

How YouHue treats children's data

Two ways to know a child.

There are two ways technology can know a child: by watching them, or by being told. Much school software watches. Students who feel watched tend to go quiet. YouHue is built on the second way. A child chooses what to share, with a teacher they trust. We call it knowing by invitation, and every decision below follows from it.

Our commitments, in one place.

We collect only what we need to provide YouHue. We show no ads, ever. We never sell school data. The school owns its data, and we act only on the school's instructions. And the teacher always decides: no decision about a child is made by software alone.

What we collect, and why.

For each student: their name, in the form the school chooses (first and last name, first name and last initial, or initials); their class and year group; their check-ins, meaning the mood they chose, any tags, any words they wrote, and when; and, if the school uses Google sign-in, their school email address. If the school uses family questionnaires, we hold the answers families give. YouHue also produces notes from check-ins, such as themes and alerts, so that teachers can act on them. That is the working set. We don't collect browsing history, location, biometrics or advertising identifiers.

Who sees what.

A student's check-in is private. It is seen by their educators and by the school staff responsible for supporting them, and never by other students. Nothing in YouHue watches a child: when a pattern in what a child has chosen to share is worth a closer look, YouHue asks the teacher, and the teacher decides. If a child's words need an adult straight away, the right adult knows now, and the school's own safeguarding process leads. Inside YouHue, access to school data is limited to the staff who need it, behind two-factor sign-in, and every access is logged.

How our AI handles what schools share.

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. The AI never diagnoses and never decides. School staff do.

Where it lives, and for how long.

School data is hosted with Amazon Web Services in the United States, encrypted in transit and at rest. We keep it while the school's account is active, so a child's picture carries over from one year to the next. Accounts with no activity for 12 months are deleted. Ask us to delete something and it is gone within 48 hours. When a school leaves, we return its data if it wants it, then delete everything within 30 days, and confirm that in writing on request. We tell schools in advance before hosting moves to another country.

If something goes wrong.

If a breach affects a school's data, we tell the school within 48 hours of becoming aware of it: what happened, who and what was affected, the likely consequences, and what we are doing about it. We help the school meet its own duties, and we notify regulators where the law requires.

Compliance.

YouHue is the school's data processor. The school stays the controller and the owner of its data. We follow the privacy laws that apply where our schools are, including the UK GDPR and Data Protection Act 2018, the EU GDPR, Australia's Privacy Act, New Zealand's Privacy Act, and US student-privacy law including COPPA and FERPA. Students use YouHue only through their school, and we never show advertising to students. In Australia, our Safer Technologies 4 Schools (ST4S) Readiness Check is in progress.

Working with your data protection officer.

We expect the DPIA conversation and we make it easy: a standard data processing agreement (written to UK GDPR Article 28 for UK and EU schools, with a US version), our subprocessor list, our retention schedule, and a technical overview written for ICT staff and DPOs. We review school-issued agreements on request. Questions go to privacy@youthue.com and are answered by a person, not a portal.

The easiest way to judge our privacy posture is to ask us the hardest question you have. privacy@youthue.com. Our full privacy policy is at youthue.com/privacy.