

Student Data Privacy Agreement

Sample agreement between a school district and CompPrep AI

Sample agreement provided for convenience. Districts may use their own DPA; we're happy to review and sign the district's standard agreement. Bracketed text is for the District to complete. This sample is not legal advice; please have it reviewed under your district's procedures.

District	[School District name], [address], [city], [state] (the "District")
Provider	CompPrep AI, Sugar Land, Texas. Contact: support@compprep.app (the "Provider," "we" or "us")
Service	CompPrep AI at compprep.app: practice tests, flashcards, lessons, an AI coach and AI practice judge for career and technical student organization (CTSO) competitions, plus chapter tools for advisors and officers (the "Service")
Effective date	The date of the last signature below

1. Purpose and scope

This Agreement explains how the Provider protects Student Data when the District, its schools, teachers or advisors use the Service. It applies to all Student Data the Provider receives from or on behalf of the District, or that students create while using the Service under the District's account or chapter. If this Agreement conflicts with the Provider's terms of service or privacy policy, this Agreement controls.

2. Definitions

- **Student Data** means any information about a student that identifies the student, or could reasonably be used to identify the student, that the Provider receives or creates through the District's use of the Service. It includes education records as defined by FERPA.
- **De-identified Data** means data from which all direct and indirect identifiers have been removed, so that there is no reasonable basis to believe it could be used to identify a student, school staff member or family.
- **Subprocessor** means a third party that processes Student Data on the Provider's behalf to help provide the Service.
- **Security Breach** means unauthorized access to, or acquisition of, Student Data that compromises its security, confidentiality or integrity.

3. FERPA and District control

For Student Data covered by the Family Educational Rights and Privacy Act (FERPA), the District designates the Provider as a "school official" with a "legitimate educational interest," as permitted by 34 CFR 99.31(a)(1). The Provider performs a service the District would otherwise use its own staff for, and is under the District's direct control with respect to the use and maintenance of Student Data.

- Student Data remains the property of, and under the control of, the District.

- The Provider uses Student Data only to provide the Service for the District's educational purposes.
- The Provider does not re-disclose Student Data except to its Subprocessors as described in this Agreement, as the District directs, or as the law requires.

4. Children under 13 (COPPA)

The Service is for users 13 and older. Sign-up asks for a birth month and year once to confirm age, blocks anyone under 13, and does not store the birth date. The Provider does not knowingly collect personal information from children under 13. If it learns it has, it deletes that information promptly. The District agrees not to direct students under 13 to create accounts.

5. Student Data we collect

The Provider collects only what the Service needs to work. Exhibit B lists each data element and why it is used. In summary:

- Name, email address, grade and school.
- Chapter membership and role (member, officer or advisor), attendance check-ins and chapter points.
- Practice activity and scores, including test answers, written responses and AI judge transcripts.
- AI coach messages, which are processed to produce an answer and are not saved on the Provider's servers.
- Optional: a device address (push token) if a student turns on notifications, and a parent or guardian email if a student adds one.

Payments. Payments are handled by Stripe. The Provider never sees or stores full card numbers.

What we do not collect. The Provider does not collect precise (GPS) location, contacts or advertising identifiers. It does not store photos or video of students: optional camera feedback runs entirely on the student's device and is never uploaded. Voice practice is turned into text by the student's browser, and the Provider never receives the audio. The Provider does not build advertising profiles.

6. Permitted uses and prohibitions

The Provider may use Student Data only to provide, secure, support and improve the Service for the District's educational purposes. The Provider will not:

- Sell, rent or trade Student Data.
- Use Student Data for targeted advertising or to choose ads, or show ads to students covered by the District's chapter plan.
- Build a profile of a student for any purpose other than the educational purposes of the Service.
- Use Student Data to market products or services to students or families.
- Disclose Student Data except as allowed by this Agreement or required by law.

Ads. Students covered by a chapter plan never see ads in the app. A student using a free account may see one small, labeled Google AdSense ad at the end of a few overview screens, never during practice, tests or AI sessions. These ads are non-personalized and tagged for teen treatment, and the Provider never sends Student Data to the ad network. As with any web content, the ad loads from Google, which receives the

device's IP address and browser details and may use cookies to limit repeats and prevent fraud.

The Provider may create and use De-identified Data to improve the Service and for aggregate reporting (for example, which practice topics are most often missed). The Provider will not try to re-identify De-identified Data and will not share it in a way that could identify a student or school without the District's consent.

7. AI processing

The AI coach, AI practice judge and feedback features are powered by Claude, an AI model provided by Anthropic through its commercial API.

- To produce feedback, the Provider sends the practice question or scenario, the student's response or transcript, and the event. The Provider does not include the student's name or email address. Text a student types is sent as written.
- Under the Provider's agreement with Anthropic, inputs and outputs sent through the commercial API are not used to train Anthropic's models by default. The Provider does not opt in to sharing Student Data for model training, and does not itself use Student Data to train AI models.
- AI feedback is practice help. It can be wrong, and it is not an official score or a prediction of competition results.

8. Subprocessors

The Provider uses the Subprocessors listed in Exhibit A, each under a written agreement that limits its use of data to providing its service and requires it to protect that data. The Provider keeps a current list at compprep.app/dpa and will notify the District by email before adding a Subprocessor that will handle Student Data. The Provider remains responsible for its Subprocessors' handling of Student Data under this Agreement.

