

EDUCATION SERVICES AND STUDENT DATA PRIVACY ADDENDUM

Effective Date: July 25th, 2026

This Education Services and Student Data Privacy Addendum (“Education Addendum”) is entered into between NaturalSoft Ltd., a company incorporated in British Columbia, Canada (“NaturalSoft”), and the educational agency, school district, school, college, university, library, education consortium, or other educational institution identified in the applicable Order (“Institution”).

This Education Addendum supplements and forms part of the Master Subscription Agreement, Data Processing Addendum, Order, or other written agreement governing the Institution’s use of NaturalReader EDU or other NaturalReader education services (collectively, the “Agreement”).

NaturalSoft and Institution may each be referred to as a “Party” and together as the “Parties.”

1. Purpose and Scope

This Education Addendum governs NaturalSoft’s processing of Student Data in connection with NaturalReader products and services purchased, authorized, or administered by Institution.

The Services may include:

- text-to-speech;
- document reading;
- OCR and document parsing;
- document libraries;
- generated audio;
- AI-assisted reading and document features;
- translation;
- summaries;
- quizzes;
- questions and answers;
- podcast-style content;
- voice generation;
- authorized voice cloning;
- accessibility and reading-support features;
- administrator controls;
- mobile applications;

- the NaturalReader Chrome extension; and
- related support and account-management functions.

This Education Addendum applies only to Institution-managed accounts and Services. It does not govern an individual's separate direct-to-consumer subscription that is not controlled by Institution.

2. Relationship to Other Agreements

This Education Addendum is incorporated into the Agreement.

If there is a conflict concerning Student Data, the following order of precedence applies:

1. an applicable state-specific rider signed by both Parties;
2. this Education Addendum;
3. the Data Processing Addendum;
4. the applicable Order;
5. the Master Subscription Agreement; and
6. other incorporated policies.

A purchase order or Institution procurement document does not modify the Agreement unless NaturalSoft expressly accepts the modification in writing.

3. Definitions

3.1 Applicable Student Privacy Laws

"Applicable Student Privacy Laws" means laws applicable to the Institution's use of the Services and NaturalSoft's processing of Student Data, which may include:

- the Family Educational Rights and Privacy Act and its regulations ("FERPA");
- the Children's Online Privacy Protection Act and its regulations ("COPPA");
- applicable state student privacy statutes;
- applicable state data breach laws;
- applicable state education records laws; and
- other privacy laws expressly identified in a signed state rider or Order.

Applicable Student Privacy Laws do not include a law merely because Institution is subject to it. The law must also apply to NaturalSoft's processing or obligations under the Agreement.

3.2 Authorized User

"Authorized User" means a student, educator, employee, contractor, administrator, parent, guardian, or other person whom Institution authorizes to access the Services.

3.3 Customer Content

“Customer Content” means information submitted to, stored in, processed by, or generated through the Services by Institution or its Authorized Users.

Customer Content may include:

- typed or pasted text;
- prompts;
- uploaded documents;
- PDFs;
- images;
- OCR-extracted text;
- webpages;
- voice input;
- voice recordings;
- reference audio;
- voice samples;
- text submitted for speech generation;
- generated audio;
- downloadable audio;
- AI-generated content;
- annotations;
- project information;
- error records; and
- associated operational information.

3.4 Education Records

“Education Records” has the meaning given under FERPA where FERPA applies.

3.5 Eligible Student

“Eligible Student” means a student to whom rights have transferred under FERPA or applicable law, including an eligible postsecondary student.

3.6 Parent

“Parent” includes a parent, legal guardian, or other person who has legal authority concerning the student under applicable law.

3.7 Student Data

“Student Data” means personal information relating to an identifiable student that NaturalSoft processes on behalf of Institution through the Services.

Student Data may include personally identifiable information from Education Records.

Student Data does not include information that has been aggregated or de-identified so that it cannot reasonably be associated with an identifiable student, household, school account, or small group of students.

3.8 Subprocessor

“Subprocessor” means a service provider engaged by NaturalSoft to process Student Data on NaturalSoft’s behalf in connection with the Services.

4. Ownership and Control

As between NaturalSoft and Institution:

- Institution and its Authorized Users retain their rights in Customer Content;
- Institution retains control over Student Data submitted through Institution-managed accounts;
- NaturalSoft obtains no ownership interest in Student Data; and
- NaturalSoft may process Student Data only as permitted by the Agreement.

NaturalSoft will treat Institution’s documented use, account configuration, administrator settings, support instructions, and written requests as instructions concerning Student Data.

Institution may instruct NaturalSoft to:

- delete supported Student Data;
- disable Institution-managed user accounts;
- disable AI functions;
- disable voice-cloning functions; and
- terminate the Institution account.

