Data Retention and Deletion Notice

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

This notice supplements the Privacy Policy by summarizing the retention and deletion characteristics reflected in Think Tech's current data inventory. Actual retention can vary by table, feature, district agreement, technical implementation, legal hold, and backup cycle.

Data category	Baseline retention approach	Deletion / disposition notes
Customer Data in active school or district accounts	Retained while the account, contract, or district-authorized use remains active	Account closure, administrative deletion, archival, or district-specific deletion workflow; many records use soft-delete or archival states before permanent removal
Student profile and roster records	Often persist until removed, overwritten by sync, soft-deleted, or otherwise administratively removed	Student and roster records may remain in protected systems after deactivation; some integration-linkage rows do not automatically cascade delete
Live lesson, response, comment, and message data	No uniform application-level TTL identified in the current inventory	Remains until archived, deleted, or otherwise removed through platform or administrative workflows
AI query logs	No explicit scheduled TTL identified in the current inventory	Prompt/response records remain until manually purged or removed through future lifecycle controls
Refresh tokens	90 days from creation	Expired tokens are automatically cleaned up during login flows
Passkey challenges	Seconds or minutes until expiration	Intended for immediate use and expiry as part of WebAuthn ceremonies
Passkey credentials	Persist until deleted by the user or removed with the related account	Long-lived authentication material containing public-key metadata only
Billing, tax, contract, and procurement records	Retained as required by law, accounting rules, and contract administration needs	May outlast service-access periods

Backups and disaster-recovery copies	Retained according to AWS RDS / S3 configuration and environment-specific backup schedules	Residual copies may remain in encrypted backups until overwritten or deleted in the ordinary course

Where a district agreement or DPA requires more specific deletion timing, secure destruction language, or certificates of destruction, Think Tech may provide those commitments in the applicable agreement or contract supplement. Residual copies may remain in protected backup or log systems for continuity, incident response, or legal compliance until they age out or are overwritten.