Data Processing Agreement

Clarity for Education

Version 1.0

Prepared: 11 July 2026

Shareable procurement review template - not for signature

Procurement review template - not for signature

Document control	Detail
Processor	SENDlink LTD, trading as Student Radar
Company number	16602655
ICO registration	ZC016361
Registered office	10 Masefield Gardens, Plymouth, PL5 3HU
Review version	1.0
Prepared	11 July 2026
Status	Shareable procurement review template - not for signature
Data protection contact	dpo@studentradar.com

This document is a shareable review template. It is not an executed agreement, a signature copy, a Transfer Risk Assessment, a Data Protection Impact Assessment or legal advice. It creates no subscription, renewal, payment obligation or automatic paid continuation.

The Controller's legal identity, schools in scope, term, selected Packages, specific processing instructions and authorised school-enabled AI capabilities must be recorded in the signed Order Form and any incorporated capability schedule. No customer-specific information should be added to this reusable template.

1. Parties and contractual structure

1.1 This Data Processing Agreement (DPA) is intended to be entered into between:

- the Customer identified as Controller in the applicable Order Form (Controller); and
- SENDlink LTD, trading as Student Radar (Processor).

1.2 This DPA forms part of the Student Radar Master Services Agreement (MSA) only when it is included in an approved execution pack signed by both parties.

1.3 If documents conflict:

- this DPA prevails for the protection and processing of Controller Personal Data;
- the Order Form prevails for the Controller's legal identity, schools in scope, selected Services, dates, term, commercial terms and specific lawful processing instructions;
- a signed capability schedule provides additional instructions for that capability but cannot reduce this DPA's protections; and
- the MSA applies to liability and other commercial matters except where this DPA expressly says otherwise.

2. Definitions and interpretation

Applicable Data Protection Law means the UK GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 where applicable, and other binding UK data protection law applicable to the processing.

Controller Personal Data means Personal Data that the Processor processes on behalf of the Controller in providing the authenticated Student Radar Services. It does not include information for which Student Radar determines separate purposes as an independent Controller, as described in clause 3.4.

Data Subject, **Personal Data**, **Personal Data Breach**, **Processing**, **Processor**, **Controller**, **Special Category Data** and **Sub-processor** have the meanings in Applicable Data Protection Law.

Restricted Transfer means a transfer of Personal Data to a recipient in a country outside the United Kingdom that requires a safeguard under Chapter V of the UK GDPR.

Services means the Packages and capabilities selected in the Order Form.

UK GDPR has the meaning given in section 3(10), as supplemented by section 205(4), of the Data Protection Act 2018.

Terms defined in the MSA have the same meaning in this DPA. References to legislation include amendments and replacement legislation in force from time to time.

3. Roles, scope and duration

3.1 For Controller Personal Data, the Customer is Controller and Student Radar is Processor. Nothing in this DPA relieves either party of its own obligations under Applicable Data Protection Law.

3.2 This DPA applies only to Processing described in Annex 1 and only to the extent necessary to provide the selected Services in accordance with documented instructions.

3.3 Processing continues for the Subscription Term and then only for the return, deletion, legal retention and protected backup age-out described in clause 13.

3.4 Each party acts as an independent Controller for business contact details it determines are necessary to administer the commercial relationship, meet its own legal obligations or protect its systems. Student Radar also acts as Controller for its marketing website, enquiries, cookieless web analytics and visitor-triggered public Echo and Sensory Profiler tools, as described in its public Privacy Policy. Those independent purposes do not authorise Student Radar to use Controller Personal Data for advertising or unrelated product purposes.

3.5 The public Echo and public Sensory Profiler are not authenticated school platform capabilities and are outside the Processor instructions in this DPA. They are not an authorised channel for the Controller or its Authorised Users to submit Controller Personal Data.

4. Controller obligations and instructions

4.1 The Controller is responsible for:

- determining lawful purposes and an Article 6 lawful basis;
- identifying and documenting any applicable Article 9 condition and Data Protection Act 2018 Schedule 1 condition for Special Category Data;
- identifying any lawful authority for processing criminal offence data;
- providing required privacy information to Data Subjects;
- deciding and documenting retention periods;
- ensuring Controller Personal Data and instructions are adequate, relevant, limited and accurate;
- deciding whether a DPIA or prior consultation is required;
- authorising appropriate users and access roles; and
- ensuring that its instructions and use of the Services comply with Applicable Data Protection Law.

