Braintrust Tutors Inc.
Privacy Policy

Effective Date: July 1, 2026
Last Updated: October 5, 2026

1. Introduction

Braintrust Tutors Inc. ("Braintrust," "we," "us," or "our") provides academic intervention products and services to schools and school districts ("Schools" or "LEAs") through Braintrust's learning platform ("Platform"), including High-Impact Tutoring ("HIT"), in which Braintrust contracts with tutors directly to deliver tutoring and academic interventions to students using the Platform and Braintrust curricula, and Braintrust Spark ("Spark"), in which a School's own staff utilizes the Platform to deliver instruction directly to students. We refer to HIT and Spark together herein as the "Services."

This Privacy Policy explains what information we collect through the Services and Braintrust's public website (the "Website"), how we use and share it, and the choices and rights available to students, parents and guardians, teachers, district staff, and Website visitors. It also describes the specific commitments we make regarding student data under the Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA").

This Policy is a statement of Braintrust's privacy practices, applicable across every state in which we operate. It is not itself a contract, and it does not create, expand, or limit any legal obligation beyond those in the applicable Service Agreement and Data Privacy Agreement ("DPA") between Braintrust and a School. In most cases, Braintrust provides the Services under a written agreement with a School or LEA, including a DPA that governs our handling of student data for that School. Where this Policy and a School's DPA address the same subject, the DPA controls as between Braintrust and that School; this Policy describes our general practices and is intended to be consistent with, and to supplement, those agreements.

2. Who This Policy Covers

This Policy applies to information we collect through the Services and the Website from or about:

- Students who use HIT or Spark through their School;
- Parents and guardians, to the extent they interact with the Services or receive communications about a student's participation in HIT or Spark;
- Teachers, school counselors, and district administrators who use the Services to refer, monitor, or support students; and
- Visitors to the Website and individuals who contact Braintrust directly, including prospective School and district partners.

This Policy applies to the Services and the Website and, solely as described in Section 19, to recruiting text messages sent to job applicants and candidates. Except for those recruiting text messages, this Policy does not govern Braintrust's employment, recruiting, tutor payroll, or other internal personnel records, or any separate direct-to-consumer product Braintrust may offer outside a School relationship. A separate privacy notice may apply to those activities. Sections 7 and 8 describe protections that apply specifically to student data under FERPA and COPPA, Section 6 describes the automated and artificial intelligence systems used in the Platform, and Section 9 describes Braintrust's prohibition on advertising and tracking within the student-facing portions of the Services.

3. Our Role: We Work For Schools, Not Advertisers

Braintrust is retained by Schools and LEAs to deliver HIT and Spark on their behalf. With respect to student data, Braintrust acts as a service provider and, for purposes of FERPA, as a "school official" with a legitimate educational interest in student data — not as an independent data controller free to use student information however it wishes. We collect and use identifiable student data only to provide, operate, secure, and support the Services; fulfill the School's instructions; and perform other School-authorized educational purposes permitted by the applicable agreement and law. We use de-identified and aggregated data for general product improvement only as described in Section 12.

Because Schools are our contracting partners, Braintrust does not initiate communications with parents, guardians, or students without the School's prior approval and only does so in connection with the Services. Braintrust never initiates communications with parents, guardians, or students for marketing, satisfaction surveys, or general outreach. If a parent, guardian, or student contacts Braintrust directly, Braintrust may respond to that specific inquiry, but any further communication requires the School's prior approval and must relate to the Services.

In this Policy, student data means personal information directly related to an identifiable student that Braintrust receives, maintains, or creates in providing the Services for a School, and includes education records protected by FERPA where applicable. For readability, this Policy uses "student data" in lowercase throughout rather than as a capitalized defined term, but the meaning is consistent every time the phrase is used.

4. Information We Collect

4.1. Information About Students

Depending on the services a School has engaged Braintrust to provide, we may collect the following categories of student information, generally provided to us by the School or generated through a student's use of the Services:

- **Identifiers:** first and last name, student ID number, school-issued email address, and grade level.
- **Enrollment and roster data:** school, class, and program or intervention assignment.
- **Assessment and progress data:** assessment scores, responses, and academic progress information.
- **Session and attendance data:** session dates, duration, and attendance, whether the session is a HIT tutoring session or a Spark instructional session.
- **Program and intervention records:** progress reports and multi-tiered support (MTSS) documentation.
- **Session content:** interaction and work product from live HIT tutoring sessions or Spark instructional sessions and an audio and/or video recording of the session and an associated transcript. Where a session is recorded, the recording and transcript are used for the purposes described in Section 5 and, where applicable, the AI-assisted analysis described in Section 6.2, and are retained consistent with Section 12.
- **Guardian or contact information:** a parent or guardian's name or contact information, where required for a particular engagement.

