

# YouHue data protection and security overview

Written for the people who have to sign this off. Direct answers; anything not yet in place is stated as such. The full privacy policy is at [youthue.com/privacy](https://youthue.com/privacy). Last updated 14 October 2026.

## 1

### Role and purpose.

YouHue FZ-LLC (Dubai, United Arab Emirates) is the data processor for school data. The school is the controller and owns its data. We process school data only to provide YouHue to the school, on the school's documented instructions, and to keep the service secure, accurate and safe, which includes reviewing missed or mistaken safety alerts and refining the instructions we give our AI.

School data is never sold, never used for advertising, and never used to build profiles of students beyond providing the service to their school.

Everything YouHue sends to AI model providers, including what students write and families' questionnaire answers, is covered at every step: the providers can't use it to train their models, and they keep it only for a limited time. Our privacy policy sets out how long. Account details, like students' names, are replaced with a code before the AI sees anything. What a student writes is sent as written, and the AI is never allowed to write a name back. We never train or fine-tune AI models on a school's data, including how the product is used. We improve how our AI works by refining its instructions, guided by feedback from schools, teachers and students, and by reviewing missed or mistaken alerts.

No decision about a student is made solely by automated processing; school staff decide.

## 2

### Data inventory.

- **Students:** name, in the form the school chooses (first and last name, first name and last initial, or initials); school email address only where the school uses Google sign-in; class and grade or year level; check-ins (mood, mood tags, any written reflection, date and time); and the outputs the service produces about check-ins (sentiment, themes, alerts, insights). Written reflections may reveal health or wellbeing information and are treated as special category data.

## 2

- **School staff:** name, work email address, password (stored hashed, never in readable form), role, school details, the document provided to verify their role, and account activity.
- **Parents and carers:** their answers to family questionnaires, where the school uses them.
- **From connected systems (Clever, Wonde/MyLogin, ManageBac+):** the class lists and account details the school chooses to share.
- **Website:** standard usage analytics (Google Analytics) and the details people give when they contact us or book a demo.
- **Not collected:** browsing history, location, biometrics, advertising identifiers. YouHue never stores card numbers; teacher purchases are processed by Stripe.

## 3

### Hosting and residency.

All school data is hosted with Amazon Web Services in the United States (US East, Virginia). YouHue FZ-LLC operates from the United Arab Emirates, and our subprocessors process data in the United States. Data is encrypted in transit and at rest. We notify schools in advance before hosting moves to, or expands into, another country, or before anyone in a new country gains access to unencrypted school data.

**Transfers:** UK schools sign the ICO's International Data Transfer Agreement alongside the DPA; EU schools use the European Commission's Standard Contractual Clauses; for Australian and New Zealand schools we take reasonable steps consistent with the Australian Privacy Principles and New Zealand's Information Privacy Principles; each subprocessor's terms include an approved transfer mechanism.

## 4

### Access controls.

Access to school data is limited to the YouHue staff who need it to provide and support the service. It is protected by two-factor sign-in, and access is logged. Everyone with access is bound by a duty of confidentiality.

We are adding background checks and annual security, privacy and online-safety training for staff with access, regular vulnerability scanning, and independent penetration testing.

## 5

### Subprocessors.

All process data in the United States. We notify schools at least 30 days before adding or replacing a subprocessor, and schools may object on reasonable data protection grounds. The current list is also published in the privacy policy.

| Subprocessor               | Purpose                                                                                                   | Data                                                                       |
|----------------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Amazon Web Services</b> | Hosting and storage                                                                                       | All service data                                                           |
| <b>Google (Gemini)</b>     | AI analysis of check-ins: safety checks, sentiment, themes, reports, suggestions and supportive responses | Pseudonymised reflections, mood, grade level, family questionnaire answers |
| <b>Anthropic</b>           | AI generation of monthly insights                                                                         | Pseudonymised check-in data                                                |
| <b>Twilio SendGrid</b>     | Transactional and notification email                                                                      | Staff names, email addresses, notification content                         |
| <b>Loops</b>               | Email to staff users                                                                                      | Staff names, email addresses, school and plan                              |
| <b>Intercom</b>            | Customer support and help centre                                                                          | Staff contact details and support conversations                            |
| <b>Stripe</b>              | Payments for teacher purchases                                                                            | Purchaser name, email and payment details                                  |
| <b>Sentry</b>              | Error and performance monitoring                                                                          | Technical data and limited account identifiers                             |
| <b>Google Workspace</b>    | Company email and file storage, where a school shares data with us by email or file                       | Whatever the school sends                                                  |
| <b>Google Analytics</b>    | Usage analytics for the website and service                                                               | Usage and device data                                                      |

Clever, Wonde (MyLogin) and ManageBac+ are the school's own integration providers; they pass class lists and account details to YouHue, which we use only on the school's instructions.

