



Data Protection Impact Assessment

Clarity for Education

Version 1.1

Current supplier template for due diligence. It is not a completed or approved DPIA until the controller completes the school-specific sections, consults its DPO or Data Protection Lead, records any additional measures and signs the outcome.



Supplier information and school/controller completion template

Document control	Detail
Supplier	SENDlink LTD, trading as Student Radar
Company number	16602655
Supplier contact	dpo@studentradar.com
Version	1.1
Supplier technical review date	11 July 2026
Next supplier review	On a material processing change, and no later than 11 July 2027
Status	Current supplier template for due diligence. It is not a completed or approved DPIA until the controller completes the school-specific sections, consults its DPO or Data Protection Lead, records any additional measures and signs the outcome.

How to use this document

The subscribing school or trust is normally the controller for pupil, parent/carer and school-staff data in the authenticated Student Radar platform. SENDlink LTD is the processor. The controller remains responsible for deciding whether a DPIA is required, completing it before high-risk processing begins, consulting affected people where appropriate, and keeping the assessment under review.

Student Radar has supplied the verified service facts and a structured risk template. The controller must not treat an uncompleted supplier template as its legal approval. A processor may assist with a DPIA, but the controller remains accountable for it.

This assessment deliberately separates:

- the authenticated school platform, where the school determines the purpose and enables capabilities; and
- public Student Radar tools, where SENDlink LTD is the controller for a visitor's direct use.

The public tools are not required to use the subscribed platform. If a school directs pupils or staff to use a public tool as part of its own process, the school should include that local use, any resulting printed or downloaded records, and any additional context it combines with the output in its DPIA.

Part A - controller details and screening

A1. Controller and project

Field	Controller to complete
School or trust legal name	
Schools covered	



Field	Controller to complete
Project owner	
DPO / Data Protection Lead	
Assessment date	
Planned go-live date	
Student Radar packages/capabilities enabled	
Wonde connection fields authorised	
Optional communications enabled (email/SMS)	
Any school-enabled platform AI capability	
Public Echo or Sensory Profiler included in the school's process?	
Number and age range of pupils affected	
Staff and parent/carers groups affected	
Review date and trigger	

A2. Why a DPIA is appropriate

Student Radar may process information about children, including health, SEND and safeguarding records, on an ongoing basis. Depending on the controller's scale and configuration, the processing may include special category data, criminal offence information, data matching through an MIS connection, information about vulnerable individuals, and technology used to prioritise or present risk-related information.

These factors warrant a DPIA as a matter of good practice and may make it mandatory. The controller must record its own screening decision rather than relying on a pupil-number threshold invented by the supplier.

Controller screening decision:

[Explain which UK GDPR Article 35 and ICO risk indicators apply. If the controller concludes that a DPIA is not required, record the reasons and obtain DPO/Data Protection Lead advice.]

Part B - verified supplier description

B1. Roles and processing contexts

Context	Controller	Processor / recipient	Trigger
Authenticated Student Radar platform	School or trust	SENDlink LTD and the authorised sub-processors for enabled services	The school enters data, authorises Wonde fields or enables a capability
Website enquiries, demo requests and Pathfinder applications	SENDlink LTD	Supabase for storage; other providers only where needed to deliver the requested response	A visitor submits a form
Public Echo interpretation and speech	SENDlink LTD	Vercel hosting and OpenAI API	A visitor selects Interpret



Context	Controller	Processor / recipient	Trigger
Public Sensory Profiler generation	SENDlink LTD	Vercel hosting and OpenAI API	A visitor selects Generate after choosing catalogue entries
Public Sensory Profiler PDF rendering	SENDlink LTD	Vercel hosting; rendering is local to the Student Radar route and does not call OpenAI	A visitor requests a PDF using an unexpired signed generated result
Public API abuse prevention	SENDlink LTD	Upstash	A request reaches a rate-limited public route
Marketing measurement	SENDlink LTD	Vercel Web Analytics and Speed Insights	Production page view or an approved non-personal interaction event

B2. Authenticated platform data

The exact data depends on the controller's selected capabilities and Wonde authorisation. It may include:

- pupil identifiers and demographic information;
- attendance, behaviour and assessment information;
- SEND status, support plans, provision and outcome information;
- health, allergy, dietary, medication or disability information;
- safeguarding flags, concerns and authorised case material;
- parent/carer contact details where a selected workflow requires them; and
- staff identity, role, access and audit information.

