



Safeguarding Assurance Note

Clarity for Education

Version 2.0

Reviewed: 11 July 2026

Current external assurance note



Document control	Detail
Version	2.0
Technical evidence reviewed	11 July 2026
Publication status	Current external assurance note
Review trigger	A material change to Safeguard, data handling or statutory guidance, and at least annually

Purpose

This note explains the boundary between Student Radar's technology and a school's safeguarding responsibilities. It gives procurement teams, Designated Safeguarding Leads and Data Protection Officers a concise description of the safeguards currently represented in the product and public documentation.

Student Radar is a technology provider. It does not replace the professional judgement, statutory role or local procedures of the DSL, headteacher, governing body, local authority, police or children's social care. The school remains the data controller and decision-maker for safeguarding matters.

Product scope

Safeguard is an optional Student Radar package and requires Core. Core includes the SEND and Lead capabilities. The current public catalogue describes Safeguard as providing:

- concern logging and triage;
- a DSL Action Board;
- case chronology and history; and
- role-based access and audit.

These functions support recording, coordination and oversight. They do not determine whether a referral should be made, establish that abuse has occurred, or replace the school's safeguarding policy and escalation route.

Responsibility and human decision-making

Schools are responsible for:

- deciding who may access Safeguard and assigning roles appropriately;
- reviewing records, concerns and actions for accuracy and completeness;
- making and documenting safeguarding decisions;
- making referrals and notifications required by law, guidance or local procedure;
- setting the lawful basis and retention instructions for safeguarding records; and
- training authorised users in the school's safeguarding and information-governance procedures.

Student Radar's role is to provide the configured service, apply the documented technical controls and process school data on the school's instructions under the executed agreement and Data Processing Agreement.



Access and data protection safeguards

Current published controls include:

- a UK-hosted primary database in Supabase's London region;
- AES-256 encryption at rest and TLS 1.2 or higher in transit;
- mandatory AAL2 multi-factor authentication for staff accounts;
- role-based permissions and database row-level security; and
- audit-oriented product functionality for the Safeguard package.

Access must remain need-to-know. The presence of a technical role does not itself make access appropriate; the school must configure and review access in line with its own responsibilities.

AI and public-tool boundary

Student Radar does not present an AI output as a safeguarding decision. AI-assisted capabilities in the authenticated platform are optional, school-enabled and advisory. A member of staff must review any output before using it. The exact input fields, purpose, retention and safeguards for a school-enabled capability must be documented before enablement.

The free public Echo and Sensory Profiler tools are not safeguarding reporting channels:

- Echo accepts a bounded AAC phrase. Visitors should not enter names, contact details, safeguarding narratives or other identifying information.
- Sensory Profiler generation accepts anonymous catalogue selections and rejects pupil identity, school, SEND status, year group, settings and free text.

Public Responses API calls use `store=false`, but Student Radar does not claim blanket Zero Data Retention. Provider abuse-monitoring logs may be retained for up to 30 days unless approved retention controls apply.

No public tool should be used to investigate a concern, determine risk, draft a referral or store an official safeguarding record.

Retention and record ownership

The school determines the retention period for safeguarding records and must align it with current statutory guidance, local policy and any active investigation or legal hold. The current public service position is deletion within 30 days after the subscription ends unless the school instructs otherwise, with encrypted backups normally retained for disaster recovery for up to 90 days. A longer backup period must be required by law or the school's documented instruction.

Before relying on Student Radar as the primary safeguarding record, the school should ensure that its required retention period, export arrangements and termination instructions are expressly covered by the executed agreement. This note does not promise an age-based retention configuration or replace the school's records-retention schedule.

Security incidents and safeguarding data

Student Radar maintains a documented incident response process. A confirmed or suspected compromise involving school data is assessed, contained and investigated. Where a personal data breach affects data processed for a school, Student Radar will notify the school without undue delay and provide available information to support the school's assessment.



The school remains responsible for safeguarding referrals and for deciding whether the ICO or affected individuals must be notified in its capacity as controller. Student Radar will provide reasonable assistance in accordance with the executed Data Processing Agreement.

Assurance status and contact

This is an external assurance note, not a safeguarding policy, legal opinion or substitute for capability-specific due diligence. Contractual data-protection documents and any school-specific configuration remain controlling.

Questions should be sent to dpo@studentradar.com. Do not include pupil details or safeguarding case content in an initial email; request a secure route if case-specific information must be exchanged.