Incident Response and Breach Notification 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 process change, major incident or legal change, and at least annually

Purpose and scope

This document gives schools and trusts an external summary of how Student Radar handles suspected security incidents and personal data breaches. It replaces an internal or confidential operational policy for public procurement use.

Detailed detection rules, credentials, technical runbooks, provider contacts and evidence-handling instructions remain internal. This summary does not create a service level, fixed response time or legal conclusion about a particular event.

Roles

For pupil and staff data processed through the subscribed platform:

- the school or trust is normally the data controller;
- SENDlink LTD, trading as Student Radar, acts as processor; and
- Student Radar provides information and reasonable assistance so the controller can meet its obligations under the executed Data Processing Agreement.

For personal data that Student Radar controls directly, such as appropriate enquiry and operational data, Student Radar assesses and performs its own controller obligations.

The school remains responsible for safeguarding decisions and referrals. A security incident process does not replace the school's DSL, local-authority, police or children's social-care procedures.

Response lifecycle

Student Radar's incident process follows these stages, adjusted to the event:

1. **Receive and validate.** Record the report, distinguish an availability issue, security event and potential personal data breach, and identify the affected service and customer scope.
2. **Triage and contain.** Limit further unauthorised access, disclosure, alteration or loss while preserving information needed to understand the event.
3. **Assess.** Establish what happened, which data and people may be affected, the likely consequences, and whether a supplier or other party is involved.
4. **Recover safely.** Remove or mitigate the cause, restore affected functions when it is safe to do so, and continue monitoring for recurrence.
5. **Notify and support.** Notify affected controllers without undue delay where a personal data breach affects data processed for them, and provide reliable information as it becomes available.
6. **Review.** Record lessons, corrective actions and any required change to controls, documentation or supplier management.

An initial assessment may change as further evidence becomes available. Updates distinguish confirmed facts from working assumptions.

Notification to a school or trust

If Student Radar becomes aware of a personal data breach affecting data processed for a school or trust, it will notify the controller without undue delay. The notification will include, so far as the information is then available:

- the nature and known scope of the breach;
- the categories of data and people affected;
- likely consequences or risks identified;
- containment and mitigation steps taken or proposed; and
- a contact for follow-up.

Missing information should not delay an appropriate initial notification. Further details can follow as the investigation develops.

The school or trust decides whether it must notify the Information Commissioner's Office under Article 33 of the UK GDPR and whether affected people must be told under Article 34. Student Radar will provide reasonable assistance and relevant available information. Where the reporting threshold is met, the controller must report without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. That legal notification window is not a promise that every technical investigation will be complete within 72 hours.

Where Student Radar is controller for the affected data, it assesses notification to the ICO and individuals directly in accordance with applicable law.

Safeguarding and sensitive data

Safeguarding, health and SEND records can create a higher risk if compromised. Incident handling therefore applies need-to-know access and data minimisation. The school retains authority over safeguarding actions and referrals. Student Radar supplies technical facts and processor assistance; it does not make the school's safeguarding decision.

Do not send pupil records, credentials or safeguarding narratives through an unsecured initial report. Ask for a secure transfer route if evidence containing sensitive data is required.

Supplier and AI-related incidents

Where a service provider is involved, Student Radar coordinates the technical investigation and contractual notification path while remaining accountable for its processor obligations to the school.

The public Echo and Sensory Profiler tools use OpenAI only when a visitor requests processing. Responses calls set `store=false`; this is not a blanket Zero Data Retention claim, and provider abuse-monitoring logs may be retained for up to 30 days unless approved controls apply. A suspected disclosure through a public or school-enabled AI flow is assessed against the actual data submitted, provider path and configured retention controls.

After an incident

After containment and recovery, Student Radar records the outcome and tracks proportionate corrective actions. Depending on the event, that can include code or configuration changes, access changes, supplier follow-up, documentation updates and additional verification.

A customer-facing summary can be supplied where appropriate and lawful. It will avoid disclosing information that would weaken security, prejudice an investigation, expose another customer or reveal personal data unnecessarily.

Reporting and document status

Report security and data-protection concerns to dpo@studentradar.com. State the affected service, approximate time and observable symptoms. Do not include passwords, API keys, pupil data or confidential case details in the first message.

This is an external assurance summary. The executed Data Processing Agreement and service agreement govern notification duties, assistance and any contractual timescales.