



Appropriate Policy Document

Clarity for Education

Version 1.1

Reviewed: 11 July 2026

Current supplier assurance statement for due diligence. It does not replace a school or trust's own Appropriate Policy Document.



Supplier statement on special category and criminal offence data

Document control	Detail
Organisation	SENDlink LTD, trading as Student Radar
Company number	16602655
Registered office	10 Masefield Gardens, Plymouth, PL5 3HU
Document owner	Student Radar Data Protection Lead
Version	1.1
Technical review date	11 July 2026
Next review	On any material change to special category or criminal offence processing, and no later than 11 July 2027
Status	Current supplier assurance statement for due diligence. It does not replace a school or trust's own Appropriate Policy Document.
Contact	dpo@studentradar.com

1. Purpose and legal scope

Some conditions in Schedule 1 to the Data Protection Act 2018 require the controller relying on them to maintain an Appropriate Policy Document. That document must explain the controller's procedures for complying with the data protection principles and its policies for retaining and erasing the relevant special category or criminal offence data.

In the strict statutory sense, this document is SENDlink LTD's Appropriate Policy Document only for processing for which SENDlink LTD is itself the controller and relies on a Schedule 1 condition that requires one. For school Customer Data, SENDlink LTD is normally a processor; the school or trust must identify its own lawful basis and conditions and maintain its own Appropriate Policy Document where required.

This document has two purposes:

1. to explain how SENDlink LTD handles such data when Student Radar processes it on a school or trust's instructions; and
2. to state clearly which public Student Radar services are not designed to collect such data.

For pupil, parent and school-staff records held in the authenticated Student Radar platform, the subscribing school or trust is normally the data controller and SENDlink LTD is its processor. The controller decides the purposes, Article 6 lawful basis, Article 9 condition, Article 10 authority and any applicable Schedule 1 condition. It must maintain its own Appropriate Policy Document where the condition it relies on requires one. Student Radar does not assign those conditions on the controller's behalf.

The current public-site activities described in this document are not designed to collect special category or criminal offence data, and SENDlink LTD does not assert a Schedule 1 condition for them. If SENDlink LTD begins controller processing that relies on a condition requiring an Appropriate Policy Document, this document must be updated before that processing starts to identify the condition, purpose, data, Article 5 procedures and specific retention/erasure policy.



This supplier statement supports, but does not replace, the executed Data Processing Agreement, the controller's privacy notices, record of processing activities, retention schedule or DPIA. If an executed agreement sets a more specific requirement, that agreement applies. The DPA 2018 does not require an Appropriate Policy Document to be published; this buyer-facing copy is shared voluntarily for transparency and must not expose confidential security detail.

2. Processing boundaries

Processing context	Intended data	SENDlink LTD's role	Special category / criminal offence position
Authenticated school platform	Pupil, parent/carer and staff records selected or entered by the school, including attendance, assessment, SEND, health and safeguarding information where the school uses those capabilities	Processor acting on the controller's documented instructions	Special category data may include health, disability, racial or ethnic origin, religious or philosophical belief, and information about sex life or sexual orientation where it appears in an authorised record. Safeguarding material may also contain alleged or confirmed criminal offence data. The school must document its conditions and necessity.
Wonde MIS connection	The fields the school authorises through its Wonde connection	Processor	The school controls the authorised connection and remains responsible for ensuring the selected fields are necessary for its purposes.
Public Sensory Profiler generation	Generic sensory domain, pattern and behaviour catalogue selections	Controller for the public service	The generation schema has no name, school, SEND status, year group, setting or free-text field and rejects those fields if submitted. It is not designed to receive personal, special category or criminal offence data.
Public Sensory Profiler PDF	The anonymous catalogue selections, unchanged validated generated content and a short-lived server signature	Controller for the public service	The route rejects unsigned, expired, modified or client-authored profile text. The PDF request is not intended to contain an identifier. A separate email address is collected only if the visitor requests PDF access.
Public Echo interpretation and speech	A bounded tapped phrase and the ordered button labels or vocalisations selected by the visitor; the generated short utterance is then sent for speech generation	Controller for the public service	Echo does not ask for a name and warns visitors not to include names or identifying details. Because its text fields are user controlled, SENDlink LTD does not describe every possible submission as anonymous. Visitors must not use Echo to submit identifiable health, safeguarding or criminal offence information.
Enquiry, demo and Pathfinder forms	Name, work email, school, role, selected interests and optional business context	Controller	These forms are for commercial or programme enquiries. They must not be used for pupil records, safeguarding narratives, medical information or other special category data.