## 6

### Retention and deletion.

School data is kept while the school's account is active; check-ins and student profiles carry over from one school year to the next. Accounts with no activity for 12 months are deleted.

We delete school data within 48 hours of confirming a school's deletion request.

## 6

When a school leaves, at its choice we return its data in a commonly used format and then delete it, or delete it; deletion is completed within 30 days after the service ends, and we confirm it in writing on request.

Backup copies are deleted when they expire under our normal backup cycle and are not used in the meantime.

## 7

### Breach notification.

If a personal data breach affects a school's data, we notify the school without undue delay and in any event within 48 hours of becoming aware of it.

The notice covers what happened and when, the categories and approximate numbers of people and records affected, the likely consequences, the measures taken or proposed, and a contact for more information, with further detail as it becomes available.

We help the school meet its own notification duties, notify regulators where the law requires, and do not notify regulators, pupils or parents about a breach of school data without first consulting the school, unless the law requires it.

## 8

### Compliance positioning.

We follow the privacy laws that apply where our schools are: the UK GDPR and Data Protection Act 2018, the EU GDPR, Australia's Privacy Act 1988 (including the Australian Privacy Principles), New Zealand's Privacy Act 2020, and US student-privacy laws including COPPA and FERPA.

**COPPA:** students use YouHue only through their school; where US law allows, schools may give consent on parents' behalf for use within the school, as COPPA permits; we show no advertising to students and allow no contact from outside the school through YouHue.

**FERPA:** we act as the school's processor, on its instructions, for the school's educational purposes only, with no onward disclosure.

**UK and EU GDPR:** we process under Article 28 terms, with safeguards for special category data, and we support DPIAs.

**Australia:** our Safer Technologies 4 Schools (ST4S) Readiness Check is in progress.

**Certifications:** we don't hold SOC 2 or ISO 27001 today. Our security measures are described in sections 3 and 4, and we complete security questionnaires on request.

## 8

**Accessibility:** we have not assessed YouHue against WCAG 2.1 AA and make no conformance claim.

Our rebuilt educator design system sets requirements for colour contrast, visible keyboard focus, screen-reader labels, reduced motion, and captions and transcripts for activity video and audio, and the student app's redesign follows written guidelines for colour contrast, touch-target size, keyboard focus and screen-reader labels. These are still being applied, have not yet been tested in the app, and no testing with assistive technology has been done.

The student app includes a voice accessibility option: a teacher switches it on for the class, each student then chooses whether to use it on their own device, and with it on a student can listen to their Learning Moment, the short supportive message they may receive after a check-in, read aloud. Tell us about specific needs and we'll answer directly.

## 9

### DPIA support.

For schools running a data protection impact assessment we provide: the data inventory and flows (section 2), this document, the subprocessor list, the retention schedule, and our standard DPA.

Questions go to [privacy@youthue.com](mailto:privacy@youthue.com) and are answered by a person; we respond within 7 business days.

## 10

### Agreements.

A standard data processing agreement is available to every school: written to UK GDPR Article 28 for UK and EU schools, with a version for US schools. We review school-issued DPAs on request.

Our DPA provides that the school owns its data; use is limited to providing, securing and supporting the service; no disclosure beyond the school's instructions; 30 days' notice of subprocessor changes with a right to object; return or deletion on exit within 30 days; 48-hour breach notice; audit and information rights (on 30 days' notice, once a year unless a breach or a regulator requires more); no decisions about a pupil made solely by automated processing; and UK transfer terms (the ICO's IDTA).

Where a DPA conflicts with our privacy policy or terms, the DPA prevails on data protection.

Anything this document does not answer, ask directly: [privacy@youthue.com](mailto:privacy@youthue.com).