Braintrust collects only the categories of student data reasonably necessary to deliver the services a School has engaged us to provide, as documented in our agreement with that School.

4.2. Information About Teachers and District Staff

We collect the name, work email address, role, and school/district affiliation of teachers and administrators who use the Services, along with their login and usage activity on the Platform, in order to administer accounts and support HIT and Spark.

4.3. Technical and Platform Data

Like most software platforms, we automatically collect limited technical information needed to operate and secure the Services, such as device and browser type, IP address, log-in timestamps, and application error and performance logs. We use this information for operational, security, and product-improvement purposes described in Section 5 — never to serve advertising, as described in Section 9.

4.4. Information From Our Public Website

If you visit our public marketing website (as opposed to the Platform), we may collect standard website analytics and information you submit through a contact form. This information is not student data and is handled separately from the Platform.

5. How We Use Information

We use the information described above only for the following purposes:

- To deliver HIT tutoring and Spark instructional services, including scheduling, conducting, and supporting live and platform-based sessions;
- To provide progress reports, dashboards, and analytics to the School regarding a student's participation and progress;
- To operate, maintain, secure, and troubleshoot the Services;
- To develop and improve the Services, including through the automated and AI systems described in Section 6 and, for product improvement generally, using de-identified or aggregated data as described in Section 12; and
- To comply with our contractual obligations to Schools and applicable law.

We do not use student data for marketing, advertising, data mining, or behavioral profiling, and we do not use it for any commercial purpose unrelated to providing and improving the Services. This restriction is described further in Section 9.

6. Artificial Intelligence and Automated Systems

The Platform uses two categories of automated systems in connection with HIT and Spark. The first is a rules-based system and does not use artificial intelligence or machine learning. The second uses artificial intelligence to analyze session content only after all Confidential Information and student data have been removed. Braintrust does not use these systems to make decisions that produce legal or similarly significant effects on a student, such as decisions regarding enrollment, discipline, or eligibility for services. For purposes of this Section, "Confidential Information" includes information designated as confidential under the applicable agreement and all student data.

6.1. Diagnostic and Lesson-Recommendation Engine

The Platform's diagnostic and lesson-recommendation logic is a rules-based engine that applies deterministic performance thresholds to a student's responses in order to produce mastery classifications and recommend that student's next lesson. This engine is not a machine-learning system: it has no trained model, and it is not updated or trained using student data. A given student's response data is used only to compute that student's own recommendations at the time they use the Platform, whether in a HIT or a Spark session.

6.2. AI-Assisted Post-Session Analysis

Separately, the Platform uses large language models — currently provided through AWS Bedrock (Anthropic Claude) and OpenAI — to analyze session transcripts after a HIT or Spark session has ended. This analysis supports guidance to the person who led the session (a Braintrust tutor in HIT, or a School staff member in Spark) and assesses instructional fidelity, including identifying safety signals, assessing session quality, and surfacing curriculum-alignment insights to Braintrust staff and program operators. Braintrust does not submit Confidential Information or student data to any artificial intelligence system. Before any transcript or other

session content is submitted, Braintrust removes all Confidential Information and student data. Only scrubbed, de-identified content is submitted for AI-assisted analysis.

6.3. Limits on Our AI Vendors, and On Us

Our written agreements with these AI providers, including AWS Bedrock's standard terms:

- Prohibit the provider from using the data we submit, or the outputs generated, to train, fine-tune, improve, or otherwise develop the provider's underlying models;
- Prohibit the provider's personnel from reviewing the data we submit, except where necessary for abuse monitoring or as required by law; and
- Are separate from Braintrust's own commitment: Braintrust does not use Confidential Information or student data to create, train, fine-tune, improve, or otherwise develop any artificial intelligence or machine-learning system.

7. FERPA Compliance

7.1. Braintrust's Role as a "School Official"

Braintrust provides services that a School would otherwise use its own employees to perform, operates under the direction and control of the School with respect to education records, and is subject to the use and confidentiality restrictions described in this Policy and in our agreements with Schools. On that basis, Braintrust acts as a "school official" with a "legitimate educational interest" in student education records under FERPA (20 U.S.C. § 1232g; 34 C.F.R. Part 99), permitting the School to share student education records with us without separate parental consent for the purpose of providing the Services.