Public Echo and Sensory Profiler processing is separate from any AI-assisted capability inside the authenticated platform. A school-enabled platform capability must have a current capability notice and assessment defining its fields, purpose, retention and safeguards before it is enabled. No blanket tokenisation, de-identification or Zero Data Retention claim applies across all platform AI processing.

3. Controller conditions and documented instructions

The controller must record, for each relevant school processing activity:

- the purpose and necessity of the processing;
- the Article 6 lawful basis;
- the Article 9 condition for each type of special category data;
- the Article 10 authority and DPA 2018 condition for criminal offence data;
- the specific Schedule 1 condition and whether it requires an Appropriate Policy Document;
- the people who may access the information;
- the controller's retention period and disposal decision; and
- any safeguarding, legal-hold or disclosure restrictions.

Conditions such as safeguarding of children, equality of opportunity, statutory functions, health or social care, or preventing unlawful acts may be relevant in a particular controller context. They are not interchangeable and are not automatically applicable merely because the customer is a school. The school or trust should obtain its own data-protection advice when selecting them.

SENDlink LTD will process Customer Data only for the contracted service and on documented instructions, subject to the limited exceptions required by law. An instruction that would require unlawful processing should be escalated to the Data Protection Lead rather than implemented without review.

4. Procedures for compliance with the data protection principles

4.1 Lawfulness, fairness and transparency

- The executed Data Processing Agreement defines the processor relationship and authorised processing.
- Schools are responsible for giving pupils, parents/carers and staff appropriate privacy information about their use of Student Radar.
- Student Radar publishes separate privacy information for data it controls directly, including website enquiries, technical data and public-tool use.
- Public-tool notices explain the data sent to the server and OpenAI and tell visitors not to enter identifiers or confidential case material.
- A capability-specific notice is required before school-enabled platform AI processing is treated as approved.

4.2 Purpose limitation

- Customer Data is used to provide, secure and support the capabilities selected by the controller, not for advertising.
- Public AI requests are made only after the visitor actively selects Generate or Interpret.
- Enquiry details are used to deliver and support the requested response. Supplying an email for a PDF or estimate is not treated as consent to unrelated marketing.
- A proposed new purpose must be assessed and documented before the data is reused.



4.3 Data minimisation

- The controller should authorise only the MIS fields and platform capabilities it needs.
- Public Sensory generation accepts only anonymous catalogue selections and rejects pupil context and free text.
- Echo limits field and request sizes but necessarily sends the visitor's chosen phrase and button text as submitted; users must keep it non-identifying.
- Public API routes apply same-origin checks, strict schemas and body-size limits. Rate limiting uses a policy-specific HMAC-SHA256 value derived from the request IP; the raw IP and form fields are not sent to the rate-limit store.

4.4 Accuracy

- The school remains responsible for the accuracy of Customer Data and for correcting information in its authoritative source where appropriate.
- Generated public-tool output is advisory drafting. The Sensory Profiler is not a diagnosis or professional assessment, and Echo interpretation may not reflect the user's intended meaning.
- Users must review output before relying on or adding it to a school record.