9. Security

The Provider maintains reasonable administrative, technical and physical safeguards appropriate to the sensitivity of Student Data, including:

- Encryption in transit (HTTPS/TLS) and encryption at rest through its database and hosting providers.
- Access controls that limit each user to the data their role allows, enforced in the database with row-level security.
- Limiting staff access to Student Data to people who need it to run or support the Service.
- Logging of administrative actions, such as role and points changes in chapters and administrator actions in the Service.
- Keeping software and dependencies up to date and reviewing security advisories from its providers.

The Provider does not claim any third-party security certification. Its Subprocessors maintain their own security programs.

10. Security Breach notification

If the Provider discovers a Security Breach affecting the District's Student Data, it will notify the District's contact in writing within 72 hours of discovery. The notice will describe, as far as then known: what happened and when, the types of Student Data involved, the steps taken to contain it, and a contact person. The Provider will update the District as it learns more, cooperate with the District's response, and help the District meet any notice duties it has to families or authorities under applicable law.

11. Access and correction requests

The District may ask the Provider to provide, correct or export a student's Student Data. The Provider will respond within 30 days. If a parent, guardian or eligible student contacts the Provider directly about District Student Data, the Provider will refer them to the District or act at the District's direction, unless the request is one students can complete themselves in the app. Students can view, edit, download and delete their own data from Profile in the app at any time.

12. Data retention and deletion

- The Provider keeps Student Data only as long as needed to provide the Service or as this Agreement allows.
- Within 30 days of the District's written request, or of the end of this Agreement, the Provider will delete the District's Student Data, including from backups, which are overwritten within 30 days. On request, the Provider will confirm the deletion in writing.
- Students can delete their own account at any time from Profile. Deletion is immediate in live systems; backups are cleared within 30 days.
- Accounts with no sign-in for 24 months are deleted, after a warning email 30 days before.
- The Provider may keep De-identified Data, and records it must keep by law (such as payment and tax records). These records are not used for any other purpose.
- Before deletion, the District may request an export of its Student Data in a common, readable format.

13. Compliance with law

The Provider complies with laws that apply to its handling of Student Data, including FERPA, the Children's Online Privacy Protection Act (COPPA), and applicable state student privacy laws, including Texas Education Code Chapter 32. If the District is in another state, the Provider will work with the District in good faith to meet that state's student privacy requirements, which the parties may add as an addendum.

14. Term and termination

- This Agreement starts on the Effective Date and stays in effect while the District uses the Service, until either party ends it under this Section.
- Either party may end this Agreement with 30 days' written notice. Either party may end it immediately if the other materially breaches it and does not fix the breach within 30 days of notice.
- When this Agreement ends, Section 12 (deletion) applies. Obligations that by their nature should continue, including confidentiality and deletion, survive termination.

15. General

- Changes to this Agreement must be in writing and signed by both parties.
- This Agreement is governed by the laws of the state where the District is located.
- Notices go to the contacts in the signature blocks below, by email or mail. Notices to the Provider: support@compprep.app.
- Signatures may be electronic, and this Agreement may be signed in counterparts.

Signatures

Each person signing confirms they are authorized to sign for their party.

School District

Name

Title

Signature

Date

Email

CompPrep AI

Name

Joseph Almijbilee

Title

Founder

Signature

Date

Email

support@compprep.app

Exhibit A: Subprocessors

Subprocessor	Purpose	Data handled
Supabase	Database, sign-in and server functions	Account, profile, chapter and practice data
Cloudflare	Hosting for compprep.app and protection from attacks	IP address and basic request details
Anthropic	AI coach, AI practice judge and practice feedback	Practice content, responses and transcripts, without names or email addresses
Resend	Account, reminder and summary emails	Email address, first name and the email's contents
Stripe	Payments, invoices, receipts and sales tax	Billing name, email, billing address or ZIP code; card and bank details are entered on Stripe's pages
Google	Sign in with Google, and text-to-speech for the AI judge's voice	Sign-in details the user allows; for text-to-speech, the AI judge's words only
PostHog	Cookieless usage analytics: page views and sign-up steps	Page addresses without codes or IDs, sign-up steps, device and browser type; no names, emails, ages, schools or user IDs

Exhibit B: Data elements

Data element	Why it is used	Required?
Name	So advisors and chapter members know who the student is	Yes
Email address	Sign-in, account and security emails	Yes
Grade	To tailor practice content	Yes
School	To help advisors confirm chapter membership	Optional
Chapter membership and role	To run chapter features	If the student joins a chapter
Attendance check-ins and chapter points	Chapter attendance and leaderboards	If the chapter uses them
Practice activity and scores	To score practice and show progress	Yes, when practicing
Written responses and AI judge transcripts	To give feedback the student can review	When the student uses those features
AI coach messages	To answer the student's question; not saved on our servers	When the student uses the coach
Push notification token	To send notifications the student turns on	Optional

Data element	Why it is used	Required?
Parent or guardian email	Monthly progress summary, after the parent confirms	Optional
Birth month and year	Age check at sign-up only; not stored	Checked, not kept