The school must complete a field-level data map for its configuration. It must not assume that every field available through an MIS is necessary.

B3. Authenticated platform flow

1. The school authorises its Wonde connection and/or authorised staff enter information directly.
2. Student Radar stores and presents the data for the capabilities selected by the school.
3. Authorised school users access information according to their assigned role and permissions.
4. Optional providers are used only for the related enabled function.
5. Customer Data is retained for the subscription and is deleted or returned in accordance with the controller's instructions and the executed Data Processing Agreement.

The current published platform control set includes encryption in transit and at rest, role-based access control, database row-level security and multi-factor authentication for staff accounts. The controller remains responsible for assigning the least privilege necessary, removing leavers promptly and reviewing school-user access.

B4. Public Echo flow

1. The visitor taps AAC buttons and actively chooses Interpret.
2. The request contains the bounded phrase and ordered button labels or vocalisations. Echo does not ask for a name and warns the visitor not to include identifying details.
3. The Student Radar server validates the request, applies body-size and rate limits, and sends a purpose-limited prompt to the OpenAI Responses API with `store:false`.
4. The generated short utterance is sent to OpenAI's audio speech endpoint.
5. The interpreted text and generated audio may be cached in volatile process memory for up to 10 minutes, keyed by a SHA-256 digest of the request. The route does not write them to the Student Radar database.



The fields remain user controlled. Student Radar therefore does not make a blanket claim that every Echo submission is anonymous or tokenised. A school must not use public Echo to submit pupil names, safeguarding narratives, medical details or other identifiable case information.

B5. Public Sensory Profiler flow

1. The visitor chooses generic sensory domains, patterns and behaviour catalogue entries. The browser stores those selections in session storage so the output page can read them.
2. The generation API accepts only those catalogue selections. Its strict schema rejects pupil identity, school, SEND status, year group, settings, self-advocacy and free text.
3. The server sends a purpose-limited prompt to the OpenAI Responses API with `store:false`, validates the result and uses curated fallback content if necessary.
4. Validated generated output may be cached in volatile process memory for up to 10 minutes. The server issues a separate HMAC-SHA256 signature over the generated profile content that expires after 10 minutes.
5. PDF rendering receives the anonymous selections, unchanged validated generated content and signature. It rejects unsigned, expired, modified or client-authored profile text and does not call OpenAI.
6. If the visitor requests PDF access, an email address and optional role are stored in an enquiry record. The sensory selections and generated profile are not stored with that record.

The output is advisory and not a diagnosis or professional assessment. The tool does not create a persistent Student Radar pupil profile. If a school prints, downloads or attaches the output to an identifiable pupil record, that later action is the school's processing and must be assessed and retained under the school's policy.

B6. Provider and transfer position

The current technical register is the Student Radar Sub-Processor List, version 1.5, reviewed 11 July 2026. Its current categories are:

Provider	Current use
Supabase	Core database, authentication, file storage and backups; primary project configured in eu-west-2 (London)
Vercel	Application hosting, server-side functions, static assets and edge delivery; no blanket single-location claim is made
Wonde	Read-only MIS integration for participating schools
Upstash	Shared public-API rate limiting; receives a policy-specific HMAC-SHA256 IP token and request count, not the raw IP or form fields; configured London region with no global read replicas
Resend	Conditional transactional email
Twilio	Conditional SMS delivery
OpenAI	User-triggered public Echo and Sensory generation, and separately any school-enabled platform capability described in a current capability notice
Sentry	Conditional error and performance monitoring where configured



OpenAI public Responses calls use store:false, but Student Radar does not claim that its current OpenAI account has Zero Data Retention. Default provider abuse-monitoring logs may contain request or response content and may be retained for up to 30 days. The public implementation calls the general OpenAI API domain and does not claim UK-only processing. The controller must review the current contractual transfer safeguards for any school-enabled capability before enabling it.

