Sherpa
Unlock your child's potential

Sherpa Online Safeguarding Policy

Last updated 4th June 2026

Application Labs Limited, trading as Sherpa Online

Policy owner	Designated Safeguarding Lead (DSL)
Approved by	Board of Directors, Application Labs Limited
Date of issue	June 2026
Review frequency	Annual, or sooner if law, guidance, or our operating model changes
Applies to	All directors, employees, contractors, and tutors operating on the Sherpa platform

1. Purpose and scope

Sherpa Online is an online-only tutoring marketplace. We connect independent tutors with families and adult learners. Tuition takes place exclusively through video sessions delivered inside our platform. We do not provide tuition in person, in homes, or in schools.

This policy sets out how Sherpa keeps users safe on the platform, how concerns are reported and handled, and how we work with the authorities when something needs escalating beyond the platform. It is written to reflect what Sherpa actually does, not what a school or in-person tuition agency would do.

This policy is proportionate to our service. It is anchored in the legal framework that applies to an online user-to-user service (see section 14), and not in statutory guidance written for schools and colleges.

2. Our operating model: the safeguards that are built in

The strongest safeguards on the Sherpa platform are structural. They sit in the design of the service rather than in policy text. They are:

- All tuition is delivered through video sessions inside the Sherpa platform. There is no in-person contact between tutors and students at any stage.
- All sessions are video and audio recorded and retained securely for a period of 12 months. Recordings are available for review by parents, students, and Sherpa.

- Session audio is automatically transcribed and screened for indicators of grooming behaviour, inappropriate language, and contact-exchange attempts. Flagged content is reviewed by the safeguarding team.
- Tutors and students are contractually prohibited from contacting one another off-platform. Sharing of personal contact details, social media handles, or external meeting links is a breach of our Terms and grounds for removal.
- Tutors complete identity verification before they can offer lessons.
- Parents and students can report concerns directly through the Sherpa platform at any time, and can review session recordings to verify what has taken place.

These structural controls mean that almost all risks that would exist in face-to-face or unrecorded online tuition are either eliminated or detectable. This policy supports those controls; it does not replace them.

3. What information we hold, and why

Because tuition is entirely online and never takes place at a physical address, Sherpa does not collect, hold, or need:

- The student's home address.
- The student's school name or contact details.
- The student's surname (we record first name only).

The exception to this is where a tutor is also an examiner, in which case the student's school name, centre code and school postcode may be obtained from the parent and passed to the tutor for them to submit to their awarding body (without the student's name). This is to ensure the tutor is not allocated their student's paper to officially mark.

We hold the minimum information required to operate the service safely:

- Parent or account-holder name and email address.
- Student first name (surname if the parent decides to include it) and age.
- Billing postcode (held by Stripe, our payment processor, and tied to the cardholder).
- Session recordings and transcripts.
- Records of in-platform messaging between users.

In the event that a safeguarding matter escalates to a formal investigation or police inquiry, our payment processor Stripe holds additional information, including full billing details, which can be provided to the relevant authorities upon lawful request. This is the correct route for that

information: it sits with the regulated payment processor and is released only on proper legal authority, rather than being held by Sherpa in the ordinary course of business.

This data minimisation is deliberate. Holding less data reduces risk to the children and adults who use the platform, is consistent with UK GDPR principles, and aligns with the Children's Code (Age Appropriate Design Code) issued by the Information Commissioner.

4. Who this policy is for

This policy applies to all directors, employees, contractors, and tutors who provide, support, or operate the Sherpa platform. Users of the platform – students, parents, and adult learners – are not subject to this policy but benefit from the protections it puts in place, and can rely on it when raising concerns.

5. Recognising harm

Anyone working on or for Sherpa should be able to recognise the main forms of abuse and harm that may surface on or through the platform. The categories below are not exhaustive and are not intended as a clinical or legal definition; they are a working summary to help people identify when something needs to be reported.

Physical, emotional, and sexual abuse, and neglect

These are the recognised categories of child abuse. For Sherpa, the most likely surfaces for any indicator are: what a student says or does during a session, what appears in a session recording or transcript, and what a tutor or other user reports having observed.

Online grooming and exploitation

Behaviour by a user (most likely a tutor, but potentially another adult connected to the student) intended to build inappropriate trust with a child, normalise inappropriate contact, sexualise the relationship, or move communication off-platform. Sherpa's transcript screening is specifically designed to detect early indicators of this.

Child-on-child abuse

Less common in a one-to-one tutoring context, but can include disclosure of bullying, sexual harassment, or coercive behaviour by peers outside the session.

Self-harm and mental health concerns

A student may disclose, or show indicators of, suicidal ideation, self-harm, an eating disorder, or other mental health distress. This is treated as a safeguarding concern.

