

Institutions are encouraged to designate a primary FERPA / privacy contact and a security incident contact at the time of agreement so that notices under this Addendum reach the appropriate institutional representative.

Schedule 1. Processing Details

Subject Matter	Processing of institutional Personal Data, Student Data, assignment data, audio data, transcripts, AI-Assisted Output, and related Education Records through VerbalCheck.
Duration	For the duration of the applicable agreement, pilot, course, assignment review period, or approved institutional use, plus any retention period required for service support, dispute handling, security, backup limitations, or legal obligations.
Nature and Purpose	To provide VerbalCheck Services, including academic integrity support, authorship review, assignment workflows, interview workflows, transcription, AI-assisted review, reporting, instructor review, account management, support, security, analytics, and compliance.
Data Subjects	Students, instructors, institutional administrators, staff, authorized users, parents or eligible students (where applicable), support contacts, and other individuals whose information is submitted to or processed through VerbalCheck.
Categories of Personal Data	Names, emails, roles, institution names, course details, assignment details, submissions, rubrics, prompts, audio files, transcripts, AI-Assisted Outputs, metadata, logs, support communications, and related academic context.
Sensitive or Regulated Data	Education Records and related institutional records may be processed when submitted by or on behalf of the institution. Audio recordings and transcripts may constitute sensitive personal information under applicable state law. Users should avoid submitting unnecessary sensitive personal information.
Retention	Recommended default retention is 180 days after the end of the applicable course, pilot, or assignment review period unless the institution directs otherwise or law requires a different period. See Section 16 for the differentiated retention schedule and 35-day backup cap.
Processing Location	Personal Data is processed in the United States by the Subprocessors listed in the Subprocessor Register at https://verbalcheck.com/subprocessors unless different terms are agreed in writing.

Transfer Mechanism	EU/UK Standard Contractual Clauses (Modules 2 and 3), UK IDTA, EU–U.S. / UK Extension / Swiss–U.S. Data Privacy Framework (where self-certified), and successor mechanisms — available on request for institutions or data subjects in the EEA, United Kingdom, or Switzerland.
Security Framework	NIST Cybersecurity Framework aligned; SOC 2 Type II in progress; annual penetration testing once at production scale (see Section 12).

An executable signature version of this Data Processing Addendum is available upon request for authorized institutional representatives.

Revision History

Version	Effective Date	Summary of Changes
1.0	May 8, 2026	Initial published version. Consolidates prior comprehensive draft (revision dated May 5, 2026); harmonizes definitions across the DPA, Privacy Policy, and Terms of Service; adds dedicated voice and biometric data section addressing BIPA, Texas CUBI, and Washington biometric statutes; tightens encryption commitments to TLS 1.2+ and AES-256; documents OpenAI Zero Data Retention configuration; adds 30/15-day Subprocessor change-notice and objection mechanics; adds termination assistance period with documented export formats; tightens Reportable Security Incident definition and adds 30-day post-incident report; adds HECVAT and SOC 2 documentation commitments; adds DPIA and Article 30 cooperation; adds GDPR Standard Contractual Clauses / UK IDTA commitment; adds de-identified and aggregated data carve-out; carves security, confidentiality, indemnity, and data-protection obligations out of the liability cap; references centralized Subprocessor Register.
1.1	May 16, 2026	Legal review revisions: adds Last Updated date; adds CCPA/CPRA service provider provisions with required statutory restrictions and certification of understanding; adds explicit processor commitments under Colorado, Connecticut, Virginia, Utah, Oregon, Texas, Tennessee, and Montana comprehensive privacy laws; expands FERPA commitments to include PPRA where applicable; adds dedicated Section 24 New York Education Law § 2-d / 8 NYCRR Part 121 commitment with Parents Bill of Rights and supplemental information; adds dedicated Section 25 Modifications to this DPA with 30-day advance-notice commitment; expands Section 2 Parties and Roles to explicitly include CCPA service provider status and Choice Pursuits' liability for Subprocessor acts and omissions; expands Section 12 Security Safeguards with CIA Triad and Article 32(2) risk-based language,

		NIST CSF alignment, SOC 2 Type II progress, multi-factor authentication for admin and Subprocessor consoles, encryption key management, quarterly access reviews, expanded annual training topics (FERPA, COPPA, biometric, AI/ML, social engineering), annual penetration testing at production scale, vulnerability disclosure channel, and Privacy by Design statement; expands Section 14 Subprocessors with explicit flow-down to sub-subprocessors, Choice Pursuits liability for Subprocessor acts and omissions as if its own, and disposition of data on Subprocessor replacement; expands Section 15 Transfers to include DPF / UK Extension / Swiss–U.S. DPF and transfer impact assessment cooperation; expands Section 16 with 35-day backup retention cap, no-restoration commitment, and written certification of deletion on request; expands Section 17 to reference state, FERPA, COPPA, and GDPR Article 33/34 breach-notification frameworks; expands Section 18 to add VPAT commitment, annual penetration test executive summary, GDPR Article 28(3)(h) audit provisions with 30-day audit notice, 1-per-12-month cadence, confidentiality, and cost allocation; expands Section 20 with explicit consumer-rights assistance under U.S. state laws, regulator cooperation, and legal-process objection commitment; strengthens Section 21 Insurance with specific coverage types (cyber / tech E&O / CGL); strengthens Section 22 Indemnification with sole-remedy framing for IP claims and full procedural mechanics; strengthens Section 23 with essential-basis-of-bargain and failure-of-essential-purpose language and greater-of cap floor; expands Schedule 1 with security framework, parent/eligible-student data subjects, and SCC Module 2/3 references.