VerbalCheck

Privacy Policy

Choice Pursuits Technologies LLC

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

1. Privacy Summary

This Privacy Policy explains how Choice Pursuits Technologies LLC ("Choice Pursuits," "we," "us," or "our") collects, uses, discloses, stores, protects, and manages information through the VerbalCheck platform. VerbalCheck is an educational technology platform designed to support academic integrity review, assignment workflows, instructor review, interview workflows, AI-assisted learning support, and related instructional processes.

This summary is provided for convenience. The full Sections that follow control in the event of any conflict.

Who This Policy Covers	Institutions, school districts, faculty, administrators, students, parents and eligible students (where applicable), pilot participants, standalone users, authorized reviewers, and website visitors.
Primary Data Categories	Account information, institutional information, course information, student identifiers, assignment content, audio and transcription data, AI-assisted output, usage logs, security logs, cookies or similar technologies, and support communications.
Primary Purposes	Providing VerbalCheck, supporting academic review, processing assignments and interviews, generating transcripts and AI-assisted review support, managing accounts, securing the platform, responding to support requests, and complying with legal or institutional obligations.
Student Data Restrictions	We do not sell student data, do not use student data for behavioral or targeted advertising, do not use student data for unrelated consumer profiling, and do not use customer student data to train Choice Pursuits owned or controlled models. AI Subprocessors are configured for Zero Data Retention where available.
No Sale of Personal Information	Choice Pursuits does not sell personal information of any individual—student, faculty, administrator, or website visitor—for monetary or other valuable consideration.
Voice and Biometric Data	We do not create voiceprints or speaker identification templates and do not generate biometric identifiers within the meaning of BIPA, Texas CUBI, the Washington biometric statute, or analogous state laws.

Human Review	VerbalCheck provides decision-support information for instructors and authorized educational decision makers. VerbalCheck does not make final grading, academic misconduct, disciplinary, or student rights decisions.
Recommended Retention Default	180 days after the end of the applicable course, pilot, or assignment review period, unless the institution, agreement, or law requires a different period. Differentiated retention by data category is described in Section 18.
Security Framework	Administrative, technical, and organizational safeguards aligned with the NIST Cybersecurity Framework. Choice Pursuits is working toward SOC 2 Type II attestation. See Section 17.
Material Change Notice	Choice Pursuits will provide at least 30 days' advance notice of material changes that affect institutional student data, where reasonably practicable.
Privacy Contact	privacy@choicepursuits.com

2. Scope and Institutional Use Notice

This Privacy Policy applies to VerbalCheck users, including institutions, school districts, faculty, administrators, students, parents and eligible students (where applicable), pilot participants, standalone users, authorized reviewers, and website visitors. Additional terms may apply under an institutional agreement, Data Processing Addendum, pilot authorization, purchase order, procurement approval, or other written arrangement.

VerbalCheck may process student education records or other student data when used by a participating institution or authorized faculty member. Institutions, faculty users, and school users should confirm that use of VerbalCheck is permitted by applicable institutional policy before uploading student data, student work, student recordings, audio files, transcripts, or other education records.

FERPA School Official Status. When VerbalCheck processes student education records on behalf of a participating institution, Choice Pursuits is designated as a school official with a legitimate educational interest under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g, subject to the institution's direct control regarding the use and maintenance of education records. Choice Pursuits will use education records only for purposes authorized by the institution, the applicable agreement, this Privacy Policy, the Data Processing Addendum, and applicable law. Choice Pursuits will not redisclose education records except as authorized by the institution, required to provide the Services through approved service providers, required by law, or otherwise permitted under FERPA.

Related Federal Frameworks. Institutions remain responsible for compliance with other federal frameworks that may apply to their use of VerbalCheck, including the Children's Internet Protection Act (CIPA), the Protection of Pupil Rights Amendment (PPRA), the Individuals with Disabilities Education Act

(IDEA), and Section 504 of the Rehabilitation Act. Choice Pursuits will cooperate with reasonable institutional requests to support compliance with these frameworks.

Limitation. This Privacy Policy does not create institutional approval for use of VerbalCheck where institutional approval, procurement review, privacy review, security review, accessibility review, legal review, or parental notice or consent is required.

3. Key Definitions

Defined terms used in this Privacy Policy share meaning with corresponding terms in the Terms of Service and Data Processing Addendum.