NaturalSoft is not required to follow an instruction that violates law, compromises system security, discloses another customer’s information, or is technically impossible. The Parties will work in good faith to identify a lawful alternative.

5. FERPA

Where FERPA applies and Institution discloses personally identifiable information from Education Records to NaturalSoft under the school-official exception, the Parties intend that NaturalSoft act as a contractor performing an institutional service or function for which Institution would otherwise use employees.

NaturalSoft agrees that it will:

1. process the Education Records only to provide, secure, maintain, and support the contracted Services;

2. remain under Institution's direct control regarding the use and maintenance of Education Records as established through the Agreement and Institution's documented instructions;
3. use Education Records only for the purposes for which Institution disclosed them;
4. limit internal access to personnel who require access to perform their responsibilities;
5. not redisclose personally identifiable information from Education Records except:
 - to authorized Subprocessors performing the contracted Services;
 - on Institution's behalf and consistent with FERPA;
 - with valid consent;
 - as required by law; or
 - as otherwise expressly permitted by FERPA and the Agreement;
6. require authorized Subprocessors to protect the information and use it only for contracted purposes;
7. assist Institution with reasonable requests concerning access, correction, or deletion; and
8. delete or return Student Data as described in this Education Addendum.

Institution is responsible for:

- determining that NaturalSoft satisfies Institution's school-official criteria;
- identifying NaturalSoft as a school official where required by Institution's annual FERPA notice;
- determining that NaturalSoft has a legitimate educational interest;
- using reasonable methods to restrict access to Education Records;
- authorizing only appropriate users;
- providing notices required under FERPA; and
- determining whether a FERPA exception or consent permits disclosure.

Nothing in the Agreement requires Institution to disclose more Student Data than is necessary to use the Services.

6. COPPA and Users Under 13

Where COPPA applies and Institution authorizes students under 13 to use the Services, Institution represents that:

- the Services are being used for the benefit of Institution and its students;
- the processing is within the educational context;

- Institution has authority to provide consent on behalf of Parents or has obtained required parental consent;
- Institution has reviewed NaturalSoft's collection, use, retention, and disclosure practices;
- Institution will provide required notices to Parents; and
- Institution will not direct NaturalSoft to process children's personal information for an unrelated commercial purpose.

NaturalSoft will process information collected under Institution's school authorization only to:

- provide the Institution-authorized Services;
- maintain and secure the Services;
- provide support;
- prevent fraud and abuse;
- comply with law; and
- perform other functions expressly authorized by Institution and permitted by COPPA.

NaturalSoft will not use information collected from children under Institution's authorization for:

- targeted advertising;
- behavioral advertising;
- marketing to students;
- marketing to Parents;
- creating commercial student profiles;
- selling information; or
- an unrelated commercial purpose.

NaturalSoft will make its relevant data practices available to Institution so Institution may provide appropriate notices.

7. Data Minimization

NaturalSoft requires only an email address for standard EDU account creation and authentication.

NaturalSoft does not require Institution or Authorized Users to provide the following as standard account-profile fields:

- telephone number;
- mailing address;
- date of birth;
- student identification number;

- grade level;
- demographic information;
- attendance records;
- discipline records;
- medical information;
- disability information;
- IEP or 504 information; or
- government identification numbers.

Institution or an Authorized User may nevertheless include such information in an uploaded document, image, prompt, voice recording, or other Customer Content.

Institution is responsible for limiting Customer Content to information reasonably necessary for the intended educational purpose.

NaturalSoft will not require an Authorized User to disclose more information than is reasonably necessary to use an applicable feature.

8. Permitted Uses of Student Data

NaturalSoft may process Student Data only to:

- authenticate users;
- provide text-to-speech;
- read and process documents;
- perform OCR and document parsing;
- provide requested AI features;
- generate audio;
- store user Library content;
- synchronize authorized content across supported devices;
- provide accessibility and reading tools;
- provide administrator functions;
- maintain account settings;
- provide support requested by Institution or an Authorized User;
- monitor availability and performance;
- diagnose errors;
- prevent security threats, fraud, and abuse;
- comply with legal obligations; and
- enforce the Agreement.

NaturalSoft may create and use aggregated or de-identified information to:

- understand general feature usage;
- measure service performance;

- improve reliability;
- allocate infrastructure;
- identify general product priorities; and
- produce non-identifying statistics.

NaturalSoft will not attempt to reidentify de-identified Student Data.