4.5 Storage limitation

- Live Customer Data is retained for the subscription and for up to 30 days after termination unless the controller gives a different documented instruction or a legal hold applies.
- Disaster-recovery backups may take up to 90 days to age out after termination.
- Public Echo and Sensory generated working data may be held in volatile process memory for up to 10 minutes and is not written to the Student Radar database by those routes.
- Sensory PDF signatures expire after 10 minutes.
- OpenAI Responses calls for the public tools set `store:false`. This prevents Responses application-state storage for those calls, but it is not Zero Data Retention. OpenAI may retain abuse-monitoring logs containing content for up to 30 days unless an approved provider control changes that position.
- The full supplier schedule is set out in the current Data Retention and Deletion Schedule. The controller remains responsible for its own statutory school-record retention.

4.6 Integrity and confidentiality

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. Customer access must also be configured by the school according to role and need.

Public API routes add input validation, request-size limits, same-origin checks and shared rate limits. Sensory PDF content is accepted only with a valid short-lived HMAC-SHA256 signature. Logs for these routes record bounded error categories rather than request bodies.

Detailed control evidence belongs in the current security and incident-response materials. This document does not extend a control claim beyond the scope supported by current evidence and makes no universal tokenisation or provider-retention promise.

4.7 Accountability

SENDlink LTD maintains:

- a Data Protection Lead and contact route;
- an executed Data Processing Agreement for school processing;
- a current Sub-Processor List;



- an AI Processing and Transfer Overview;
- a Data Retention and Deletion Schedule;
- security and incident-response documentation; and
- capability-specific review requirements for material new processing.

Material changes to a provider, data category, location, retention control or AI request boundary must trigger a review of the relevant records and customer information.

5. Access, disclosure and rights requests

Access to Customer Data must be restricted to authorised users and support personnel with a genuine need. The school is responsible for assigning and removing school-user access. SENDlink LTD must restrict administrative access to the purpose for which it is needed.

Where SENDlink LTD receives a rights request concerning data it processes for a school, it will direct the requester to the school or notify the school and provide reasonable technical assistance under the Data Processing Agreement. SENDlink LTD responds directly where it is the controller, for example in relation to an enquiry record or public-service technical data.

Special category or criminal offence data must not be disclosed through ordinary email or public-site forms. A proposed disclosure must be authorised by the controller, checked for third-party information and safeguarding restrictions, and transferred through an appropriate secure route.

6. Erasure, legal holds and incidents

Deletion instructions are subject to the controller's statutory duties and any documented legal or safeguarding hold. A hold must identify its owner, scope, reason and review date; it must not become indefinite by default.

If SENDlink LTD becomes aware of a personal-data breach affecting Customer Data, it will notify the controller without undue delay and provide available information to support the controller's assessment and reporting duties. SENDlink LTD does not decide on the controller's behalf whether the controller must notify the ICO or affected people.

7. Review and retention of this document

This document is reviewed when the relevant processing or legal framework changes and at least annually. Where it is being relied on as an Appropriate Policy Document for SENDlink LTD's own controller processing, it will be retained throughout that processing and for at least six months after the relevant processing ends. It will be supplied to the ICO without charge if lawfully requested.

8. Related documents and sources

- Student Radar Privacy Notice
- Student Radar Data Retention and Deletion Schedule
- Student Radar Data Protection Impact Assessment - Supplier Information and School Template
- 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 Security and Data Protection page
- Executed Customer Data Processing Agreement



- ICO, [Special category data guidance](#)
- ICO, [Substantial public interest conditions and Appropriate Policy Documents](#)
- ICO, [Criminal offence data conditions and Appropriate Policy Documents](#)
- ICO, [Policy document for special category and criminal offence data](#)

9. Version history

Version	Date	Change
1.0	21 February 2026	Withdrawn. It contained blanket AI tokenisation and control claims and did not separate public tools from school processing.
1.1	11 July 2026	Rewritten as a supplier statement; separated controller and processor responsibilities; documented the anonymous Sensory boundary, bounded Echo processing, current retention position and capability-specific AI review requirement.