Think Tech Solutions Privacy Policy

Think Tech Solutions, Inc.
Think Tech legal and district documentation set

Effective date: March 6, 2026

Last updated: March 6, 2026

Think Tech Solutions, Inc. ("Think Tech," "we," "us," or "our") provides apps, software, websites, mobile-enabled functionality, and related educational technology services that are collectively referred to in our Terms of Service as the "Services." This Privacy Policy explains how we collect, use, disclose, protect, retain, and otherwise process Personal Information when people visit our websites, communicate with us, or use the Services.

This Privacy Policy should be read together with our Terms of Service, school or district agreements, Data Privacy Agreements, and any other applicable order forms or procurement documents. If a school or district agreement imposes stronger privacy or security protections for Customer Data or Student Data, that agreement controls to the extent of any conflict.

1. Scope and user types

There are two primary types of users associated with the Services: (a) Educators, which include teachers, administrators, and other authorized employees or representatives of educational institutions; and (b) Students who may interact with portions of the Services at the direction of an Educator or Educational Institution. Think Tech markets and contracts primarily with Educators and Educational Institutions, not directly with children as consumers.

This Privacy Policy applies to:

- Educators and Educational Institutions that purchase, administer, or use the Services;
- Students whose information is processed in connection with school-authorized use of the Services;
- Parents or guardians who contact us about Student Data or a student's school-authorized use of the Services;
- Visitors to Think Tech websites, help resources, pricing pages, demo pages, and procurement pages; and
- Individual Educators who purchase a subscription directly, where offered.

2. Our role; school official status; controller and processor relationships

For Customer Data and Student Data handled on behalf of an Educational Institution, Think Tech generally acts as a service provider or processor and, where applicable, as a "school official" with a legitimate educational interest, subject to the direction and control of the applicable Educational Institution and the limits of FERPA and other applicable law.

For website visitors, procurement contacts, demo requests, support inquiries, newsletter or event signups, billing contacts, and other direct business interactions, Think Tech generally acts as the controller of the Personal Information it collects for those purposes.

Education Institutions remain responsible for determining what Student Data is shared with Think Tech, for configuring school-authorized integrations and student access workflows, and for handling requests that must be processed at the school or district level.

3. Information we collect

3.1 Educator and Educational Institution information

- names, work email addresses, usernames, passwords, authentication credentials, and profile details;
- school, district, building, subject, grade-level, classroom, and account role information;
- billing, invoicing, tax, purchase order, subscription, and BOCES / CoSer procurement information;
- support, implementation, training, and contract-related communications; and
- materials created or stored by Educators in the Services, including lesson plans, lesson materials, reports, presentations, assessments, or other educational content.

3.2 Student and classroom information

Depending on how an Educator or Educational Institution configures the Services, we may process the following categories of Student or classroom information:

- student profile and account data, such as first and last name, email address, external or district student identifiers, organization or school affiliation, grade level, profile image, accessibility or accommodation preferences, and terms-acceptance records;
- classroom, roster, enrollment, group, and lesson participation data, whether entered directly by an Educator or received from a district-enabled SSO, rostering, LMS, or SIS integration;
- student responses, work product, scores, grades, highlights, teacher feedback, user comments, parent-student messages where messaging is enabled, and related progress or performance data;
- behavioral and engagement metadata such as timestamps, lesson position, last-seen data, session events, and certain classroom-integrity indicators such as background or tab-switch events where a feature is designed to monitor active lesson participation;
- district or regional benchmark or standard-performance data imported by authorized administrators; and
- authentication and security information such as hashed passwords, password reset codes, SSO provider IDs, refresh tokens, passkey credentials or challenges where enabled, and push-notification tokens where mobile notifications are enabled.

3.3 Information collected automatically

- IP address, browser type, operating system, device identifiers, network information, and other general device or connection details;
- authentication events, timestamps, session identifiers, access logs, feature usage records, error logs, and security audit trails;
- performance and diagnostic data used to maintain, secure, monitor, and improve the Services; and
- cookies, local storage entries, pixels, SDKs, and related technologies used for session management, chat, analytics, advertising attribution, and preferences.