9. Prohibited Uses

NaturalSoft will not:

- sell Student Data;
- rent Student Data;
- exchange Student Data for monetary consideration;
- disclose Student Data to data brokers;
- disclose Customer Content to marketers;
- use Student Data for targeted advertising;
- use Student Data for cross-context behavioral advertising;
- use Student Data to advertise to students or Parents;
- create a commercial profile about a student;
- use Student Data to determine creditworthiness;
- use Student Data for employment screening;
- use Student Data for insurance eligibility;
- use Student Data for an unrelated commercial purpose;
- use Student Data to train, fine-tune, or improve a general-purpose AI or large language model;
- use voice samples or cloned voices to train a general voice model;
- claim ownership of Student Data;
- make admissions, grading, discipline, disability, financial aid, or eligibility decisions on behalf of Institution; or
- disclose Student Data except as permitted by the Agreement or law.

NaturalSoft may communicate with adult Institution administrators about:

- account administration;
- security;
- support;
- billing;
- renewals;
- service changes; and
- other contracted NaturalReader services.

NaturalSoft will not use Student Data to market directly to students or Parents.

10. AI-Assisted Features

NaturalSoft may provide AI-assisted features using paid business or API services.

The EDU AI assistant currently may use paid Google Gemini API services. Selected speech or AI functions may use other providers listed in the applicable Subprocessor schedule.

NaturalSoft will not use prompts, uploaded documents, OCR content, AI-generated output, or related Student Data to train, fine-tune, or improve NaturalSoft or third-party general-purpose AI models.

AI output may:

- contain inaccuracies;
- omit important information;
- misunderstand a document;
- contain inappropriate material;
- vary between requests;
- provide incomplete citations;
- reflect limitations or biases; or
- be unsuitable for a specific student or educational purpose.

Institution and Authorized Users are responsible for reviewing AI output before relying on it.

NaturalSoft does not intend AI output to make consequential educational decisions without human review.

10.1 Administrator Control

Institution administrators may disable available AI-assisted features for Institution-managed users.

Where Institution disables an AI feature, NaturalSoft will not make that feature available to Institution-managed users while the setting remains disabled, subject to reasonable processing time and technical limitations.

10.2 Provider-Specific Retention

Some AI providers may retain limited prompts, context, or output for security and abuse monitoring.

Where Google Gemini AI features are enabled, Google may retain prompts, contextual information, and output for up to 55 days for abuse monitoring under Google's applicable service practices.

Institution may disable the AI assistant if this provider-side retention is not acceptable to Institution.

NaturalSoft will identify material provider-specific retention practices in its EDU provider documentation.

11. Voice and Voice-Cloning Features

Voice-related Student Data may include:

- text submitted for speech generation;
- voice recordings;
- reference audio;
- voice samples;
- consent recordings;
- speaker or voice profiles;
- generated synthetic audio; and
- associated metadata.

NaturalSoft will process voice-related Student Data only to provide the requested voice function, maintain security, provide support, and comply with law.

NaturalSoft will not:

- sell voice data;
- disclose voice data to marketers;
- use voice data for targeted advertising;
- create commercial student profiles from voice data; or
- use voice data to train a general-purpose AI or voice model.

Institution administrators may enable or disable available voice-cloning features.

Enabling voice cloning through an administrator setting does not by itself establish legally sufficient consent.

Institution is responsible for:

- determining whether voice cloning is appropriate for its users;
- obtaining required Parent or student authorization;
- obtaining authorization from the person whose voice is used;
- providing required synthetic-media notices;
- complying with biometric, privacy, publicity, personality, education, and child-protection laws; and
- preventing impersonation or deceptive use.

An Authorized User must not clone another person's voice without valid authorization.

NaturalSoft may request evidence of authorization and may suspend or delete an unauthorized voice.

12. Analytics

NaturalSoft may collect general usage events to understand:

- feature adoption;
- document-upload activity;
- document types;
- MP3 feature usage;
- voice-feature usage;
- AI-feature usage;
- service reliability;
- system performance; and
- error rates.

NaturalSoft will not intentionally send the following to its general analytics provider:

- document contents;
- prompt contents;
- OCR-extracted text;
- voice-recording contents;
- generated audio contents;
- raw Student Data; or
- direct student names or email addresses.

Analytics may use pseudonymous device, session, account, or event identifiers where necessary for service measurement and security.

NaturalSoft will not use analytics to:

- identify a student for advertising;
- create a commercial student profile;
- market to students or Parents;
- sell Student Data; or
- train AI models.

13. Security Measures

NaturalSoft will maintain reasonable administrative, technical, and organizational safeguards appropriate to the nature of Student Data.