- **Account information** means information used to create, manage, authenticate, support, or administer a VerbalCheck account.
- **AI-assisted output** means generated summaries, transcripts, retrieval results, authorship review support, suggested feedback, scoring support, flags, comments, and other outputs created or supported by AI-enabled services.
- **Controller** means the institution, school district, or authorized customer that determines the purpose and means of processing institutional personal data or student education records.
- **De-identified information** means information that cannot reasonably be used to identify, relate to, describe, be associated with, or be linked to a particular individual or household, and that Choice Pursuits maintains and uses in de-identified form, including by committing not to attempt re-identification.
- **Directory information** means categories of student information that an educational institution has, under FERPA, designated as directory information and that may be disclosed without prior written consent unless the parent or eligible student has opted out through the institution.
- **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.
- **Eligible student** means a student who has reached 18 years of age or who attends a postsecondary institution, as defined under FERPA.
- **Personal information or personal data** means information that identifies, relates to, describes, or can reasonably be linked to an individual.
- **Personally identifiable information from education records (PII from Education Records)** means has the meaning given in 34 C.F.R. § 99.3, including direct identifiers, indirect identifiers, and other information that, alone or in combination, would allow a reasonable person to identify a student with reasonable certainty.
- **Processor** means Choice Pursuits Technologies LLC when processing personal data or education records on behalf of an institution, school district, or authorized customer.

- **Sensitive personal information** means categories of personal information that are treated as sensitive under applicable law, as further described in Section 6.
- **Student data** means personal information connected to a student, course, class, assignment, submission, recording, interview, evaluation, academic review, or education record.
- **Services** means the VerbalCheck platform, including standalone access, learning workflow support, assignment workflows, academic integrity support, AI-assisted review, reporting, file storage, audio services, administrative tools, and support services.
- **Subprocessor** means a service provider engaged by Choice Pursuits to process personal data in support of VerbalCheck.

4. Categories of Information Collected by User Type

The categories below describe the information VerbalCheck may collect or process depending on the features used, the role of the user, the institution's configuration, and the content submitted through the platform.

Students	Name, email address, student identifier if provided, role, course enrollment context, class participation, assignment status, submission history, uploaded files, written responses, interview responses, audio recordings if used, transcripts, reflection responses, timestamps, AI-assisted review outputs, instructor feedback, review status, usage logs, device information, and security logs.
Faculty and Instructors	Name, email address, institution, role, course information, class information, assignment settings, rubrics, prompts, instructor questions, review comments, scoring-support activity, class management activity, support communications, login activity, usage logs, device information, and security logs.
Administrators and Institutional Reviewers	Name, email address, institution, role, account permissions, administrative dashboard activity, course or class oversight records, reporting access, procurement communications, privacy review communications, support requests, login activity, usage logs, device information, and security logs.
Standalone or Pilot Users	Name, email address, institution or organization, role, pilot activity, demo course information, uploaded test content, support communications, account settings, usage logs, device information, and security logs.
Parents and Eligible Students (when authorized)	Name, email address, relationship to student, institution, communications submitted to Choice Pursuits regarding access, amendment, or restriction of education records, and verification information needed to respond to a request.

Website Visitors	IP address, browser type, device information, operating system information, pages visited, referring page, approximate location derived from IP address, cookie or similar identifiers where used, form submissions, timestamps, and security logs.

5. Information We Collect

- Account and contact information, such as name, email address, user role, institution, class association, login activity, account settings, authentication details, and account status.
- Institutional and course information, such as instructor name, course name, class section, assignment title, assignment settings, rubrics, prompts, workflow configuration, and administrative settings.
- Student identifiers and academic context, such as student name, student email, student role, enrollment context, course participation, assignment status, submission history, and related academic records.
- Assignment and review content, such as uploaded documents, written responses, interview responses, reflections, instructor questions, feedback, scoring support, authorship review materials, and related coursework data.
- Audio and transcription data where voice-based features are used, such as audio files, interview recordings, speech input, speech output, speech-to-text output, text-to-speech output, transcripts, and related processing details.
- AI-assisted output, such as summaries, retrieval responses, authorship review support, suggested feedback, scoring support, flags, comments, review assistance, and other AI-generated assistance.
- Usage, device, cookie, and security information, such as IP address, browser type, device information, operating system information, timestamps, access logs, upload logs, error logs, security events, session data, and similar technical information.
- Support and communication information, such as messages submitted through support channels, request-access forms, onboarding communications, institutional review communications, procurement communications, privacy questions, and administrative correspondence.

Sources. We collect information directly from users, from the institution acting as Controller, automatically through use of the Services, and from Subprocessors that support the Services. We do not purchase personal information about students from data brokers.

6. Sensitive Personal Information

Some information processed through VerbalCheck may qualify as “sensitive personal information,” “sensitive data,” or similar designation under applicable law (including the California Privacy Rights Act, 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). Categories that may qualify include:

- Account credentials and authentication information.
- Audio recordings, voice data, and transcripts (where treated as sensitive under applicable state law).
- Personal information of known minors, where processed under institutional authorization.
- Information that, if disclosed, would reveal student academic performance, academic integrity proceedings, or disability accommodations—to the extent such information is submitted by an institution or user.