7.2. Permitted Use of Education Records

Consistent with FERPA, we use student education records solely to:

- Deliver HIT and/or Spark, as the School has engaged us to provide;
- Maintain the technical systems necessary to deliver those services;
- Provide reports and analytics to the School on student progress; and
- Improve the Services using de-identified or aggregated data as described in Section 12, or use identifiable education records for improvement only when specifically authorized by the School and permitted by the applicable agreement and law.

We do not use education records for marketing, advertising, data mining, behavioral profiling, or any other commercial purpose unrelated to providing the Services, and we do not disclose education records to third parties except to the limited service providers described in Section 10, each of which is bound by confidentiality and use restrictions.

7.3. Parent and Eligible Student Rights

Because a student's official education records are maintained by the School or LEA, requests to inspect, review, correct, or amend a student's education records should ordinarily be directed to the student's School in the first instance, consistent with the School's FERPA procedures. Braintrust cooperates with School requests to provide, correct, or delete student data in our systems, and will assist a School in responding to a parent's or eligible student's FERPA request. A parent or eligible student may also contact us directly using the information in Section 18, and we will respond to that request and coordinate with the applicable School as appropriate. Consistent with Section 3, we do not independently initiate further contact with the family beyond responding to their own inquiry, without the School's approval.

7.4. Redisclosure

We do not redisclose personally identifiable information from education records except (a) to the service providers described in Section 10, acting on our behalf and under written confidentiality and use restrictions; (b) back to the School; (c) as directed or authorized in writing by the School; or (d) as required by law, in which case, where legally permitted, we will provide advance notice to the School.

8. COPPA and Children's Privacy

Many students who use the Services are under the age of 13. The Services are provided to students exclusively through their School as part of a school-authorized academic program — students and families do not sign up to the Platform directly, and Braintrust does not knowingly collect personal information from children through a consumer-facing product outside of that school context.

8.1. School Consent on Behalf of Parents

Under guidance from the Federal Trade Commission interpreting the Children's Online Privacy Protection Act (COPPA), a school may consent on behalf of parents to the collection of a student's personal information by an education technology provider, where that information is used solely for a school-authorized educational purpose and for no other commercial purpose. Braintrust relies on this framework: our School and district agreements confirm that student data is collected and used only to provide the contracted educational services, and Braintrust does not use student personal information for any purpose beyond providing those contracted educational services — and, in particular, never for advertising or marketing, as described in Section 9.

8.2. Data Minimization for Children

Consistent with COPPA's data minimization principle, we:

- Collect only the categories of student information reasonably necessary to provide the services a School has engaged us to deliver;
- Do not condition a student's participation in HIT or Spark on the disclosure of more personal information than is reasonably necessary;
- Do not enable students to publicly post personal information or to be individually contacted by strangers through the Services; and
- Maintain the information security practices described in Section 11 to protect children's information.

8.3. Where School Authorization Is Not Sufficient

If the School's authorization is not legally sufficient, Braintrust will not collect the child's personal information until the School has obtained the required consent or has approved a legally compliant consent process. Braintrust will not independently contact a parent or guardian to obtain consent without the School's prior approval.

8.4. Parent Review, Deletion, and Opt-Out

A parent or guardian who wishes to review the personal information collected from their child, request that it be deleted, or decline further collection, may contact their School or contact Braintrust directly using the information in Section 18. Because the School is our direct partner and typically the party with the enrollment relationship, we may coordinate certain requests with the School, consistent with Section 7.3, but we will not refuse to respond to a parent's direct request solely on that basis. Consistent with Section 3, however, we will not use a parent's request as an occasion to initiate unrelated contact with the family.

9. No Advertising or Student Tracking

Braintrust does not treat student attention as a product. The following commitments apply to all student-facing components of the Services, regardless of student age, and regardless of whether a particular state independently requires them:

- *No advertising to students.* We do not display third-party advertisements to students on the Platform (in either HIT or Spark) or in student-facing communications.
- *No ad networks or ad-tech on the student experience.* We do not permit third-party advertising networks, ad exchanges, or advertising pixels, beacons, or tags on any student-facing page or in-session interface.
- *No sale of student data.* We do not sell, rent, or trade student personal information to any third party, and we do not disclose it in exchange for money or other valuable consideration, for advertising or any other purpose.
- *No behavioral profiling or targeted advertising.* We do not use student personal information to build behavioral advertising profiles, and we do not use student data for targeted or "behavioral" advertising as those terms are used in state student privacy and consumer privacy statutes.
- *No cross-context tracking of students.* We do not use tracking technologies (such as third-party cookies, advertising SDKs, or device fingerprinting) on the student experience to track students across other websites or online services, or to build a profile for any purpose unrelated to providing the Services.
- *AI is not advertising.* The AI-assisted post-session analysis described in Section 6.2 is used only for session-facilitator guidance and instructional-quality purposes; it is never used to build an advertising profile of a student or to deliver targeted content.
- *Analytics are limited and operational.* Any analytics, performance-monitoring, or session-troubleshooting tools used within the Services (see Section 10 below) are used solely to operate, secure, and improve the Services, are contractually restricted from using data for advertising, and — where they involve session capture — are configured to filter or scrub sensitive content before transmission.