Current safeguards include:

- primary backend hosting in AWS us-east-1;

- private AWS S3 storage for user Library files;
- HTTPS using TLS 1.2 or higher for supported data transmissions;
- encryption at rest using AES-256 or cloud-provider-managed encryption;
- authentication through AWS Cognito;
- role- and function-based access restrictions;
- confidentiality obligations for authorized personnel;
- application and infrastructure logging;
- monitoring;
- incident-response procedures;
- provider-management procedures;
- deletion processes; and
- automated lifecycle deletion for applicable stored files.

Data may be temporarily decrypted within a secured processing environment when necessary to provide the requested operation.

Student Data transmitted to an authorized AI, OCR, speech, or voice provider will be transmitted through an encrypted connection.

End-user multi-factor authentication is not currently available.

Institution is responsible for:

- securing administrator accounts;
- securing email and identity-provider accounts;
- assigning accounts only to authorized users;
- promptly removing former users;
- protecting devices;
- configuring AI and voice-cloning settings;
- controlling shared content; and
- notifying NaturalSoft of suspected unauthorized access.

14. Personnel Access and Training

NaturalSoft will limit access to Student Data to personnel and contractors who reasonably require access to:

- operate the Services;
- provide support;
- investigate an error;
- address fraud or abuse;
- respond to an incident; or
- comply with law.

Authorized personnel will be subject to confidentiality obligations.

Where required by an applicable state rider, personnel with access to Student Data will receive training concerning applicable confidentiality, privacy, and security obligations before or within a reasonable period after receiving access.

15. Operational and Error Logs

NaturalSoft may maintain application, infrastructure, and text-to-speech logs in AWS CloudWatch and related secured systems.

Logs may contain:

- timestamps;
- request identifiers;
- service and feature information;
- device or account identifiers;
- system status;
- error codes;
- file references;
- operational metadata; and
- limited text that could not be processed or that generated an error.

NaturalSoft may review limited failed text where reasonably necessary to diagnose an error or improve service reliability.

NaturalSoft will:

- restrict access to logs;
- use logs only for operations, security, troubleshooting, and legal compliance;
- not use log contents for advertising or AI training; and
- remove standard operational logs approximately monthly.

Institution should avoid submitting unnecessary sensitive information.

16. Subprocessors

Institution authorizes NaturalSoft to use the Subprocessors identified in Schedule 3.

NaturalSoft will:

- use Subprocessors only to provide or support the Services;
- disclose only information reasonably necessary for their function;
- require appropriate confidentiality and data-protection obligations;
- assess relevant provider security and privacy practices;
- remain responsible for Subprocessor performance to the extent required by the Agreement and law; and
- maintain a current EDU Subprocessor list.

NaturalSoft may replace or add a Subprocessor.

For paid Institution accounts, NaturalSoft will provide commercially reasonable advance notice of a new Subprocessor that will materially process Student Data.

Institution may object within 15 days on reasonable student privacy or security grounds.

The Parties will work in good faith to resolve the objection.

Where no reasonable alternative is available, Institution may:

- disable the affected optional feature; or
- terminate the affected Service before the new Subprocessor begins processing.

Any refund will be limited to prepaid fees for the unused portion of the terminated affected Service.

Payment, adult support, and sales providers may process administrator or billing contact information without processing Student Data.

17. Data Location

NaturalSoft's primary backend infrastructure and user Library storage are hosted in AWS us-east-1 in the United States.

Certain authorized AI, OCR, speech, authentication, and voice providers may process information in other provider regions or support locations.

Provider-specific locations may depend on:

- the selected feature;
- deployment region;
- provider endpoint;
- provider configuration; and
- technical availability.

NaturalSoft does not guarantee state-specific data residency unless expressly stated in a signed Order.

18. Data Retention

NaturalSoft will not retain Student Data longer than reasonably necessary for the contracted educational purpose, applicable Library functionality, security, legal compliance, and the retention periods in Schedule 2.

Unless an Order or state rider states otherwise:

- text submitted solely for text-to-speech conversion is deleted after the conversion process is completed;
- registered EDU user Library files may be retained for up to one year;

- unregistered user uploads may be retained for up to 24 hours;
- downloadable MP3 files may be retained for up to 30 days;
- standard operational logs are removed approximately monthly;
- users may delete supported Library files and audio at any time;
- account login information is deleted from active systems promptly after confirmed account deletion;
- other active account information is deleted within 24 hours after confirmed account deletion, subject to lawful exceptions;
- Azure OCR and Document Intelligence may temporarily retain inputs or results for up to 24 hours;
- Google Gemini abuse-monitoring information may be retained for up to 55 days when applicable AI features are enabled; and
- encrypted backup copies may remain until overwritten through NaturalSoft's ordinary backup rotation.

