# Information Security and Controls Summary

## Clarity for Education

Version 2.0

Reviewed: 11 July 2026

**Current external assurance summary**

| Document control | Detail |
|---|---|
| Version | 2.0 |
| Technical evidence reviewed | 11 July 2026 |
| Publication status | Current external assurance summary |
| Review trigger | A material change to architecture, processors or controls, and at least annually |

## Purpose and status

This document gives schools and trusts a buyer-safe summary of the security controls currently described and evidenced for Student Radar. It is an external assurance summary, not an internal security policy, penetration-test report or contractual schedule. The executed agreement, Data Processing Agreement and Order Form govern the service supplied to a customer.

The school or trust remains the data controller for the pupil and staff data it places in Student Radar. SENDlink LTD, trading as Student Radar, acts as processor for that data. For enquiries, public-site telemetry and inputs a visitor chooses to submit to a public tool, SENDlink LTD may act as controller as described in the current website Privacy Policy.

## Hosting and data location

- The primary Student Radar database, authentication service and file storage use a Supabase project configured in eu-west-2 (London).
- Vercel provides application hosting, server-side functions and edge delivery. Request and response data can be processed transiently by that hosting layer; this summary does not claim that all execution stays in one location.
- Wonde is the supported MIS integration route for participating schools.
- Upstash provides shared public-API rate limiting in a London region. Student Radar sends a policy-specific HMAC-pseudonymised client identifier and request count, not the raw IP address or form fields.
- Optional or user-triggered services can involve other locations. The current Sub-Processor List describes those providers and transfer boundaries.

## Data protection controls

Current published controls include:

- AES-256 encryption for data at rest in the primary data platform;
- TLS 1.2 or higher for data in transit;
- role-based access control and database row-level security to restrict records to authorised users and tenants;
- mandatory multi-factor authentication at AAL2 for staff accounts accessing the authenticated platform;
- server-side handling of privileged database credentials rather than exposing an administrative credential to the browser;
- validation, field limits and request-size limits on public JSON APIs;
- same-origin checks before public API requests reach persistence or external providers;
- shared rate limits for public APIs using HMAC-pseudonymised identifiers; and

- production web security headers including Content Security Policy, frame restrictions, content-type protection, a restricted permissions policy and a strict referrer policy.

The public rate limiter is configured so expensive AI and PDF operations fail closed when the shared limiter is unavailable. Lower-cost lead and directory routes can operate in a logged degraded mode. This is an availability trade-off; it does not remove validation or same-origin checks.

## Security governance and delivery controls

Student Radar holds a current UK Cyber Essentials certificate. This is evidence of the Cyber Essentials control baseline; it is not presented as Cyber Essentials Plus, ISO 27001 or an independent certification of every application control.

The public-site delivery pipeline runs linting, type checks, unit tests, coverage, production builds, browser tests, dependency auditing and Lighthouse budgets. High and critical production dependency findings are blocking. These checks provide evidence for the public site and its APIs; they do not by themselves certify the separate authenticated platform or replace a penetration test.

We do not make an unsupported promise of continuous security-operations-centre monitoring, a fixed secret-rotation interval, an annual independent penetration test or a particular incident response time in this summary. Where a buyer needs such a commitment, it must be supported by current evidence and stated in the executed agreement.

## AI processing boundaries

AI-assisted capabilities inside the subscribed platform are optional and enabled by the school. Those flows tokenise or remove personally identifiable information where the relevant technical control is implemented. Outputs remain advisory and require staff review; Student Radar does not make solely automated pupil decisions under Article 22 of the UK GDPR.

The free public tools are separate:

- Echo sends the visitor's bounded tapped phrase and button text to Student Radar and OpenAI for interpretation, then sends the generated short utterance to OpenAI's speech endpoint.
- Sensory Profiler generation accepts anonymous catalogue selections only. Its API rejects pupil identity, school, SEND status, year group, settings and free text. PDF rendering accepts the anonymous selections and unchanged validated generated content only when a short-lived server signature is valid.

Responses API requests set `store=false`. That prevents Responses application-state storage for those calls; it is not the same as Zero Data Retention. OpenAI may retain abuse-monitoring logs containing customer content for up to 30 days unless approved retention controls apply. This summary therefore makes no blanket Zero Data Retention or universal tokenisation claim.

## Retention, resilience and incidents

The school controls the retention period for its pupil and staff data. The current published position is that data is retained while the subscription is active and for up to 30 days after termination unless the school instructs otherwise. Encrypted disaster-recovery backups are normally retained for up to 90 days; a longer period must be required by law or the school's documented instruction.

Student Radar maintains a documented incident response process. If 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 and notifications.

## Supplier evidence and contact

Current supporting evidence includes the Cyber Essentials certificate, Sub-Processor List, AI Processing and Transfer Overview, Privacy Notice, Business Continuity and Resilience Summary, and Incident Response and Breach Notification Summary.

Security and data-protection questions should be sent to dpo@studentradar.com. Do not include pupil records, safeguarding narratives, credentials or other confidential case data in an initial enquiry.