This section reflects the type of no-sale, no-targeted-advertising commitment increasingly required by state student data privacy laws (for example, statutes modeled on California's Student Online Personal Information Protection Act, and comparable laws in other states), which Braintrust honors as a single baseline practice across every district we serve, not only where independently mandated by a particular state.

10. How We Share Information

We do not share student data with third parties except with the limited categories of service providers below, each of which is contractually bound to use data only to provide services to Braintrust, to maintain confidentiality, and to comply with applicable data protection law, including FERPA. We remain responsible for these service providers' compliance with our obligations to Schools.

- **Cloud hosting and infrastructure** (e.g., Amazon Web Services) — to host and process platform data, including student data.
- **Single sign-on and roster synchronization** (e.g., Clever, Google) — to authenticate students, teachers, and staff and keep rosters current, limited to identifiers and roster data.
- **Live session delivery** (e.g., Lessonspace) — to power the collaborative, in-session surface.
- **AI-assisted post-session analysis** (AWS Bedrock (Anthropic Claude) and OpenAI) — as described in Section 6.2.
- **Logging and monitoring** (e.g., Sumo Logic) — to aggregate application and infrastructure logs for security and reliability.
- **Business intelligence and analytics** (e.g., Amazon QuickSight) — limited to aggregated or derived metrics used to report on program outcomes.
- **Product troubleshooting and session replay** (e.g., LogRocket) — limited to client-side events and metadata, filtered to remove sensitive content before transmission.
- **Tutor scheduling notifications** (e.g., Twilio) — used only to send scheduling texts to Braintrust's adult tutors; this does not involve student data.

None of these service providers is an advertising or marketing vendor, and none is authorized to use student data for advertising, consistent with Section 9. We will notify a School in advance of any material change to the service providers who process that School's student data, consistent with our agreement with the School, and

beyond these service providers we disclose student data only: (a) to the School itself; (b) as directed or authorized in writing by the School; or (c) where required by law or valid legal process, in which case, to the extent legally permitted, we will notify the School before disclosure.

11. How We Protect Information

Braintrust maintains an information security program aligned with the NIST Cybersecurity Framework, covering product security, infrastructure security, IT security, and incident management. Key safeguards include:

- **Encryption:** student data and other personal information is encrypted in transit and at rest using strong, industry-standard cryptography (e.g., AES-256-GCM), with access-controlled, regularly rotated keys.
- **Access controls:** role-based access limits student data access to authorized personnel on a need-to-know basis; multi-factor authentication protects staff access to systems containing student data.
- **Secure development:** a secure software development lifecycle including threat modeling, code review, automated vulnerability scanning, and independent third-party penetration testing.
- **Data isolation:** logical separation of customer data in our multi-tenant environment, with all data stored in the United States.
- **Personnel:** criminal background checks and confidentiality agreements for employees, mandatory security training, and prompt deactivation of access upon role change or departure.
- **Monitoring and incident response:** continuous monitoring and alerting, a documented incident response process, and post-incident root-cause review.
- **Insurance:** cyber liability insurance covering data breach response and liability.

If we become aware that a security incident has affected student data, we will notify affected Schools without unreasonable delay, in accordance with the notification timeframe and process set out in our agreement with that School, and will cooperate with the School's own notification obligations to parents, students, and regulators.

12. Data Retention and Deletion

We retain student data, including authorized session recordings and transcripts, as necessary to provide the Services under our agreement with the applicable School. Promptly following the expiration or termination of the agreement, we de-identify and anonymize student data so that neither an individual student nor the School can reasonably be identified or re-identified. We may retain and use de-identified data for product improvement, research, and analytics.

Upon the School's written request, we will delete the applicable student data in accordance with the School's agreement and applicable law. Deletion is subject to limited exceptions for secure backup copies, legal holds, dispute preservation, and security logs. Information retained under an exception remains protected, is not used for any other purpose, and is deleted when the applicable retention requirement ends.