NaturalSoft may retain limited information where reasonably necessary for:

- billing;
- tax;
- fraud prevention;
- security investigations;
- legal claims;
- regulatory requirements;
- enforcement of agreements; or
- a lawful preservation obligation.

Retained information remains subject to applicable confidentiality and security obligations.

19. Institution-Directed Deletion

Institution may request deletion of Student Data under Institution's control.

NaturalSoft will delete supported Student Data from active systems within a commercially reasonable period and no later than 30 days after receiving a verified written request, unless:

- Institution requests a later date;
- deletion is technically dependent on Institution action;
- law requires retention;
- the information is subject to a preservation obligation; or
- the information has already been de-identified.

Individual Library deletion functions may remove active files sooner.

Residual information may remain temporarily in encrypted backups until overwritten through the ordinary backup cycle.

NaturalSoft will not restore deleted Student Data to active production systems except where reasonably necessary for disaster recovery or security investigation.

20. Access, Correction, and Portability

Institution is responsible for receiving and verifying requests from:

- Parents;
- students;
- Eligible Students;
- educators; and
- other authorized persons.

NaturalSoft will provide reasonable assistance to Institution to:

- locate supported Student Data;
- provide available copies;
- correct supported account information;
- delete supported Student Data; and
- respond to legally valid privacy requests.

NaturalSoft may direct an individual who submits a request directly to NaturalSoft to contact Institution.

NaturalSoft will not disclose Institution-controlled Student Data directly to an individual unless:

- Institution authorizes the disclosure;
- the individual's authority has been appropriately verified; or
- law requires NaturalSoft to respond directly.

21. Security Incidents

NaturalSoft maintains an incident-response process covering:

- detection;
- triage;
- containment;
- investigation;
- remediation;
- recovery;
- notification; and
- post-incident review.

NaturalSoft will notify Institution without unreasonable delay after confirming a Security Incident that results in unauthorized acquisition, access, use, or disclosure of Student Data.

The notice will include, to the extent reasonably available:

- the nature of the incident;
- relevant dates;
- affected systems or Services;
- categories of affected information;
- categories or approximate number of affected individuals;
- containment and remediation steps;
- recommended Institution actions; and
- an incident contact.

NaturalSoft may provide information in stages as its investigation develops.

Institution is responsible for notifying Parents, students, employees, regulators, or other affected persons unless applicable law expressly assigns that obligation to NaturalSoft.

NaturalSoft will reasonably cooperate with Institution's legally required notifications.

Notification under this section does not constitute an admission of fault or liability.

Where an applicable state rider requires a shorter period or additional process, the state rider controls.

22. Legal Requests

NaturalSoft may disclose Student Data where required by a valid law, regulation, subpoena, warrant, court order, or governmental demand.

Unless legally prohibited, NaturalSoft will:

- notify Institution before disclosure;
- provide sufficient information for Institution to seek protection;
- reasonably challenge a demand NaturalSoft believes is unlawful or disproportionate; and
- disclose only information legally required.

NaturalSoft may disclose information without prior notice where reasonably necessary to address an imminent threat to safety or where law prohibits notice.

23. Return and Destruction at Termination

Before expiration or termination, Institution should use available export functions to retrieve information it wishes to retain.

Upon expiration or termination, NaturalSoft will:

- terminate Institution-managed user access;
- preserve Student Data for a limited transition period where agreed;
- delete active Student Data upon Institution's verified request; and
- otherwise apply the retention periods in Schedule 2.

Unless the Order provides a longer transition period, Institution should submit an export or deletion request within 30 days after termination.

NaturalSoft may delete remaining active Student Data after that period.

NaturalSoft may retain de-identified information and legally required records.

24. Accessibility

NaturalSoft develops NaturalReader as an accessibility-focused reading and text-to-speech platform.

NaturalSoft considers accessibility factors including:

- reading usability;
- keyboard access;
- screen-reader support;
- highlighting;
- font adjustment;
- color contrast;
- reduced visual distraction;
- OCR-supported reading;
- mobile accessibility;
- dyslexia-friendly presentation options; and
- immersive reading functions.

Accessibility support may vary by:

- web, mobile, or extension platform;
- browser;
- operating system;
- assistive technology;
- document type;
- source-document accessibility;
- AI feature; and
- third-party component.

NaturalSoft will make its current Accessibility Statement and VPAT available to Institution.

NaturalSoft does not represent that every Service component fully conforms to WCAG 2.1 AA unless a current product-specific VPAT or signed Order expressly states that level of conformance.