VerbalCheck uses sensitive personal information only to provide the Services, support academic and instructional workflows, maintain security, comply with legal obligations, and perform activities authorized by the institution. We do not use sensitive personal information to infer characteristics about an individual, for behavioral advertising, or for unrelated profiling. California residents have the right to limit our use of sensitive personal information as described in Section 21.

Information Users Should Not Submit. VerbalCheck does not request or require users to submit Social Security numbers, driver license numbers, passport numbers, financial account numbers, payment card numbers, medical records, disability records, unrelated disciplinary records, or unrelated demographic information. Users should not submit such information unless an institution has specifically authorized that submission and determined that it is lawful and appropriate. If sensitive information is submitted in error, the submitting user or institution should promptly notify privacy@choicepursuits.com so that Choice Pursuits may assist with appropriate handling or deletion.

7. How We Use Information

- Provide, operate, maintain, secure, and improve VerbalCheck.
- Support academic integrity review, authorship review, assignment workflows, interview workflows, reporting, instructor review, and related instructional processes.
- Provide AI-assisted help, retrieval, transcription, text-to-speech, speech-to-text, scoring support, and review support.
- Manage accounts, authentication, user roles, class setup, assignment setup, permissions, administrative tools, and institutional configurations.
- Respond to support requests, troubleshoot errors, communicate service information, provide onboarding support, and assist with institutional review requests.
- Maintain security, detect misuse, investigate incidents, prevent unauthorized access, enforce acceptable use requirements, and protect the platform.

- Create internal application analytics based on VerbalCheck data, such as class-level usage, assignment activity, workflow activity, feature usage, system performance, and administrative trends.
- Comply with legal obligations, institutional requirements, procurement review, privacy review, security review, accessibility review, audit requests, and lawful instructions from authorized institutional representatives.
- Generate de-identified and aggregated information for the limited internal purposes of operating, securing, evaluating, and improving the Services and for reporting aggregate platform statistics. Choice Pursuits will not attempt to re-identify de-identified information, will require any recipient to commit to the same, and will not use de-identified or aggregated information to train Choice Pursuits owned or controlled models trained on customer student data.

8. Legal Bases for Processing

For individuals in the European Economic Area, the United Kingdom, Switzerland, and other jurisdictions where a legal basis for processing must be identified, our legal bases include:

- Performance of a contract with the institution or user, or to take steps at the request of the institution or user prior to entering into a contract.
- Compliance with a legal obligation to which Choice Pursuits is subject.
- Legitimate interests pursued by Choice Pursuits or by the institution, including operating, securing, supporting, and improving the Services, where those interests are not overridden by the rights and freedoms of the data subject.
- Consent of the data subject, where required by applicable law and obtained through the institution or directly from the user.
- Performance of a task carried out in the public interest or in the exercise of official authority, where applicable to a public educational institution acting as Controller.

Where processing is based on consent, the data subject may withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal.

9. What We Do Not Do with Student Data

Consistent with the principles of state student data privacy laws (including the Student Online Personal Information Protection Act-style statutes in California, Illinois, Colorado, Connecticut, and other states):

- We do not sell student data.
- We do not share student data for cross-context behavioral advertising.
- We do not use student data for behavioral advertising or targeted advertising.

- We do not use student data for unrelated consumer profiling, including profiling that produces legal or similarly significant effects.
- We do not intentionally disclose student data to unauthorized parties.
- We do not use customer student data to train, fine-tune, or otherwise improve Choice Pursuits owned or controlled models.
- We do not authorize our AI Subprocessors to use customer student data to train their models. AI Subprocessors are configured for Zero Data Retention where available.
- We do not use student education records for direct marketing to students.
- We do not knowingly amass profiles of students except in furtherance of authorized educational purposes.
- We do not make final grading, academic misconduct, disciplinary, or student rights decisions. VerbalCheck provides decision support information for human review.

10. AI Processing and Human Review

VerbalCheck currently uses OpenAI as the active AI service provider for AI help, retrieval, speech-to-text, text-to-speech, audio services, and related AI-assisted functionality. Choice Pursuits has enabled OpenAI's Zero Data Retention configuration for the API endpoints used by VerbalCheck. Under Zero Data Retention, OpenAI does not retain prompt or completion content after the request is processed and does not use customer content to train OpenAI models. The specific AI models in use are identified in the Subprocessor Register.

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. Changes to the AI Subprocessor or to the configuration that affect institutional student data will be reflected in the Subprocessor Register and treated as a material change under Section 29 where applicable.

Nature of AI-Assisted Output. AI-assisted output may include summaries, transcripts, feedback support, authorship review support, scoring support, flags, comments, and other instructional assistance.

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, 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.