B7. Retention position

- Live Customer Data: subscription term plus up to 30 days after termination, unless the controller gives a different documented instruction or a legal hold applies.
- Backups containing Customer Data: up to 90 days to age out after termination.
- Public Echo and Sensory server cache: up to 10 minutes in volatile process memory.
- Sensory PDF signature: 10 minutes.
- OpenAI public-tool abuse-monitoring logs: up to 30 days by default; store:false is not ZDR.
- Rate-limit counters: expire a little over two minutes after the one-minute policy window.
- Public lead records: handled under the current Student Radar Data Retention and Deletion Schedule and not treated as marketing consent.
- Browser storage: described in the Cookie, Client Storage and Telemetry Notice.

Part C - controller necessity and proportionality assessment

The controller must complete each item before approval.

C1. Purpose

[Describe the educational, inclusion, safeguarding or operational outcomes the school is trying to achieve. Identify the exact enabled capabilities. Avoid generic statements such as "better insights" without a defined use.]

C2. Lawful basis and special-category conditions

[Record the controller's Article 6 basis; each relevant Article 9 condition; Article 10 authority; DPA 2018 Schedule 1 condition; and whether the controller must maintain an Appropriate Policy Document. Do not copy a supplier condition without confirming it fits the school's purpose.]

C3. Necessity and alternatives

[Explain why each data category and capability is necessary. Record less intrusive options considered, including limiting Wonde fields, using fewer packages, keeping an optional provider disabled, shortening retention or using non-identifying public-tool inputs.]

C4. Data minimisation decisions

Decision	Controller answer
Wonde fields authorised and why	
Staff roles allowed to view SEND data	
Staff roles allowed to view safeguarding data	
Export permissions	
Parent/carers data required	



Decision	Controller answer
Optional email/SMS enabled and why	
Platform AI enabled? Link to current capability assessment	
Public tools used in a school process? Safeguards	

C5. Consultation

[Record consultation with the DPO/Data Protection Lead, safeguarding lead, SENCo, information-security owner, staff representatives and, where appropriate, pupils and parents/carers or their representatives. Explain if consultation was not appropriate or possible.]

C6. Transparency

[Identify the school privacy notices, age-appropriate pupil information, staff guidance and any just-in-time notice that must be updated before go-live.]

C7. Rights and complaints

[Describe how the school will handle access, correction, restriction, objection and erasure requests; how Student Radar assistance will be requested; and how third-party or safeguarding information will be reviewed before disclosure.]

Part D - risk assessment

The inherent risk descriptions below are starting points, not supplier-certified scores. The controller must use its own likelihood and severity method, record additional local controls and decide the residual risk.

Risk	People and potential harm	Verified supplier measures	Required controller measures	Residual decision
Unauthorised access or cross-school disclosure	Pupils, families and staff could experience distress, stigma, discrimination or safeguarding harm	Current published controls include encryption, role-based access, row-level security and staff-account MFA	Apply least privilege; restrict safeguarding roles; remove leavers promptly; review access and exports; secure managed devices	[Rate and justify]
Excessive MIS collection	Unnecessary sensitive fields increase impact and reduce transparency	Wonde is the only claimed direct MIS integration; school authorises the connection	Approve a field-level map; disable unnecessary fields and capabilities; review after implementation	[Rate and justify]
Inaccurate or stale data	Incorrect decisions, missed support or unfair treatment	Data can be sourced from the school MIS and updated by authorised users; public output is described as advisory	Define the authoritative source, correction workflow and review frequency; require staff to verify before action	[Rate and justify]
Safeguarding or criminal-offence information disclosed through export or communication	Serious welfare, confidentiality and legal harm	Platform access controls; public forms prohibit sensitive case information	Restrict exports and recipients; train users; use secure channels; review third-party information before disclosure	[Rate and justify]