4.2 Documented instructions consist of this DPA, the signed Order Form, selected platform settings, a signed capability schedule and other written directions from an authorised Controller contact that are consistent with those documents.

4.3 An instruction to make a Restricted Transfer must be documented and must identify or permit a valid transfer mechanism. An instruction does not require the Processor to breach Applicable Data Protection Law or a Sub-processor contract.

4.4 The Controller must not direct staff to put pupil names, UPNs, dates of birth, safeguarding narratives or other Controller Personal Data into a public AI tool.

5. Processor obligations

5.1 The Processor will:

- process Controller Personal Data only on the Controller's documented instructions, including for a Restricted Transfer, unless UK law requires otherwise;
- inform the Controller before processing required by law, unless that law prohibits notice on important grounds of public interest;
- immediately inform the Controller if, in the Processor's reasonable opinion, an instruction infringes Applicable Data Protection Law;
- ensure persons authorised to process Controller Personal Data are subject to confidentiality obligations;
- implement and maintain appropriate technical and organisational measures under Article 32, including those in Annex 2;
- meet the Sub-processor obligations in clause 8;
- assist the Controller with Data Subject rights under clause 11;
- assist the Controller with security, breach, DPIA and prior consultation obligations under clauses 6, 7 and 12;
- return or delete Controller Personal Data under clause 13;
- provide information reasonably necessary to demonstrate compliance and allow audits under clause 14; and
- maintain records required of a Processor under Applicable Data Protection Law.

5.2 The Processor will not sell Controller Personal Data, use it for advertising, or use it to train a general-purpose or third-party model.

5.3 If the Processor must disclose Controller Personal Data to a court, regulator, law enforcement body or safeguarding authority, it will notify the Controller in advance where legally permitted, limit the disclosure to what is required and keep an appropriate record of the request and response.

6. Security of processing

6.1 Taking account of the state of the art, implementation costs, the nature, scope, context and purposes of Processing, and the risks to Data Subjects, the Processor will maintain technical and organisational measures appropriate to the risk.

6.2 The current control framework is summarised in Annex 2. Precise commitments that depend on a selected Service, provider configuration, retention period, availability target or recovery objective must be recorded in the Order Form or an approved security schedule. This DPA does not carry forward unverified claims about universal tokenisation, watermarking, honey tokens, immutable logs, fixed testing frequency or one-country execution.

6.3 The Processor may update security measures as technology and risks change, provided the overall protection of Controller Personal Data is not materially reduced.

6.4 The Controller will use available access controls, multi-factor authentication and user-management functions, and will promptly notify the Processor of suspected compromise.

7. Personal Data Breaches

7.1 The Processor will notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Controller Personal Data. An initial notification may be incomplete and followed by phased updates as facts become available.

7.2 The notification will include, to the extent known:

- the nature of the breach;
- the categories and approximate number of Data Subjects and records concerned;
- likely consequences;
- measures taken or proposed to contain, investigate and mitigate the breach; and
- a contact for further information.

7.3 The Processor will take reasonable steps to contain and remediate the breach, preserve relevant evidence and provide information reasonably required for the Controller's risk assessment and notification duties.

7.4 The Controller decides whether it must notify the ICO or affected Data Subjects, unless the Processor has a separate legal duty to notify. The Processor will not make a public statement identifying the Controller without prior consultation unless legally required.

8. Sub-processors

8.1 The Controller gives general written authorisation for the Processor to use the Sub-processors listed in Annex 3 for the stated purposes and only where the relevant Service or function is supplied.

8.2 The Processor will enter into a written agreement with each Sub-processor that imposes data protection obligations offering an equivalent level of protection for Controller Personal Data, including appropriate security measures.

8.3 The Processor remains responsible to the Controller for the Sub-processor's performance of its data protection obligations.

8.4 The Processor will give at least 30 days' written notice of an intended new or replacement Sub-processor where practicable. Shorter notice may be used for an urgent security, continuity or legal reason, with an explanation.

8.5 The Controller may object within 15 Business Days on reasonable and documented data protection grounds. The parties will work in good faith to resolve the concern. If they cannot:

- for an optional provider, the Processor will not enable or will discontinue the affected optional function; or
- for a provider necessary to the affected core Service, either party may terminate that affected Service without penalty, and the Processor will refund prepaid Fees for the unused period.