Human Review Requirement. AI-assisted output should be reviewed by an instructor or authorized institutional decision maker. VerbalCheck is not intended to be the sole basis for grading, academic misconduct findings, discipline, denial of student rights, or other decisions affecting a student.

Institutions and faculty remain responsible for applying their own policies and procedures, including notice and appeal procedures owed to students.

11. Voice, Audio, and Biometric Information

VerbalCheck may collect or 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 for the purpose of identifying or authenticating any individual. VerbalCheck does not generate "biometric identifiers" or "biometric information" 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.), the Colorado Privacy Act biometric provisions, 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, we will (a) update this 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 and transcripts may still be considered sensitive personal information, education records, or biometric-related information under certain state laws 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. Cookies and Similar Technologies

VerbalCheck may use cookies, local storage, session storage, pixels, logs, or similar technologies to operate the platform, maintain secure sessions, remember user settings, support authentication, protect against misuse, improve performance, and understand platform usage.

Essential Cookies and Storage	Used for authentication, session management, account access, security, load balancing, and core platform functions. These are needed for VerbalCheck to work properly.
Preference Technologies	Used to remember user settings, display preferences, workflow settings, and similar choices where configured.
Security and Fraud Prevention Technologies	Used to detect misuse, protect accounts, investigate errors, monitor security events, and help prevent unauthorized access.
Analytics Technologies	Used for internal application analytics, usage trends, performance, troubleshooting, and service improvement. VerbalCheck does not currently use an external advertising analytics provider.
Marketing Cookies	VerbalCheck does not currently use student data for behavioral advertising or cross-context advertising. If optional marketing or advertising cookies are later used, Choice Pursuits will update this Privacy Policy, provide additional notice, and offer consent or opt-out options where required by applicable law.

Browser Controls and Global Privacy Signals. Users may adjust browser settings to block or delete cookies. Some VerbalCheck features may not function properly if essential cookies or required browser storage are disabled. Where required by applicable law (for example, the California Privacy Rights Act), Choice Pursuits will treat a recognized opt-out preference signal (such as the Global Privacy Control) received from a website visitor as a valid request to opt out of the sale or sharing of personal information through the channel that received the signal.

13. Analytics

VerbalCheck may use internal application analytics to understand platform activity, assignment activity, class-level usage, feature usage, system performance, error patterns, and administrative trends. These analytics are used to operate, secure, support, and improve the platform.

VerbalCheck does not use student data for behavioral advertising, unrelated consumer profiling, or the sale of personal information. VerbalCheck does not currently use an external advertising analytics provider. If Choice Pursuits later adds an external analytics provider, the provider will be added to the Subprocessor Register at https://verbalcheck.com/subprocessors and additional notice will be provided as required by law or institutional agreement.

14. Service and Marketing Communications

Service Communications. Choice Pursuits may send service-related communications, including account notices, security notices, support messages, product updates, onboarding information, policy updates, institutional review communications, and operational messages. These communications are part of providing and supporting VerbalCheck.

Marketing Communications. Choice Pursuits may send marketing communications to institutional contacts, faculty, administrators, pilot participants, or prospective customers where permitted by law, including in compliance with the CAN-SPAM Act (15 U.S.C. § 7701 et seq.) and applicable state and international anti-spam laws. Marketing emails will include a working unsubscribe mechanism and a valid postal address. Recipients may opt out of marketing communications by using the unsubscribe link in the message or by contacting privacy@choicepursuits.com. Opt-out requests will be honored within 10 business days.

No Marketing to Students. Choice Pursuits will not use student education records or student data for targeted marketing, behavioral advertising, or unrelated promotional campaigns. Choice Pursuits will not market directly to students using student education records collected through institutional use of VerbalCheck.

15. Subprocessors and Service Providers

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

Advance Notice and Objection. Choice Pursuits will provide participating institutions with at least 30 days' advance notice before adding or replacing a Subprocessor that will process institutional student data, except where a Subprocessor must be engaged on an emergency basis to maintain security or continuity of the Services (in which case Choice Pursuits will provide notice as promptly as reasonably practicable). Institutions may object to a new Subprocessor on reasonable data-protection grounds through the procedure described in the Data Processing Addendum. Institutions may subscribe to Subprocessor change notifications by contacting privacy@choicepursuits.com.

Flow-Down Obligations. Choice Pursuits will require each Subprocessor that processes personal data on its behalf to be bound by written commitments that are no less protective than those in this Privacy Policy and the Data Processing Addendum, including obligations of confidentiality, security, limitation of use, and breach notification.

No active external advertising analytics provider is wired into the current platform. Analytics functionality is based primarily on internal application data and database-backed routes.

16. Data Sharing

Choice Pursuits may share information in the following limited circumstances:

- With institutions, faculty, administrators, school officials, or authorized users as needed to provide VerbalCheck.

