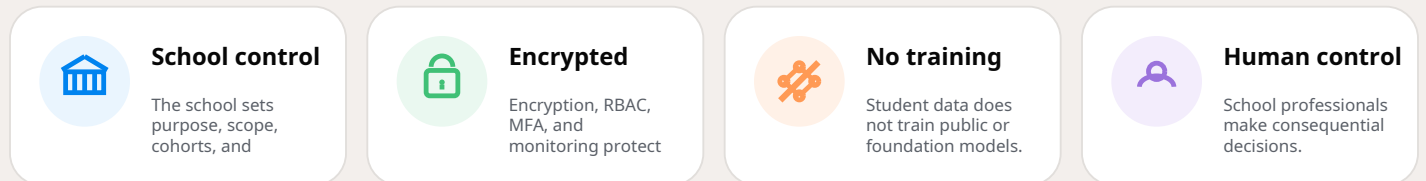


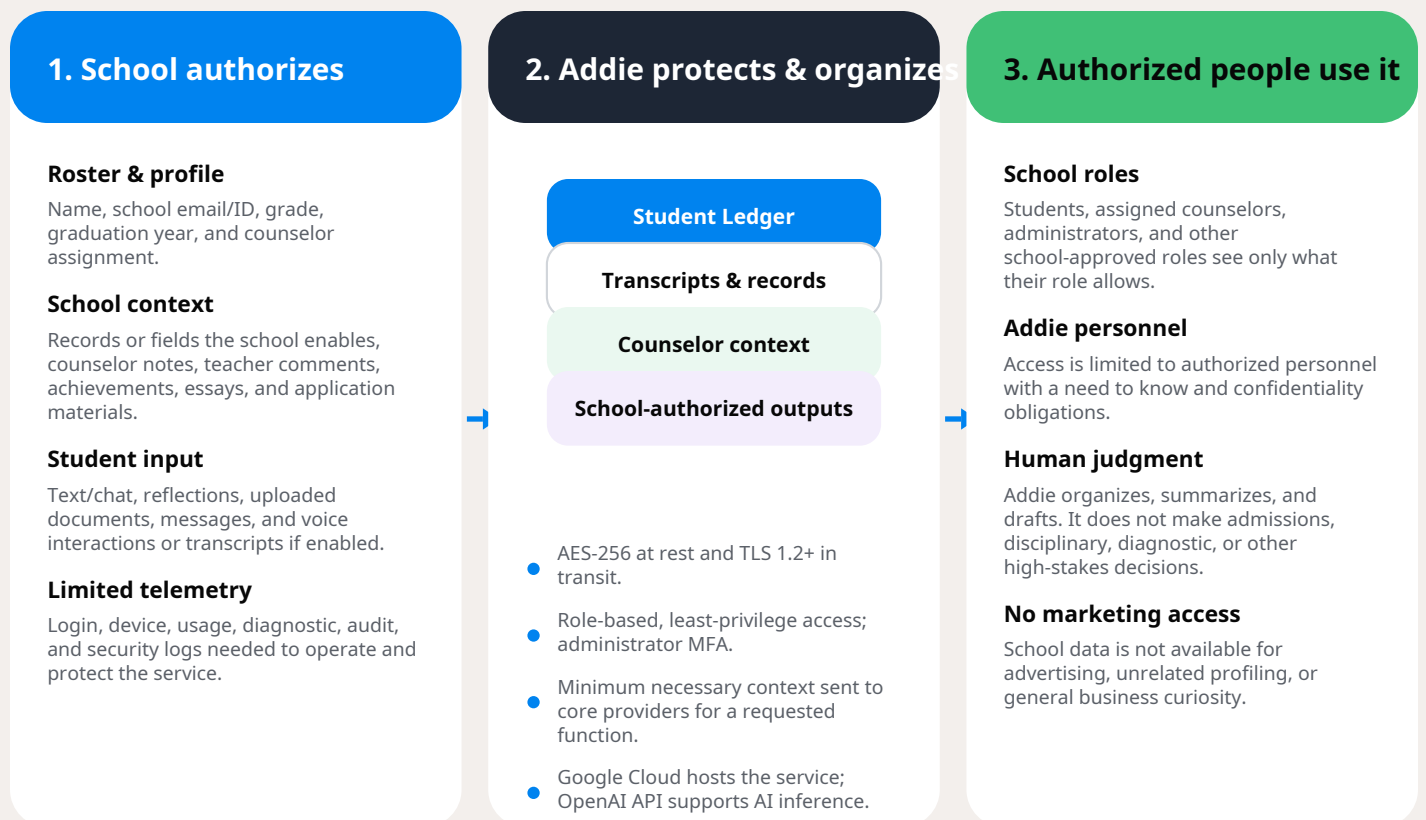
Trust is built into how Addie handles student data.

A plain-language overview for counselors, school leaders, and IT/privacy reviewers.



WHAT HAPPENS TO STUDENT INFORMATION

A simple, school-controlled data flow



Voice and audio: optional, configurable, and documented before launch

Schools can disable voice globally or by cohort. When voice is enabled, Addie documents whether the selected channel creates recordings and the applicable retention window. Transcripts and resulting context are retained only according to the school's instructions and agreement.

The school stays in control.

Addie is accountable for the service chain.

The public policy explains the baseline. A school-specific DPA or privacy pack turns those commitments into reviewable, contractual terms.



School control

The school defines the educational purpose, participating cohorts, enabled fields, voice use, prompt categories, and optional integrations. It can request export, correction, restriction, return, or deletion.



Access & security

Encryption in transit and at rest, role-based and least-privilege access, administrative MFA, confidentiality obligations, and logging/monitoring protect school-managed data.



Retention & deletion

Production data is targeted for deletion within 45 days of a verified school request or contract end, unless different terms apply. Residual encrypted backups age out through the normal rotation.



Incident response

After a confirmed incident affecting school data, Addie notifies the school without unreasonable delay and no later than 72 hours, unless a shorter timeline is required.



FERPA, COPPA & DPA

FERPA school-official terms are available when applicable, with equivalent contractual protections for private schools. Under-13 use can follow school authorization or parent consent. DPA available.



Safeguarding boundaries

Addie may flag content for school-defined adults, but it is not an emergency service, crisis hotline, medical device, or mental-health diagnostic tool. The school owns escalation and student support.

TRUST ARCHITECTURE

PURPOSE LIMITED

ROLE-BASED ACCESS

HUMAN DECISIONS



AI & MODEL DATA USE

School-managed personal data is not used to train Addie's general models or third-party foundation models. OpenAI API business data is not used for model training by default. Core providers: Google Cloud and OpenAI API.

Ready for your school's review

Request the full packet, a jurisdiction-specific privacy pack, or a school-specific DPA. The signed school agreement controls if it provides stricter terms than the public policy.

support@getaddie.com | getaddie.com/privacy



FULL PROCUREMENT & SECURITY PACKET - AVAILABLE ON REQUEST

- | | | | |
|---|---------------------------|-----------------------------------|---|
| ✓ Security overview | ✓ Data-flow diagram | ✓ Data Processing Agreement (DPA) | ✓ Terms of service |
| ✓ Privacy policy | ✓ Subprocessor list | ✓ Insurance certificates | ✓ W-9 |
| ✓ Accessibility information | ✓ Data-retention policy | ✓ Incident-response overview | ✓ AI model/data-use statement |
| ✓ Standard security questionnaire answers | ✓ FERPA/COPPA explanation | ✓ Common Sense Privacy evidence | ✓ Safeguarding & escalation explanation |