Radicalisation

Indicators that a child or adult is being drawn into extremism. The Prevent duty does not apply to Sherpa as a private online service, but we treat radicalisation concerns as safeguarding matters and refer them where appropriate.

Harm to adults at risk

Sherpa is used by adult learners as well as children. Where an adult user appears to have care or support needs and is experiencing, or at risk of, abuse or neglect, this is handled by the safeguarding team on the same reporting routes as concerns relating to a child.

6. Tutor verification

Before a tutor can offer lessons on the platform they complete identity verification. This is a meaningful check designed for an online marketplace; it is not equivalent to, and does not claim to be equivalent to, the safer recruitment regime operated by schools.

DBS checks

Sherpa is not a regulated activity provider under the Safeguarding Vulnerable Groups Act 2006. There is no statutory requirement for tutors providing online-only tuition through a marketplace to hold an Enhanced DBS check.

Tutors may, at their own option, obtain an Enhanced DBS check (with Children's Barred List information where applicable) and upload it to their profile. Sherpa verifies any uploaded certificate and, where the check is valid and within date, displays a DBS-verified badge on the tutor's profile.

Parents and students can filter tutor search results to show only DBS-verified tutors. Sherpa does not require parents to choose a DBS-verified tutor and does not treat the absence of a DBS check as a safeguarding risk in itself, given the platform's structural controls (recording, transcript screening, off-platform prohibition).

This is an area we keep under review as policy and guidance develop.

Referral duty under SVGA 2006

If Sherpa removes a tutor from the platform because they have harmed a child or adult at risk, or because they pose a risk of harm, we will make a referral to the Disclosure and Barring Service under section 35 of the Safeguarding Vulnerable Groups Act 2006. This duty applies to us as a service that arranges work bringing adults into contact with children, even though the work itself is not regulated activity.

7. Reporting a concern

How to report

Anyone – a parent, student, tutor, employee, or member of the public – can raise a safeguarding concern with Sherpa using the reporting form linked here, or by contacting us through the support channels published on our website.

Reports should describe what has happened or been observed, when, who was involved, and any session ID or message thread that the safeguarding team can use to locate the relevant material. Reports do not need to use particular language and do not need to be made by the person directly affected.

If someone is at immediate risk

If a child or adult appears to be at immediate risk of harm – for example, a disclosure of imminent self-harm, or a serious incident unfolding live in a session – the most important action is to ensure the police or emergency services are contacted. Anyone can call 999. The Sherpa safeguarding team should be informed in parallel, but contacting the emergency services should not be delayed for any internal process.

What we do with reports

All safeguarding reports are logged and reviewed by the DSL or Deputy DSL. Depending on the nature of the report, we will:

- Review the relevant session recording, transcript, and message history.
- Take any immediate platform action required (for example, suspending a tutor account pending review).
- Where the concern relates to abuse, neglect, or risk of harm to a child or adult at risk, make a referral to the relevant statutory authority. Because we do not hold the student's address, we will identify the correct local authority using information given by the person making the report, the parent or account holder's billing postcode (obtained from Stripe), and where necessary direct enquiry with the parent or account holder.
- Make a referral to the police where a criminal offence may have been committed, or where the police are best placed to act.
- Make a referral to the DBS where a tutor has been removed in circumstances triggering section 35 of the SVGA 2006.
- Make a referral to the Teaching Regulation Agency where a tutor is, or was, a qualified teacher and the conduct meets the TRA's referral threshold.
- Keep the person who raised the concern informed to the extent appropriate, recognising that confidentiality and the integrity of any external investigation may limit what we can share.

Confidentiality

Safeguarding reports are handled on a need-to-know basis. We do not promise absolute confidentiality: if a referral to a statutory authority is required, we will make it. We will explain that to the person raising the concern wherever practical.

8. Allegations against tutors, employees, or directors

Where a safeguarding concern relates to the behaviour of a tutor, employee, or director of Sherpa, the DSL will:

- Review the available evidence, including session recordings, transcripts, and messaging records.
- Consider whether immediate precautionary action is needed on the platform – typically suspending the individual's account pending review.
- Refer the matter to the police if a criminal offence may have been committed.
- Refer to the DBS under SVGA 2006 s.35 if the threshold is met.
- Refer to the TRA where the individual is or was a registered teacher and the conduct meets the TRA's threshold.

Where the allegation is made against the DSL, it should be raised with any other director of Application Labs Limited, who will appoint a different senior person to discharge the DSL role for the purpose of handling the allegation.

LADO referral is not generally a route open to Sherpa in the way it is to schools and regulated providers. The LADO framework is designed for organisations whose staff work directly with children in regulated settings. Where relevant – for example where a tutor is also employed by a school – we will share information with the LADO at the request of the relevant local authority.

9. Online safety on the platform

Sherpa is an online user-to-user service used by children. As such we have duties under the Online Safety Act 2023 to protect users, and particularly children, from illegal content and from content harmful to children.