Risk	People and potential harm	Verified supplier measures	Required controller measures	Residual decision
Optional provider or international transfer used without assessment	Loss of control, unexpected jurisdiction or longer provider retention	Current Sub-Processor List and AI Transfer Overview disclose locations and limits; optional services are separated from core/public contexts	Review current DPA/transfer terms and necessity before enablement; update notices; keep an exit/disable route	[Rate and justify]
Public Echo used with identifiable case information	User-controlled text could reach Student Radar and OpenAI and appear in an ephemeral cache or provider abuse log	No name requested; prominent warning; bounded schema/body; store:false; up-to-10-minute Student Radar cache	Prohibit names, medical/safeguarding narratives and identifiers in local guidance; supervise child use where appropriate	[Rate and justify]
Sensory output treated as diagnosis or automated pupil decision	A child could be labelled or receive unsuitable support	Anonymous selection schema; no free text; validated/fallback content; no persistent profile; signed PDF boundary; advisory wording	Require professional judgement; record source and review date if added to a pupil record; set a school retention period	[Rate and justify]
School-enabled platform AI enabled on obsolete assumptions	Sensitive data could be sent without an accurate field, retention or transfer assessment	No blanket tokenisation or ZDR claim; current capability notice required before enablement	Obtain and approve the current capability-specific assessment and sample data flow; keep disabled until complete	[Rate and justify]
Public enquiry data retained or reused beyond the request	Unwanted contact or excessive retention	Strict field limits; server-only persistence; enquiry email is not treated as marketing consent	Apply the enquiry retention schedule; separate service response from marketing permission; honour objections	[Rate and justify]
Analytics or URLs disclose personal context	School or pupil context could leak through a query string, referrer or event property	Production telemetry is Vercel Web Analytics/Speed Insights; query strings and fragments are removed; custom events use an allowlist that rejects names, emails, school names, notes and query strings	Do not place personal data in public URLs; test any new event before release	[Rate and justify]
Retention or deletion differs from the controller's statutory schedule	Records may be erased too soon or kept too long	Contractual offboarding position and backup ageing are documented	Maintain the school retention schedule and authoritative copies; issue documented instructions; record legal holds	[Rate and justify]
Service disruption or recovery gap	Staff may lose timely access to information needed for pupil support	Disaster-recovery backups are described as retained for up to 90 days; continuity and incident-response documents are available separately	Keep appropriate school continuity procedures and alternative access to time-critical safeguarding information	[Rate and justify]



Part E - automated processing and human review

The public Sensory Profiler and Echo tools generate advisory output in response to a visitor's action. They do not create a persistent Student Radar pupil profile or make a legally binding pupil decision.

Student Radar does not make a blanket statement about every capability that may be available inside the authenticated platform. Before enabling an AI-assisted or risk-prioritisation capability, the controller must obtain its current capability description and decide:

- what input and output is involved;
- whether profiling occurs;
- whether any decision could have a legal or similarly significant effect;
- what meaningful human review, correction and override will occur;
- how bias, accuracy and over-reliance will be tested; and
- what transparency will be given to affected people.

Controller conclusion on Article 22 and profiling:

[Complete for the selected capabilities.]

Part F - outcome and approval

Decision	Controller to complete
Processing approved / approved with actions / not approved	
Actions required before go-live	
Action owners and dates	
Residual high risks	
DPO/Data Protection Lead advice	
Whether prior ICO consultation is required	
Review date and triggers	

If a high risk remains after reasonable mitigation, the controller must not begin that processing until it has considered the UK GDPR prior-consultation requirement and obtained appropriate advice.

Sign-off

Role	Name	Decision / signature	Date
Project owner			
DPO / Data Protection Lead			
Senior Information Risk Owner / equivalent			
Safeguarding lead, where relevant			



References

- Student Radar Sub-Processor List, version 1.5, reviewed 11 July 2026
- Student Radar AI Processing and Transfer Overview, version 1.4, reviewed 11 July 2026
- Student Radar Privacy Notice
- Student Radar Appropriate Policy Document - Supplier Statement
- Student Radar Data Retention and Deletion Schedule
- Executed Customer Data Processing Agreement
- ICO, [When do we need to do a DPIA?](#)
- ICO, [How do we do a DPIA?](#)

Version history

Version	Date	Change
1.0	21 February 2026	Withdrawn. It described obsolete AI capabilities, blanket tokenisation and ZDR, fixed residual-risk conclusions and unsupported technical controls.
1.1	11 July 2026	Rebuilt as verified supplier information plus a controller completion template; separated public tools from the authenticated platform and left school risk, lawful basis and approval decisions with the controller.