25. Institution Responsibilities

Institution is responsible for:

- determining that the Services are suitable for its educational use;
- complying with Applicable Student Privacy Laws;
- providing required notices;
- obtaining legally required consent;
- authorizing users;
- maintaining accurate administrator contacts;
- configuring optional AI and voice-cloning features;
- responding to Parent and student requests;
- controlling which Student Data is submitted;
- not submitting unnecessary highly sensitive information;
- protecting downloaded or exported files;
- informing NaturalSoft of state-specific requirements before purchase;
- attaching Institution-required notices, including a Parents' Bill of Rights where applicable; and
- obtaining approval from its procurement, privacy, legal, and technology personnel.

Institution will not submit:

- full payment-card information;
- Social Security numbers;
- financial aid records;
- government identification documents;
- protected health information subject to HIPAA;
- criminal investigation records; or
- biometric identification databases

unless NaturalSoft expressly agrees in writing.

26. Compliance Information and Reviews

NaturalSoft will make available reasonable documentation concerning its handling of Student Data, including:

- this Education Addendum;
- the Data Processing Addendum;
- the Privacy Policy;

- the Security Overview;
- the AI Use and Transparency Policy;
- the Subprocessor List;
- the Incident Response Policy summary;
- the Accessibility Statement;
- the VPAT; and
- reasonable questionnaire responses.

Institution may request a documentation-based compliance review no more than once per year unless:

- a confirmed Security Incident affects Institution;
- a regulator requires a review; or
- an applicable state rider provides otherwise.

Any audit must:

- provide reasonable advance notice;
- occur during normal business hours;
- avoid unreasonable disruption;
- protect NaturalSoft and other customers' confidential information;
- exclude source code;
- exclude other customers' data;
- exclude detailed vulnerability information that could create a security risk; and
- be at Institution's expense unless required otherwise by law.

27. No Universal State Certification

NaturalSoft does not represent that one standard agreement automatically satisfies every United States state, school district, university, or local education privacy requirement.

Institution must notify NaturalSoft before execution if Institution requires:

- a state-specific student data agreement;
- a Parents' Bill of Rights;
- a district-specific security plan;
- a specific breach-notification deadline;
- cyber insurance;
- a specific data-residency commitment;
- source-code escrow;
- state-specific indemnification;
- a background-check requirement; or
- a particular security certification.

State-specific terms apply only if included in a rider signed by both Parties.

28. Liability

Liability arising under this Education Addendum is subject to the exclusions and limitations of liability in the Master Subscription Agreement unless:

- applicable law prohibits the limitation; or
- a signed state rider expressly states otherwise.

This Education Addendum does not create an unlimited indemnity or unlimited liability obligation.

29. Term

This Education Addendum remains effective while NaturalSoft processes Student Data for Institution.

Provisions concerning:

- confidentiality;
- prohibited data use;
- deletion;
- legal compliance;
- liability;
- security incidents; and
- data ownership

survive termination to the extent necessary to fulfill their purpose.

SCHEDULE 1

SERVICE AND DATA DESCRIPTION

A. Educational Purposes

NaturalSoft processes Student Data to provide:

- accessibility and reading assistance;
- text-to-speech;
- document reading;
- OCR;
- audio generation;

- document storage;
- reading synchronization;
- AI-assisted education features;
- authorized voice functions;
- administrator functions;
- technical support; and
- security and service operations.

B. Data Subjects

Data subjects may include:

- students;
- prospective students;
- educators;
- administrators;
- Institution personnel;
- Parents;
- guardians;
- Eligible Students;
- contractors; and
- people whose information appears in Customer Content.

C. Data Categories

Data may include:

- email address;
- account identifier;
- Institution membership;
- authentication information;
- uploaded text;
- documents;
- PDFs;
- images;
- OCR content;
- prompts;
- AI output;
- voice input;
- voice samples;
- generated audio;
- annotations;
- reading settings;

- feature usage;
- IP address;
- device information;
- operational logs;
- error logs; and
- support communications.

D. Data Not Required for Standard Accounts

NaturalSoft does not require the following standard account-profile information:

- full legal name;
- telephone number;
- home address;
- date of birth;
- student ID;
- grade;
- attendance;
- discipline;
- medical information;
- disability information;
- IEP or 504 information; or
- demographic information.

E. Processing Frequency

Processing occurs on demand or continuously while Institution and Authorized Users use the Services.