- With Subprocessors and service providers who help host, store, process, secure, deliver, or support the platform, as identified in the Subprocessor Register.
- With legal, security, compliance, insurance, or professional advisers when necessary to protect rights, safety, security, privacy, or legal interests.
- When required by law, subpoena, court order, public authority, regulator, or other legal process, in the manner described in Section 27.
- With consent, institutional authorization, or user direction, where applicable.
- In connection with a business transaction, such as a merger, acquisition, financing, restructuring, or sale of assets, subject to appropriate confidentiality, legal, and student data protections. In any such transaction involving institutional student data, Choice Pursuits will require the successor entity to assume the obligations set forth in this Privacy Policy and any applicable Data Processing Addendum, or to obtain new authorization from the institution.

Choice Pursuits will not intentionally redisclose student education records except as necessary to provide the Services, as directed by the institution, as required by law, or as otherwise authorized in writing by the institution.

17. Security

Choice Pursuits uses administrative, technical, and organizational safeguards designed to protect information processed through VerbalCheck against unauthorized access, loss, misuse, alteration, disclosure, or destruction. Our security program is aligned with the NIST Cybersecurity Framework, and Choice Pursuits is working toward SOC 2 Type II attestation. Safeguards are reviewed periodically and adjusted as the platform, risk profile, and institutional requirements evolve.

- Encryption in transit using Transport Layer Security version 1.2 or higher.
- Encryption at rest using AES-256 (or substantially equivalent algorithms supported by hosting, database, and storage Subprocessors).
- Role-based access controls and least-privilege access for administrative functions.
- Multi-factor authentication for administrative and 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.
- Annual privacy and security awareness training for personnel with access to personal data.
- Audit logging, security logging, and monitoring appropriate to the operational stage of the platform.

- Secure development practices, code review where practical, dependency and vulnerability scanning, environment variable protection, and separation of staging and production credentials.
- Backup, recovery, and deletion practices consistent with platform capabilities and agreed institutional requirements.
- Incident response procedures designed to support investigation, mitigation, documentation, institutional cooperation, and required notifications.
- A vulnerability disclosure channel at security@choicepursuits.com for good-faith researchers to report suspected security issues.

No online service can guarantee perfect security. Users are responsible for protecting account credentials, using authorized devices and networks, and reporting suspected unauthorized access to security@choicepursuits.com.

18. Data Retention, Return, and Deletion

Choice Pursuits retains information only as long as reasonably necessary to provide VerbalCheck, support academic review, meet institutional requirements, maintain security, resolve disputes, enforce terms, and comply with legal obligations. Institutions may request deletion or return of student data according to their applicable agreement or policy.

The following table describes the recommended default retention periods by data category. Institutions may direct shorter or longer periods through the applicable agreement, Data Processing Addendum, or written instructions, subject to applicable law.

Data Category	Recommended Default Retention
Account information (faculty, administrators, students)	Duration of the active account, plus up to 12 months after account closure for support and dispute resolution, unless the institution directs earlier deletion.
Assignment submissions, written responses, AI-assisted review materials	180 days after the end of the applicable course, pilot, or assignment review period.
Audio recordings and interview recordings	Up to 90 days after transcription and review, unless the institution directs a different period or law requires otherwise.
Transcripts derived from audio	180 days after the end of the applicable course, pilot, or assignment review period.
System metadata, access logs, and security logs	Generally 90 to 365 days, depending on the log type and security needs.

Support communications and administrative correspondence	Up to 24 months after the communication, unless a longer period is required for legal or institutional purposes.
Backup copies	Retained for a limited period according to provider backup cycles before scheduled deletion, generally not exceeding 35 days after deletion from production systems.

Termination and Return. Upon termination or written request from an authorized institutional representative, Choice Pursuits will return or delete personal data according to the institution's instructions, subject to legal obligations, security requirements, backup limitations, and reasonable technical constraints. The Data Processing Addendum describes a Termination Assistance Period of 60 days during which Institutional Data may be exported in a documented machine-readable format.

Backups. When data is deleted from production systems, residual copies may persist in encrypted backups until those backups expire in the ordinary course. 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.

19. Student, User, and Institutional Privacy Rights

Depending on applicable law, institutional policy, and the nature of the data, individuals may have rights to request access, correction, deletion, restriction, objection, portability, information about how personal data is used and disclosed, opt out of certain processing, limit certain uses of sensitive personal information, opt out of profiling that produces legal or similarly significant effects, and nondiscrimination for exercising privacy rights required by law.

How to Submit a Request. Requests may be submitted by contacting privacy@choicepursuits.com. The request should include the requester's name, email address, institution, role, the nature of the request, and enough information for Choice Pursuits to reasonably verify the request.