3.4 Information from integrations and third parties

When an Educational Institution enables an integration or sign-in connection, Think Tech may receive identity, roster, provider-account, or related synchronization data from providers such as Clever, ClassLink, Google, Microsoft, Schoology, or EdLink. We may also receive payment-related data from Stripe, adult-business contact data from HubSpot or Mailchimp, website analytics data from Google Analytics or Heap, and device tokens from Firebase Cloud Messaging where those features are used.

4. How we use information

We use Personal Information and, where applicable, Customer Data and Student Data only for legitimate educational, operational, security, and legal purposes. Specifically, we use information to:

- provide the Services, create and administer accounts, authenticate users, manage role-based permissions, support district-administered account controls, and deliver requested functionality;
- operate classroom workflows, student participation features, messaging features, reporting, analytics, and district-authorized integrations;
- detect, investigate, prevent, and remediate fraud, abuse, misuse, security incidents, service disruptions, and violations of our Terms of Service or other agreements;
- provide support, onboarding, implementation assistance, training, customer success, and service-related communications;
- maintain, debug, monitor, improve, and develop the Services, including through the use of aggregated and de-identified information where appropriate;
- administer billing, invoicing, BOCES / CoSer procurement workflows, subscription management, tax compliance, and related financial operations;
- send product, support, renewal, event, or procurement-related communications to adult Educators, administrators, or other business contacts where permitted by law, while offering an unsubscribe mechanism for non-essential promotional emails;
- comply with applicable law, regulations, court orders, audits, and contractual obligations; and
- document, investigate, and respond to complaints, incidents, disputes, and enforcement matters.

5. Artificial intelligence and automated features

The Services may include artificial intelligence, machine learning, or similar automated functionality ("AI Features") to support instructional tools, content generation, educator-facing recommendations, summaries, analysis, or other school-authorized educational functions.

Current AI feature and governance practices reflected in our product and security materials include:

- Educators remain the final decision-makers and are responsible for reviewing AI-generated outputs before use with Students or for instructional decisions.
- Student personally identifiable information submitted through the Services is not used to train public or generalized AI models.
- Where feasible for a given feature, student names and teacher names are masked or replaced with placeholders before prompts are sent to an external AI provider; the reverse-mapping needed to reconstruct names remains inside Think Tech systems and is not sent to the model provider.

- AI prompts and responses may be logged inside Think Tech systems to deliver the requested result, troubleshoot issues, and maintain service quality.
- Third-party AI providers may include OpenAI, Anthropic, and Google Cloud-based AI tooling as configured for a specific feature or release.

6. How we share information

Think Tech does not sell Student Data. We may share Personal Information, Customer Data, or Student Data only in the following circumstances:

- with Educational Institutions, Educators, and other authorized users that administer or use the Services;
- with trusted service providers and subprocessors that support hosting, storage, backups, payments, communications, analytics, notification delivery, or AI-enabled functionality, subject to contractual restrictions and confidentiality obligations;
- with district-enabled integration providers such as Clever, ClassLink, Google, Microsoft, Schoology, or EdLink at the direction of the Educational Institution;
- with auditors, professional advisers, insurers, or other parties that need the information to provide services to Think Tech under appropriate confidentiality restrictions;
- in connection with a merger, acquisition, restructuring, bankruptcy, or sale of assets, subject to applicable law and reasonable continuity of privacy protections; and
- to comply with law, court order, subpoena, or other legal process, or to protect the rights, safety, security, or property of Think Tech, our users, or the public.

7. Cookies, analytics, and similar technologies

Think Tech uses cookies and similar technologies on the public website and certain Service surfaces for the following categories of purposes: strictly necessary or functional purposes such as maintaining sessions and chat continuity; analytics purposes such as understanding website and product usage; and advertising-attribution or marketing purposes on adult-facing website pages.

You can control cookies through browser settings and, where available, our website's consent or preference controls. Disabling certain cookies may limit functionality. Additional detail is provided in the Cookie and Analytics Notice later in this pack.

