

New York Education Law § 2-d / Parents' Bill of Rights and Supplemental Information

Think Tech Solutions, Inc.

Think Tech legal and district documentation set

This document is intended as district-ready supplemental language for use with contracts involving New York educational agencies. It should be reviewed together with the Privacy Policy, any district-specific DPA, Appendix R / Exhibit 2 language, and the contract scope for the applicable product modules.

Part A. Parents' Bill of Rights for Data Privacy and Security

- Student personally identifiable information ("Student PII") received by Think Tech under a school or district contract will not be sold or released for marketing or other commercial purposes unrelated to the authorized educational function of the Services.
- Parents and eligible students have the right to inspect and review the complete contents of the student's education record maintained by the Educational Institution, including portions maintained electronically by a third-party contractor.
- State and federal laws, including Education Law § 2-d, 8 NYCRR Part 121, FERPA, COPPA, and other applicable laws, protect the confidentiality of Student PII.
- Reasonable administrative, technical, and physical safeguards associated with industry standards and best practices, including encryption, access controls, logging, password protection, and backup controls, should be in place when Student PII is stored or transferred.
- Parents, eligible students, teachers, principals, and other authorized complainants have the right to have complaints about possible breaches or unauthorized releases of Student PII addressed.
- Parents and eligible students have the right to be notified in accordance with applicable law and regulation if a breach or unauthorized release of Student PII occurs.
- Think Tech personnel and authorized service providers with access to Student PII should receive privacy and security training appropriate to their roles before or as part of being granted such access.
- Contracts with third-party contractors or subprocessors that receive Student PII on Think Tech's behalf should address the applicable statutory and regulatory data privacy and security requirements.

Complaint contacts typically include:

- the Educational Institution's designated privacy / data protection contact;
- Think Tech Solutions, Inc. at hello@thinktechsolutions.org; and
- the NYSED Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, privacy@nysed.gov.

Part B. Contract supplemental information

| Field | District-ready language |
|--|--|
| Name of contractor | Think Tech Solutions, Inc. |
| Products / Services covered | Educational technology services and modules offered through Think Tech's Services, including educator tools, classroom and lesson functionality, district-authorized integrations, reporting, messaging, analytics, and AI-enabled educator support features that are authorized under the contract. |
| Exclusive purposes for which Student PII will be used | To provide, host, secure, support, maintain, authenticate, improve, and administer the district-authorized educational functionality of the Services; to enable district-authorized integrations and notifications; to investigate security or service issues; and to comply with law and contract. |
| Categories of Student PII that may be received or accessed | Depending on district configuration: student names, email addresses, internal or external student IDs, organization or school identifiers, roster or class membership, grade level, accommodation preferences, profile image, student responses and work product, scores or assessment data, comments or messages, usage and security logs, and authentication / integration identifiers. Think Tech does not require APPR data unless separately and expressly agreed in writing. |
| Whether Student PII will be sold or used for marketing | No. Student PII is not sold and is not used for advertising or unrelated commercial profiling. |
| Storage locations | Core application data is primarily stored in the United States using AWS-hosted infrastructure, including AWS RDS, S3, SES, and related services; the primary production region reflected in the current data inventory is us-east-1. |
| Encryption and security controls | HTTPS/TLS for data in transit; encryption at rest using disk or storage-level controls; role-based and organization-scoped access controls; credential and secret management; logging, monitoring, and backup / disaster-recovery practices; password hashing; and additional safeguards described in the Privacy Policy. |
| Subprocessors and authorized service providers that may access Student PII | AWS (hosting / storage / backups), AWS SES (transactional email where applicable), OpenAI / Anthropic / Google Cloud AI services used for configured AI features with minimized or de-identified data where feasible, Firebase Cloud Messaging for push notifications where enabled, and district-enabled providers such as Clever, ClassLink, Google, Microsoft, Schoology, and EdLink. |
| How parents may challenge the accuracy of Student PII | Parents and eligible students should direct education-record correction requests to the Educational Institution, which controls the student record and determines the appropriate response under FERPA and state law. |
| How complaints may be made | Complaints may be submitted to the Educational Institution, to Think Tech using the contacts above, or to the NYSED Chief Privacy Officer at privacy@nysed.gov / 89 Washington Avenue, Albany, NY 12234. |

Part C. New York breach coordination summary

If Think Tech discovers a covered breach or unauthorized release of protected student, teacher, or principal data, Think Tech will notify the educational agency without unreasonable delay and no later than seven calendar days after discovery.

The educational agency then reports the incident to NYSED's Chief Privacy Officer without unreasonable delay and no later than 10 calendar days after discovery or receipt of the contractor's notice.

Affected parents, eligible students, teachers, and/or principals are generally notified by the educational agency as expeditiously as possible and no later than 60 calendar days, unless a lawful delay applies.