Our approach to online safety is built into the platform:

- Session video and audio are recorded. Recordings are retained securely and are reviewable.
- Audio transcripts are automatically screened for indicators of grooming, sexual content, threatening language, and attempts to move contact off-platform. Flagged content is reviewed by the safeguarding team.
- In-platform messaging is subject to the same Terms of Use as sessions. Users can report messages; reports are reviewed by the safeguarding team.

- Off-platform contact between tutors and students is prohibited by our Terms. Detected attempts are acted on.
- We carry out a children's risk assessment in line with the Online Safety Act and the relevant Ofcom codes of practice, and review it as our service changes.

Online safety risks change quickly. The DSL keeps the platform's controls under review and reports to the Board on material changes in risk or in the regulatory framework.

10. Training

Safeguarding training at Sherpa is proportionate to role:

- The DSL and Deputy DSL complete formal safeguarding lead training and refresh it every two years.
- All engagement team members and contractors complete a Sherpa safeguarding induction covering: how to recognise the main forms of harm; how to report a concern; the reporting routes inside Sherpa; and the obligations under this policy. This is refreshed annually.
- Tutors are required to acknowledge our safeguarding-relevant Terms and Code of Conduct at onboarding and are pointed to plain-language guidance on what to do if a concern arises during a lesson. We do not require tutors to complete the same level of training as employees, in recognition of their status as independent contractors using the platform.

Training records are maintained by the DSL.

11. Governance

The Board

The Board of Application Labs Limited has ultimate responsibility for safeguarding at Sherpa.

The Board:

- Approves this policy and any material changes to it.
- Ensures the DSL and Deputy DSL have the resource, authority, and access to do the role.
- Receives a safeguarding update at each board meeting covering reports raised, referrals made, and any material risks or changes in regulation.

The Designated Safeguarding Lead

The DSL is the named lead for safeguarding at Sherpa. The DSL:

- Is the first point of contact for any safeguarding concern.

- Decides on referrals to external authorities.
- Maintains records of all concerns and their handling.
- Reports to the Board.
- Keeps this policy and the underlying procedures under review.

The Deputy DSL deputises for the DSL when the DSL is unavailable and supports day-to-day safeguarding work.

Current postholders are listed on the platform's safeguarding page so that the policy itself does not need re-issuing when postholders change. The contact route for any concern is safeguarding@sherpa-online.com.

12. Records and data protection

Safeguarding records are held by Sherpa in line with our Privacy Policy and our retention schedule. The lawful bases for processing safeguarding information are legitimate interests and, where relevant, legal obligation and the safeguarding condition for special category data set out in the Data Protection Act 2018 and UK GDPR.

Records are retained for as long as is necessary to discharge our safeguarding obligations, support any external investigation, and meet our duties under the Online Safety Act, and are then deleted.

13. Whistleblowing

Anyone working for or with Sherpa who has concerns about safeguarding practice – including concerns about how a particular matter is being handled – should raise them with the DSL or any director. Where someone does not feel able to raise concerns internally, external routes are available, including the NSPCC helpline (0808 800 5000) and, for matters concerning a regulated activity, the Disclosure and Barring Service. Sherpa supports anyone raising a safeguarding concern in good faith.

14. Legal and regulatory framework

This policy is built around the framework that applies to Sherpa as an online tutoring marketplace:

- **Online Safety Act 2023** – duties on user-to-user services to protect users (and children in particular) from illegal content and from content harmful to children, supported by Ofcom codes of practice.
- **Safeguarding Vulnerable Groups Act 2006, section 35** – duty to refer to the DBS where a person has been removed for relevant conduct, including in services that arrange work bringing adults into contact with children.
- **Data Protection Act 2018 and UK GDPR** – lawful processing of personal data, including special category data, in a safeguarding context.
- **Age Appropriate Design Code (Children's Code)** – issued under section 125 of the Data Protection Act 2018, governing online services likely to be accessed by children.
- **Duty of care in tort** – the general common law duty to take reasonable care to avoid foreseeable harm to users of our service.
- **Equality Act 2010** – duties in relation to protected characteristics in how we deliver the service and respond to safeguarding matters.

Sherpa is not a school, college, registered childcare provider, or regulated activity provider. Statutory guidance written for those settings – including Keeping Children Safe in Education and Working Together to Safeguard Children – does not apply to Sherpa as a matter of law. Where principles from that guidance are useful and proportionate, we adopt them; where they presume an in-person setting, a school workforce, or a delegated statutory function, they are not relevant to our service.

15. Review

This policy is reviewed at least annually by the DSL, and approved by the Board. It is also reviewed whenever:

- There is a material change to UK law or relevant regulatory guidance.
- There is a material change to Sherpa's operating model or platform.
- A safeguarding incident or external advice indicates a change is needed.

Material changes are recorded in the version history maintained alongside this policy.