Verification. Choice Pursuits may require identity verification before responding to a request. Verification may include confirming control of an email account, confirming institutional affiliation, requesting additional information, or coordinating with the institution. Authorized agents may be required to provide proof of authority and verification of the individual's identity where permitted by law.

Response Time. Choice Pursuits will acknowledge verified requests within 10 business days and will aim to respond substantively within 45 days, unless a different period is required by applicable law, institutional agreement, or the institution's written instructions. Additional time (up to an additional 45 days, where permitted by law) may be needed when requests are complex, require institutional coordination, or involve archived or backup data, and we will notify the requester of any extension.

Appeals. Where required by state law (for example, in Virginia, Colorado, Connecticut, and certain other states), individuals may appeal a denial of their request by contacting privacy@choicepursuits.com with the subject line “Privacy Rights Appeal” within a reasonable time after receiving our denial. Choice Pursuits will respond to the appeal within 45 days and will inform the requester of the right to contact the applicable state attorney general if the appeal is denied.

Education Records. If a request concerns education records or student data controlled by an institution, Choice Pursuits may refer the request to the institution or respond according to the institution’s written instructions. The institution remains responsible for determining whether a student, parent, guardian, or eligible student has rights to access, amend, delete, restrict, or challenge the education record under FERPA, state student privacy laws, institutional policy, or other applicable law.

Limits. Choice Pursuits may deny, limit, or delay a request where permitted by law, including when the request cannot be verified, conflicts with institutional instructions, affects another person’s rights, interferes with security or fraud prevention, concerns data retained for legal obligations, or involves data that cannot reasonably be separated from institutional records.

Non-Retaliation. Choice Pursuits will not discriminate or retaliate against individuals for exercising privacy rights required by applicable law.

Right to Lodge a Complaint. Individuals in the European Economic Area, the United Kingdom, or Switzerland have the right to lodge a complaint with their supervisory authority. United States residents may have the right to contact their state attorney general or applicable regulator.

20. Parents and Eligible Students Under FERPA

FERPA generally provides parents and eligible students (students who have reached 18 years of age or who attend a postsecondary institution) with rights to inspect and review education records, request amendment of education records they believe to be inaccurate, and have some control over the disclosure of personally identifiable information from education records.

Choice Pursuits processes education records as a school official acting on behalf of participating institutions. Parents and eligible students should direct requests to inspect, amend, or restrict disclosure of education records to the institution that maintains those records. If Choice Pursuits receives a request directly from a parent or eligible student, we will refer the request to the appropriate institution and respond according to the institution’s direction and applicable law.

Directory Information. Whether and how directory information may be designated and disclosed is determined by the institution. Choice Pursuits will treat student information as non-directory unless the institution provides written instructions to the contrary.

21. California Privacy Rights

This Section supplements the rest of this Privacy Policy and applies to California residents whose personal information is processed by Choice Pursuits.

21.1 Categories of Personal Information Collected

Within the prior twelve months, Choice Pursuits has collected the categories of personal information described in Sections 4 and 5 of this Privacy Policy, including identifiers, internet or other electronic network activity information, audio information, professional or education information, and inferences drawn from these categories where applicable. Sources include the institution, faculty users, students, website visitors, and Subprocessors that support the Services.

21.2 No Sale or Sharing of Personal Information

We do not sell personal information for monetary or other valuable consideration, and we do not share personal information for cross-context behavioral advertising. We do not have actual knowledge that we sell or share the personal information of consumers under 16 years of age.

21.3 Right to Limit Use of Sensitive Personal Information

California residents may request to limit our use and disclosure of sensitive personal information to those uses permitted under California law (such as providing the requested service, ensuring security and integrity, and similar permitted purposes). To submit a request, contact privacy@choicepursuits.com with the subject line “Limit Sensitive PI – California.”

21.4 Right to Know, Delete, Correct, and Portability

California residents may request to know what personal information we have collected, used, disclosed, and (if applicable) sold or shared about them; request deletion of personal information; request correction of inaccurate personal information; and request a portable copy of personal information. Requests may be submitted as described in Section 19. We will not discriminate against you for exercising these rights.

21.5 Authorized Agents

California residents may use an authorized agent to submit requests. Authorized agents must provide signed written permission from the individual and may be required to verify their own identity. We may deny requests submitted by authorized agents that lack required documentation.

21.6 Financial Incentives and Shine the Light

Choice Pursuits does not offer financial incentives for the collection, sale, or deletion of personal information. Choice Pursuits does not share personal information with third parties for those parties’ own direct marketing purposes within the meaning of California Civil Code § 1798.83 (“Shine the Light”).

21.7 California Notice of Collection

This Privacy Policy serves as our “Notice at Collection” under California law. We will not collect additional categories of personal information or use personal information for additional purposes that are materially different from those described here without providing notice to the individual.