8.6 The current public Sub-processor List is a technical register. It supports transparency but does not vary this DPA or itself authorise a Restricted Transfer.

9. International transfers

9.1 The primary Supabase database for Controller Personal Data is configured in eu-west-2 London. This is not a promise that every hosting request, edge function, support activity, resilience process or optional provider remains solely in the United Kingdom.

9.2 The Processor will not make, or authorise a Sub-processor to make, a Restricted Transfer of Controller Personal Data unless:

- the Controller has authorised the relevant processing under this DPA, the Order Form or a capability schedule;
- the transfer is covered by UK adequacy regulations or an appropriate safeguard recognised by Applicable Data Protection Law, such as the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses; and
- a transfer risk assessment, now referred to in ICO guidance as the data protection test, and any supplementary measures are completed where required.

9.3 Remote access from another country is treated as a transfer where Applicable Data Protection Law says it is. The Processor will apply the same transfer safeguards to support and onward Sub-processor access.

9.4 The Processor will notify the Controller of a material change to a primary service region or transfer mechanism through the Sub-processor change process.

10. Artificial intelligence boundary

10.1 No school-enabled platform AI capability is authorised merely because a public tool or product demonstration exists.

10.2 A school-enabled AI capability may process Controller Personal Data only where a signed Order Form or capability schedule records:

- the capability and purpose;
- permitted input fields and Data Subject categories;
- whether Special Category Data is involved;
- the provider and model or service type;
- the output and required human review;
- application and provider retention;
- transfer mechanism and relevant assessment; and
- the method for disabling the capability.

10.3 All school-enabled AI output is advisory and requires review by an appropriately authorised member of school staff. The Processor will not use AI output as the sole basis for a decision producing legal or similarly significant effects about a pupil.

10.4 This DPA makes no blanket representation that AI inputs are tokenised. It does not state that OpenAI Zero Data Retention or Modified Abuse Monitoring is enabled.

10.5 The current public Echo and Sensory Profiler Responses calls use `store:false`. That setting prevents Responses application-state storage for those calls, but is not the same as Zero Data Retention. OpenAI may retain abuse-monitoring logs containing content for up to 30 days unless approved provider controls apply. Echo's separate audio speech request does not use the `store` parameter. These public tools are processed by Student Radar as Controller and are outside this DPA.

10.6 Public Echo accepts a bounded AAC phrase and button labels or vocalisations. Public Sensory Profiler generation accepts only anonymous catalogue selections and rejects pupil identity, school, SEND status, year

group, setting and free text. Its PDF route accepts the same anonymous selections and unchanged server-generated output with a short-lived server signature. Neither public route writes the profile to the Student Radar pupil database. This public boundary must not be presented as proof that an authenticated school capability uses the same fields or controls.

10.7 Before enabling a school capability that uses OpenAI or another AI provider, the Processor will provide the current capability-specific processing information and will not opt Controller Personal Data into model training.

11. Data Subject rights

11.1 Taking account of the nature of the Processing, the Processor will use appropriate technical and organisational measures to assist the Controller to respond to requests for access, rectification, erasure, restriction, portability and objection, and to address rights relating to automated decision-making where applicable.

11.2 If a Data Subject contacts the Processor about Controller Personal Data, the Processor will promptly refer the request to the Controller and will not respond substantively unless instructed or legally required.

11.3 The Processor will provide a reasonable export or other assistance in time for the Controller to meet its statutory deadline. The Controller remains responsible for identity verification, exemptions, third-party information and the final response.

11.4 Safeguarding or third-party information will not be automatically disclosed or withheld. The Controller is responsible for applying the relevant legal tests and redactions, with reasonable technical assistance from the Processor.

12. Compliance assistance and consultation

12.1 Taking account of the nature of Processing and information available, the Processor will reasonably assist the Controller with:

- security obligations under Article 32;
- breach assessment and notifications under Articles 33 and 34;
- DPIAs under Article 35; and
- prior consultation with the ICO under Article 36.

12.2 The Processor will provide current information about architecture, processing, Sub-processors and security controls reasonably needed for the Controller's assessment. The Processor does not determine the Controller's lawful basis or replace the Controller's DPIA.

