Business Continuity and Resilience 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 architecture change, major incident or supplier change, and at least annually

Purpose and scope

This external summary explains the published continuity and resilience position for Student Radar without disclosing internal response procedures. It replaces documents labelled internal or confidential for public procurement use.

The summary is informational. It does not create an uptime warranty, service credit, recovery time objective or recovery point objective. Any customer-specific service commitment must appear in the executed Order Form or agreement.

Service architecture

Student Radar uses managed cloud services rather than school-hosted infrastructure:

- Supabase provides the primary database, authentication and storage in eu-west-2 (London).
- Vercel provides application hosting, server-side functions and edge delivery.
- Wonde is the supported MIS integration for participating schools.
- Upstash provides shared public-API rate limiting in a London region.
- Resend, Twilio, Sentry and school-enabled OpenAI capabilities are conditional services. OpenAI is also used when a visitor actively requests processing through the public Echo or Sensory Profiler tools.

The current Sub-Processor List describes the purpose and processing boundary for each provider. A provider outage can affect the function that depends on it. This summary does not claim that every feature will continue unchanged during a third-party failure.

Continuity approach

The continuity approach is based on four priorities:

1. **Protect people and data.** Restrict further access or change where a security or data-integrity risk is suspected.
2. **Understand the affected scope.** Separate a local feature failure from a wider service, provider or data incident.
3. **Restore a safe service.** Recover only after the cause and integrity risks are understood sufficiently to avoid making the incident worse.
4. **Communicate proportionately.** Give affected customer contacts accurate information as it becomes available and distinguish confirmed facts from estimates.

Detailed technical runbooks, credentials, recovery paths and escalation contacts remain internal.

Data protection and recovery

The current published position is:

- primary school data is held in the configured London database region;
- data is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher;
- the school controls its retention instructions;
- pupil and staff data is retained while the subscription is active and for up to 30 days after termination unless the school instructs otherwise; and
- encrypted backups used for disaster recovery are normally retained for up to 90 days; a longer period must be required by law or the school's documented instruction.

Backup retention is not the same as a guaranteed recovery point. This summary therefore does not state that a particular point-in-time recovery interval, geographic failover pattern or restore time has been independently verified. Buyers requiring fixed recovery objectives should agree them contractually against current operational evidence.

Change and dependency risk

The public website and its APIs use automated delivery gates covering linting, type checking, unit tests, coverage, production builds, browser journeys, production dependency auditing and Lighthouse budgets. High and critical production dependency findings are blocking for that codebase.

Those checks reduce change risk for the public site. They do not, by themselves, prove the continuity of every authenticated platform capability. Capability-specific evidence should be reviewed for the service being procured.

Where a public API depends on the shared rate limiter, higher-cost AI and PDF operations fail closed if the limiter is unavailable. Lead and directory routes may enter a logged degraded mode. Provider-dependent public tools return controlled errors or, where designed and validated, curated fallback output.

Incident coordination and customer communication

Student Radar maintains a documented incident response process. Depending on the event, actions may include validation, containment, credential or configuration changes, provider escalation, safe restoration and post-incident review.

If a personal data breach affects school data, Student Radar will notify the school without undue delay and provide available information to support the school's assessment. For other material service incidents, communications are directed to the nominated customer contact and updated as reliable information becomes available.

No fixed update interval or resolution time is promised by this summary. The executed agreement governs any such commitment.

Customer continuity responsibilities

Schools and trusts should:

- keep operational, technical and data-protection contacts current;
- define which Student Radar workflows are business-critical;
- maintain appropriate local procedures for periods when a digital service is unavailable;

- confirm record-retention and export requirements before termination; and
- report incidents without including unnecessary pupil or confidential case data in an initial email.

Contact and assurance status

Continuity, security and data-protection questions should be sent to dpo@studentradar.com. The current Cyber Essentials certificate, Sub-Processor List, Privacy Notice and Incident Response and Breach Notification Summary provide related assurance.

This summary does not disclose internal recovery instructions and does not vary the executed service agreement.