22. State Student Privacy Laws and Regional Privacy Requirements

VerbalCheck may be used by educational institutions in multiple states. State student privacy laws (including New York Education Law § 2-d, the California Student Online Personal Information Protection Act, the Illinois Student Online Personal Protection Act, Connecticut Public Act 16-189, the Colorado Student Data Transparency Act, Texas Education Code § 32.151 (Student Online Personal Information Protection), and similar statutes) may impose additional requirements related to student data, vendor contracts, advertising restrictions, data security, breach notification, parent or student rights, data deletion, school district approval, data residency, and data governance. Where applicable, Choice Pursuits will work with the institution to address state-specific student privacy requirements through the Data Processing Addendum, institutional agreement, purchase order terms, pilot authorization, or other written arrangement.

New York Education Law § 2-d. For New York public school district customers, Choice Pursuits will, on request, execute an addendum that includes the Parents Bill of Rights for Data Privacy and Security and the supplemental information required under 8 NYCRR Part 121. Choice Pursuits will not sell student personally identifiable information, will not use student personally identifiable information for marketing or commercial purposes, and will maintain reasonable administrative, technical, and physical safeguards aligned with the NIST Cybersecurity Framework.

Certain state comprehensive privacy laws (including the California Consumer Privacy Act and California Privacy Rights Act, 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) may also provide individual rights related to access, deletion, correction, opt out, sensitive personal information, profiling, or targeted advertising. Choice Pursuits will respond to applicable requests in accordance with the law, institutional direction, and the nature of the data involved.

23. Children and COPPA Scope

VerbalCheck is not directed to children under age 13 for general consumer use. VerbalCheck is intended for use by educational institutions, faculty, administrators, and students under institutional authorization.

If VerbalCheck is used in an elementary school, middle school, high school, homeschool program, youth program, or other setting involving students under age 13, the school, school district, or authorized institutional representative is responsible for determining whether it has authority to provide any

required consent on behalf of parents or guardians under the school-authorized exception to the Children's Online Privacy Protection Act (COPPA), whether additional parental notice or consent is required, and whether the use complies with COPPA, FERPA, state student privacy laws, and institutional policy.

Choice Pursuits may require a written institutional agreement, Data Processing Addendum, parental notice process, school authorization, or other written terms before supporting use involving students under age 13.

We do not knowingly collect personal information from children under age 13 outside of school-authorized contexts. If we learn that personal information from a child under age 13 has been submitted without appropriate institutional authorization or required consent, we may delete the information, restrict access, suspend the account, or refer the matter to the applicable institution. Parents or guardians who believe their child's personal information has been submitted without appropriate authorization should contact privacy@choicepursuits.com.

Choice Pursuits will not use personal information collected from students under age 13 for behavioral advertising, unrelated marketing, unrelated profiling, or any commercial purpose inconsistent with the educational use authorized by the school or institution.

24. International Users

VerbalCheck is operated from the United States. Personal data processed through VerbalCheck is stored or processed within the United States using approved Subprocessors identified in the Subprocessor Register. If information is processed for individuals outside the United States, additional privacy requirements may apply.

For institutions or data subjects in the European Economic Area, the United Kingdom, or Switzerland, Choice Pursuits will, on reasonable written request, execute the European Commission Standard Contractual Clauses and the United Kingdom International Data Transfer Addendum (or successor mechanisms) to support lawful cross-border transfers, as further described in the Data Processing Addendum. Choice Pursuits will conduct transfer impact assessments when required and will implement supplementary measures where appropriate.

Where applicable, processing may be based on performance of a contract, legitimate educational interests, institutional direction, legal obligations, consent where required, or another lawful basis recognized by applicable law. Institutions that require additional regional or international privacy terms (including under Quebec Law 25, Brazil LGPD, or other foreign privacy laws) should address those requirements through a written institutional agreement or Data Processing Addendum.

25. De-Identified and Aggregated Information

Choice Pursuits may create de-identified or aggregated information from personal data processed through VerbalCheck for the internal purposes of operating, securing, supporting, evaluating, and improving the Services and for limited aggregate reporting. When Choice Pursuits creates or uses de-identified information, Choice Pursuits will:

- Take reasonable measures to ensure that the information cannot be associated with a specific individual, household, device, or institution.
- Publicly commit to maintaining and using the information in de-identified form and not to attempt to re-identify the information, except as permitted by law to test re-identification risk.
- Contractually obligate any recipient of de-identified information to comply with these restrictions.
- Not use de-identified or aggregated information derived from customer student data to train Choice Pursuits owned or controlled models.

26. Notification of Security Incidents

If Choice Pursuits confirms a security incident that affects personal information processed through VerbalCheck, we will notify the institution acting as Controller without undue delay and, where feasible, within 72 hours of confirmation, as further described in the Data Processing Addendum.