SCHEDULE 2

EDU DATA RETENTION SCHEDULE

Data Category	Standard Retention
Text submitted solely for TTS conversion	Deleted after conversion is completed
Registered EDU Library uploads	Up to one year, subject to automated deletion and earlier user or Institution deletion

Data Category	Standard Retention
Unregistered uploads	Up to 24 hours, subject to automated lifecycle deletion
Downloadable MP3 files	Up to 30 days, then automatically deleted
User-deleted Library content	Deleted from active NaturalSoft systems after the deletion request is processed
Standard application and TTS logs	Approximately one month
Failed or unprocessed text contained in error logs	Approximately one month, with restricted troubleshooting access
Azure OCR or Document Intelligence inputs and results	Up to 24 hours under applicable provider processing
Google Gemini abuse-monitoring information	Up to 55 days where applicable AI features are enabled
Login information after confirmed account deletion	Deleted promptly from active authentication systems
Other active account data after confirmed account deletion	Within 24 hours, subject to legal and technical exceptions
Encrypted backups	Until overwritten through NaturalSoft's ordinary backup rotation
Billing, security, legal, and fraud records	As reasonably necessary for the applicable purpose or law
The Parties may agree to shorter retention periods in an Order where technically available.	

SCHEDULE 3

EDU SUBPROCESSORS AND SERVICE PROVIDERS

The exact provider used depends on Institution configuration and the features enabled.

Amazon Web Services

Purpose:

- backend infrastructure;
- AWS us-east-1 hosting;

- compute;
- databases;
- AWS S3 Library storage;
- AWS CloudWatch;
- authentication through AWS Cognito;
- monitoring; and
- application logs.

Potential Data:

- account identifiers;
- email addresses;
- Customer Content;
- documents;
- generated files;
- voice information;
- IP addresses;
- usage information;
- logs; and
- diagnostics.

Primary Location: United States.

Google Gemini

Purpose:

- paid AI assistant functionality; and
- selected AI document features.

Potential Data:

- prompts;
- selected document content;
- context;
- AI responses; and
- request metadata.

Special Practice:

Google may retain prompts, context, and output for up to 55 days for abuse monitoring.

Gemini Grounding and Gemini Live are not enabled for Institution Customer Content unless NaturalSoft gives notice and Institution authorizes the applicable feature.

Google Gemini Speech / Gemini 2.5 Flash TTS

Purpose:

- selected text-to-speech and voice generation.

Potential Data:

- text;
- speech-generation instructions;
- generated audio; and
- request metadata.

OpenAI

Purpose:

- selected text-to-speech voice functions.

Potential Data:

- text submitted for speech generation;
- generated audio; and
- request metadata.

NaturalSoft uses available Zero Data Retention or Modified Abuse Monitoring controls where supported by the applicable endpoint and approved configuration.

Microsoft Azure AI

Purpose:

- selected AI processing;
- Azure Vision OCR;
- Azure Document Intelligence;
- Azure Speech;
- standard and neural voices; and
- selected voice-related functionality.

Potential Data:

- uploaded images or documents;
- OCR-extracted content;
- text submitted for speech generation;
- voice samples;
- generated audio; and
- operational metadata.

Azure OCR and Document Intelligence may temporarily retain inputs or results for up to 24 hours.

OmniVoice

Purpose:

- selected voice cloning;
- multilingual speech generation;
- voice design; and
- text-to-speech.

OmniVoice is hosted within NaturalSoft-controlled AWS infrastructure and is treated as a NaturalSoft-operated model component rather than a separate hosted Subprocessor.

Google Analytics

Purpose:

- aggregate and pseudonymous feature-use analytics;
- system and feature performance;
- product reliability; and
- general adoption measurement.

NaturalSoft will not intentionally send document contents, prompts, OCR content, voice contents, generated audio contents, or direct student identifiers to Google Analytics.

Payment and Adult Administrative Providers

Payment, sales, and support providers may process adult administrator contact, billing, or support information.

They are not authorized to receive Student Data unless separately identified in the EDU Subprocessor List.

SCHEDULE 4

OPTIONAL CALIFORNIA K-12 RIDER

This Schedule applies only where Institution is a California K-12 local educational agency and NaturalSoft is an operator subject to the California K-12 Pupil Online Personal Information Protection Act.

For California Covered Information, NaturalSoft will not knowingly:

1. engage in targeted advertising on the Services where advertising is based on information acquired through K-12 use;
2. use information obtained through the Services to target advertising on another service;
3. create or amass a profile about a pupil except in furtherance of a K-12 school purpose;
4. sell pupil information;
5. disclose Covered Information except:
 - to provide the contracted K-12 service;
 - to an authorized service provider subject to appropriate restrictions;
 - at Institution's direction;
 - with appropriate consent;
 - for legitimate research permitted by law; or
 - as required by law;
6. use Covered Information for a purpose unrelated to the contracted K-12 school purpose; or
7. use Covered Information to train a general commercial AI model.