8. Data retention and deletion

Think Tech retains information for as long as reasonably necessary to provide the Services, operate the business, comply with law, resolve disputes, enforce agreements, and maintain backups and security records. Retention can differ materially by data type and feature.

Based on the current data inventory, key retention characteristics include:

- many production application tables use soft-delete or archival flags rather than immediate hard deletion, meaning records may remain in protected systems after they are removed from day-to-day use;
- student profile, lesson, comment, message, and integration-linkage records generally persist unless actively deleted, archived, overwritten, or removed through an account, roster-sync, or administrative workflow;
- refresh tokens are configured to expire after 90 days, while passkey challenges are short-lived and intended to expire within seconds or minutes;

- billing, tax, procurement, legal, and incident records may be retained longer where required by law or reasonably necessary to protect contractual rights; and
- district-specific agreements may impose more specific deletion timelines or secure-destruction requirements.

9. Security

Think Tech maintains administrative, technical, and physical safeguards designed to protect Personal Information and Customer Data against unauthorized access, acquisition, use, disclosure, alteration, or destruction.

Current high-level security controls reflected in our security posture materials include:

- HTTPS/TLS enforced for web traffic and encrypted transport for supported service communications;
- encryption at rest using disk or storage-level encryption controls, including LUKS and AES-256-class controls where applicable;
- role-based access control, organization-scoped data isolation, and session-based authentication for users;
- two-factor / multi-factor controls for personnel access to sensitive systems according to current public legal disclosures;
- secrets and credentials stored in Kubernetes Secrets / environment variables rather than hard-coded in production configuration;
- logging, exception handling, metrics, and monitoring through application logging and AWS CloudWatch-related telemetry;
- vulnerability management, patching, and periodic security testing and review.

10. FERPA, COPPA, and New York Education Law § 2-d

Think Tech has designed the Services to support Educational Institutions in meeting their responsibilities under FERPA, COPPA, and applicable state laws, including New York Education Law § 2-d and Part 121 where applicable. School-authorized Student Data is processed solely for educational or school-operational purposes authorized by the Educational Institution, applicable contracts, and law.

Where an Educational Institution relies on school authorization under COPPA for school-authorized use, Think Tech expects collection and use of Student information to occur only for the Educational Institution's use and benefit, and not for unrelated commercial purposes. Think Tech's school-official positioning and Student Data handling are intended to operate within the direct-control and legitimate-educational-interest requirements of FERPA.

11. Rights and choices

Rights and request pathways differ depending on the individual and on whether Think Tech is acting as a controller or as a service provider/processor.

Educators may review or update certain account information through the Services where those settings are available.

If an account is provided by an Educational Institution, the Educational Institution may manage the account, reset passwords, terminate access, view usage information, and access or modify content associated with the account.

Parents, guardians, and eligible Students seeking access to, correction of, or deletion of Student Data should generally direct their request to the applicable Educational Institution because the school or district controls the education record and determines the authorized response.

Individuals for whom Think Tech acts as a controller, such as website visitors or direct business contacts, may contact Think Tech to request access, correction, deletion, or opt-out from non-essential promotional communications, subject to verification and applicable law.

Adult users may opt out of promotional email communications by following the unsubscribe instructions in the message.

12. International processing and data location

Think Tech primarily stores and processes core application data in the United States, including AWS-hosted infrastructure in the U.S. If Think Tech later transfers Personal Information outside the United States, Think Tech will use contractual, technical, or organizational safeguards required by applicable law.

13. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes to the Services, law, or business practices. When we do, we will post the updated policy and revise the "Last updated" date. Where a change materially affects how Customer Data or Student Data is handled, we will provide any additional notice required by law, contract, or our commitments to Educational Institutions.

14. Contact us

General privacy, account, and policy inquiries, security incident reports or security questions: hello@thinktechsolutions.org

Mailing address: Think Tech Solutions, Inc., 207 Commerce Drive Suite 103, Amherst, NY 14228

Formal legal notices under the Terms of Service should be sent using the notice information specified in the current Terms of Service.