Subject to applicable law and the applicable Service Agreement and DPA, Braintrust may use and disclose data that has been de-identified and aggregated so that no student, parent, guardian, or School can reasonably be identified or re-identified, alone or in combination with other reasonably available information. Braintrust may use such data for product improvement, analytics, research, benchmarking, evaluating the effectiveness of the Services, and demonstrating program outcomes to Schools, school districts, government agencies, governing bodies, prospective customers, and other stakeholders, including through reports, presentations, proposals, and marketing materials. Braintrust applies reasonable disclosure-avoidance measures, including appropriate suppression of small data sets, and will not attempt to re-identify the data. Braintrust will not identify a School or use its name, logo, or individually attributable results without the School's prior written approval.

13. Your Rights and Choices

13.1. Requests Involving Student Data

Schools may request access to, correction of, export of, return of, or deletion of student data. Braintrust will reasonably assist with and fulfill verified School instructions in accordance with the applicable agreement and law. Students, parents, and guardians seeking to exercise rights concerning student data should ordinarily submit their requests to the School that authorized the student's participation.

13.2. Requests From Educators, Tutors, and Other Adult Users

Teachers, district staff, and tutors may access and update certain account information directly within the Platform, and may otherwise contact us directly using the information in Section 18 to request access to, correction of, or deletion of their own account information. We may need to verify the requester's identity, and may retain information where permitted or required by law or an applicable School agreement.

Anyone may ask questions about our data practices at any time using the contact information in Section 18. Consistent with Sections 7 and 8 above, we generally direct requests involving student data to the relevant School and support the School in responding.

14. State Privacy Rights (Non-Student Data)

Depending on where you live, state consumer privacy laws (such as the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and similar laws in other states) may give you rights to confirm whether Braintrust processes your personal information; to access, correct, delete, or obtain a copy of it; or to appeal our response to a request.

These rights generally apply to non-student personal information handled outside of the FERPA and COPPA framework described in Sections 7 and 8 — for example, information about educators, school personnel, or tutors, or information collected through our public website. Many of these state laws do not apply to education records governed by FERPA or to data Braintrust processes solely on behalf of a School, which remains governed by Sections 7 and 8 above and by our agreement with that School.

To exercise an applicable right regarding non-student personal information, contact us using the information in Section 18. We may need to verify your identity and authority before acting on a request, and we will not discriminate against you for exercising a privacy right.

15. Cookies and Similar Technologies

The Services use a limited set of first-party cookies and similar technologies necessary for core functionality, such as keeping a user logged in, remembering session state, and supporting the security features described in Section 11. Consistent with Section 9, we do not use cookies or similar technologies on the Platform for advertising, cross-site tracking, or behavioral profiling. Our public marketing website may use standard website analytics cookies, separate from the Platform, to understand site traffic.

16. Data Location

All Services data, including student data, is stored and processed in the United States, in industry-standard secure data centers. We do not currently transfer student data outside the United States.

17. Changes to This Policy

We may update this Policy from time to time to reflect changes in our practices or applicable law. If we make material changes, we will notify our School partners and update the "Last Updated" date above. Because this

Policy is not itself a contract, we may update it unilaterally; however, no change to this Policy will reduce the protections we have separately, contractually committed to provide to a School under that School's DPA without the School's agreement, and we will not apply a material change retroactively where doing so is prohibited by law or by our agreement with a School.

18. Contact Us

If you have questions about this Privacy Policy or Braintrust's data practices, or if you are a parent, guardian, or eligible student with a question about student data, please contact us at:

Braintrust Tutors Inc.
Attn: Privacy
Address: 100 Vandam St, Ste 5a, New York, NY 10013
Phone: (646) 397-3696

Privacy inquiries: privacy@braintrusttutors.com
Security inquiries: security@braintrusttutors.com

For requests involving student data specifically, please contact your School first, consistent with Section 13.1 above; the School can then provide Braintrust with verified instructions.

19. Information for Job Applicants and Candidates

SMS Privacy Notice. If you provide your mobile phone number and consent to receive recruiting text messages from Braintrust Tutors Inc., we may contact you via SMS we may contact you via SMS for recruiting-related purposes. These messages may include:

- Application status updates;
- Interview scheduling and confirmations;
- Reminders and follow-ups; and
- Offer-related communications.

We do not use SMS messaging for marketing purposes, and we do not sell or share your mobile number or SMS consent with third parties for their marketing use. SMS communications may be facilitated through third-party service providers (such as our texting platform, Grayscale by Paylocity), who process data on our behalf in accordance with our instructions and applicable privacy laws.