NaturalSoft will:

- maintain reasonable security procedures appropriate to Covered Information;
- require relevant providers to protect Covered Information;
- delete Covered Information under Institution's control when Institution submits a verified deletion request;
- support legally valid deletion requests from a Parent, guardian, or former pupil as required by California law;
- not use Covered Information to recommend products or services unrelated to the K-12 purpose; and
- continue to apply this Rider to Covered Information after a merger, acquisition, or corporate transaction.

This Rider does not require NaturalSoft to delete information that applicable law permits or requires NaturalSoft to retain.

SCHEDULE 5

OPTIONAL NEW YORK EDUCATION LAW §2-d RIDER

This Schedule applies only where Institution is a New York educational agency subject to Education Law §2-d and Part 121 and NaturalSoft receives Student Data or Teacher or Principal Data as a third-party contractor.

1. Incorporated Institution Documents

The following Institution documents are incorporated:

- Institution's Parents' Bill of Rights for Data Privacy and Security;
- Institution's Data Privacy and Security Policy;
- Institution's required supplemental information; and
- the completed NaturalSoft Data Security and Privacy Plan below.

Institution must provide these documents before NaturalSoft processes covered New York data.

2. Exclusive Purpose

NaturalSoft may use Student Data and Teacher or Principal Data exclusively to provide, secure, support, and maintain the contracted NaturalReader EDU Services.

NaturalSoft will not use such data for:

- marketing;
- advertising;
- sale;
- commercial profiling;
- unrelated product development;
- AI model training; or
- another purpose not expressly authorized by the Agreement.

3. Access Restrictions

NaturalSoft will limit access to personnel and authorized Subprocessors who require access to perform the contracted Services and have a legitimate educational interest in the information.

4. Disclosure Restrictions

NaturalSoft will not disclose covered information without prior written consent from the Parent or Eligible Student except:

- to authorized personnel and Subprocessors carrying out the Agreement;
- where permitted by FERPA;
- where directed by Institution; or
- where required by statute, court order, subpoena, or another lawful demand.

Where legally permitted, NaturalSoft will notify Institution no later than the time of a legally compelled disclosure.

5. Security Program

NaturalSoft will maintain reasonable administrative, operational, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of covered information.

To the extent required by New York law, NaturalSoft will maintain technologies, safeguards, and practices reasonably aligned with the applicable NIST Cybersecurity Framework requirements.

Before signing this Rider, NaturalSoft and Institution will review any Institution-specific security policy to determine whether NaturalSoft can comply.

6. Personnel Training

NaturalSoft personnel with access to covered New York Student Data or Teacher or Principal Data will receive appropriate privacy and security training concerning applicable confidentiality obligations before or within a reasonable time after receiving access.

7. Subcontractors

NaturalSoft may use the Subprocessors listed in Schedule 3.

NaturalSoft will require those Subprocessors to:

- process covered data only for the contracted purpose;
- maintain appropriate safeguards;
- limit access;
- restrict further disclosure; and
- comply with applicable contractual requirements.

8. Storage and Security

Covered information is primarily hosted in AWS us-east-1.

NaturalSoft protects information in transit using TLS 1.2 or higher and protects stored production data using AES-256 or cloud-provider-managed encryption.

9. Access and Accuracy

Institution is responsible for receiving and verifying Parent, student, Eligible Student, teacher, and principal requests.

NaturalSoft will reasonably assist Institution in locating, accessing, correcting, or deleting supported covered data.

10. Contract Expiration

Upon expiration or termination:

- Institution may export available information;
- NaturalSoft will terminate Institution-managed access;
- NaturalSoft will delete active covered information upon Institution's verified instruction;
- deletion will occur within the period stated in Section 19 of the Education Addendum unless Institution requires a shorter legally mandated period; and
- residual encrypted backups will be deleted through the ordinary backup cycle.

11. Security Incidents

NaturalSoft will notify Institution of a breach or unauthorized release in the most expedient way possible and without unreasonable delay.

NaturalSoft will provide reasonably available information needed for Institution to investigate and make legally required notices.

To the extent required by New York law, NaturalSoft will reimburse Institution for legally mandated notification costs resulting directly from an unauthorized release caused by NaturalSoft or its authorized Subprocessor.

12. Complaints and Cooperation

NaturalSoft will reasonably cooperate with Institution's Data Protection Officer and with legally authorized New York State Education Department inquiries.

13. Data Security and Privacy Plan

NaturalSoft's plan consists of:

- the security measures in Section 13;
- the personnel controls in Sections 14 and 15;
- the Subprocessor controls in Section 16;
- the incident-response provisions in Section 21;
- the return and deletion provisions in Sections 18, 19, and 23;
- the provider information in Schedule 3; and

- NaturalSoft's Security Overview and Incident Response Policy.