Content of Notice. To the extent known at the time of notice, our notice will describe: (a) the nature of the incident, (b) the categories and approximate volume of personal information affected, (c) the categories and approximate number of individuals affected, (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. Choice Pursuits will provide updates as additional information becomes available.

Where required by applicable law, Choice Pursuits will also provide notice directly to affected individuals or to the appropriate regulator, in coordination with the institution and within the timelines required by applicable state, federal, or international breach notification laws. Notice may be delayed where law enforcement or applicable law requires delay.

27. Legal Requests and Institutional Notification

Choice Pursuits may disclose information when required by law, subpoena, court order, regulator, public authority, or other legal process. When legally permitted and reasonably practical, Choice Pursuits will notify the applicable institution before disclosing student education records or institutional data in response to legal process, so the institution may seek appropriate protection or provide direction. Choice Pursuits will provide only the information reasonably required to respond to the legal request and will object to overbroad requests where appropriate.

Choice Pursuits may also disclose information when necessary to protect rights, safety, security, privacy, or legal interests, including to investigate misuse, respond to security incidents, enforce terms, or prevent harm.

28. Accessibility and Privacy Support

Choice Pursuits is committed to reviewing accessibility and privacy concerns submitted by users or institutions.

- Privacy concerns: privacy@choicepursuits.com.
- Accessibility concerns: accessibility@choicepursuits.com.
- Security concerns: security@choicepursuits.com.

Accessibility-related communications may be processed as support communications and may include user contact information, technical information, and information needed to evaluate or resolve the request.

29. Changes to This Privacy Policy

Choice Pursuits may update this Privacy Policy as VerbalCheck changes, laws evolve, service providers change, or institutional requirements require clarification. Choice Pursuits will update the version number and effective date when material changes are made.

Notice of Material Changes. For changes that materially expand the categories of personal information collected, the purposes of use, the categories of recipients, or the retention periods, Choice Pursuits will provide at least 30 days' advance notice before the change takes effect, where reasonably practicable, by posting a notice, sending an email, providing notice through the platform, or notifying participating institutions through the applicable institutional process. Material changes are summarized in the Revision History.

If a material change affects institutional student data under an executed agreement, the terms of the applicable institutional agreement or Data Processing Addendum will control where required.

30. Contact

Company	Choice Pursuits Technologies LLC
Product	VerbalCheck
Privacy	privacy@choicepursuits.com
Security	security@choicepursuits.com
Accessibility	accessibility@choicepursuits.com

Subprocessor Register	https://verbalcheck.com/subprocessors
Governing Law	State of Oklahoma, United States, unless another governing law is required by an executed institutional agreement.

Revision History

Version	Effective Date	Summary of Changes
1.0	May 8, 2026	Initial published version. Consolidates the prior public Privacy Policy (revision dated May 7, 2026); harmonizes definitions with the Terms of Service and Data Processing Addendum; documents OpenAI Zero Data Retention configuration; strengthens biometric / voiceprint statement with citations to BIPA, Texas CUBI, and Washington biometric statutes; tightens encryption commitments to TLS 1.2+ and AES-256; adds dedicated Sensitive Personal Information section; adds GDPR Article 13/14 legal-basis section; adds dedicated California Privacy Rights section; adds Parents and Eligible Students FERPA section; strengthens COPPA disclosure with parent-contact route; adds direct user breach-notification commitment; adds differentiated retention table by data category; references the centralized Subprocessor Register; adds dedicated accessibility and security contact addresses.
1.1	May 16, 2026	Legal review revisions: adds Last Updated date; expands definitions to include Eligible Student, Directory Information, De-identified Information, and PII from Education Records; adds CIPA/PPRA/IDEA/Section 504 acknowledgments; broadens no-sale commitment to cover all personal information; adds SOPIPA-aligned commitments; adds annual AI Subprocessor review commitment; specifies 30-day Subprocessor advance-notice and objection right; adds flow-down obligation language; adds vulnerability disclosure channel; adds NIST Cybersecurity Framework alignment and SOC 2 Type II progress disclosure; adds multi-factor authentication commitment; clarifies backup retention (35-day cap) and post-deletion behavior; adds appeal procedure for state privacy rights denials; adds 10-business-day acknowledgment commitment; adds Global Privacy Control recognition; adds CAN-SPAM compliance reference and 10-business-day opt-out commitment; adds successor-entity assumption requirement for business transactions; adds New York Education Law § 2-d Parents Bill of Rights commitment; references Texas Education Code § 32.151 and the 2023–2024 state comprehensive privacy laws (Oregon, Texas, Tennessee, Montana); adds dedicated De-Identified and Aggregated Information section; expands security-incident notice content per GDPR Article 33-style requirements; adds 30-day advance-notice

		commitment for material policy changes; adds Quebec Law 25 / Brazil LGPD acknowledgment.