12.3 If a proposed instruction requires material development, an unusual audit or substantial work outside the Services, the parties will agree a reasonable scope, timetable and any charge in writing. The Processor will not charge for assistance made necessary by its own breach.

13. Return, deletion and retention

13.1 During the Subscription Term, the Processor will retain Controller Personal Data in accordance with the Controller's documented retention instructions and the capabilities selected in the Order Form.

13.2 On expiry or termination, the Controller may choose return or deletion. Unless the Order Form or an approved retention schedule states a shorter period:

- the Processor will make a reasonable structured export available and delete Controller Personal Data from live systems within 30 days after the relevant instruction or end of the agreed export window; and
- protected backup copies will be put beyond routine use and will age out on the normal backup cycle within a maximum of 90 days.

13.3 The Processor will delete existing copies held by Sub-processors, subject to the same backup and legal-retention limits, and will provide reasonable written confirmation on request.

13.4 If UK law requires continued retention, the Processor will identify the legal requirement where permitted, isolate the retained data from routine use, protect it and delete it when the requirement ends.

13.5 The Processor will not keep Controller Personal Data after termination for benchmarking, model training, advertising or unrelated product development.

14. Information, audits and inspections

14.1 The Processor will provide information reasonably necessary to demonstrate compliance with Article 28 and this DPA, including current assurance documents and relevant independent certifications available to it.

14.2 The Controller or an independent auditor bound by confidentiality may audit compliance once in any 12-month period on at least 30 days' notice. Additional or shorter-notice audits are permitted where reasonably required by a Personal Data Breach, regulator or credible evidence of material non-compliance.

14.3 Audits should begin with documents and remote evidence. An on-site inspection must be proportionate, take place during normal business hours, protect other customers' confidentiality and avoid unreasonable disruption. An auditor must not be a competitor of the Processor.

14.4 The Controller bears its audit costs unless the audit identifies material non-compliance by the Processor, in which case the Processor will bear its reasonable remediation costs and will not charge for the necessary cooperation.

14.5 The Processor will cooperate with a competent data protection authority exercising lawful powers.

15. Liability

15.1 Each party remains responsible for its own compliance with Applicable Data Protection Law and for damage caused by its own acts and omissions.

15.2 Contractual liability under this DPA is governed by the liability provisions in the MSA execution copy. A contractual cap does not limit a regulator's powers or a Data Subject's statutory rights where the law does not permit limitation.

15.3 The Processor is not responsible for an unlawful instruction after it has informed the Controller under clause 5.1, except to the extent the Processor proceeds beyond what law requires or otherwise contributes to the breach.

16. General provisions

16.1 This DPA is governed by the laws of England and Wales and the courts of England and Wales have exclusive jurisdiction, without limiting the powers of the ICO or another competent regulator.

16.2 An amendment to an executed DPA must be in writing and signed by authorised representatives of both parties. A technical register or website update cannot reduce the protection in an executed DPA.

16.3 If a term is unenforceable, the remaining terms continue. No failure to enforce a right is a waiver.

16.4 This review template intentionally contains no signature block. The parties must create a clean execution copy with the applicable Order Form and version-controlled annexes.

Annex 1 - Details of Processing

Required detail	Processing description
Subject matter	Provision, hosting, operation, support and security of the authenticated Student Radar Packages selected in the Order Form.
Duration	The Subscription Term, followed only by the agreed export, live deletion and protected backup age-out periods in clause 13.
Nature	Collection from authorised sources, recording, organisation, storage, retrieval, consultation, display, analysis, reporting, communication, export, support, security logging, return and deletion. Optional activities apply only when the relevant Package or capability is selected.
Purpose	To provide the Customer's selected educational, pastoral, SEND, safeguarding, communication, assessment, health, office or teaching workflows and related administration.
Frequency	Ongoing during the Subscription Term and on actions initiated by Authorised Users, the configured Wonde sync or an expressly selected capability.
Data sources	Wonde MIS integration; direct input by authorised school staff; configured parent or guardian workflows; and other sources expressly identified in the Order Form. Wonde is the only direct MIS integration claimed by Student Radar unless the Order Form expressly states another verified integration.
Data Subjects	Pupils; parents, guardians and carers; school staff; governors or trust personnel where authorised; and professional or agency contacts whose information is lawfully included by the Controller.
Personal Data	Identifiers and demographics; education, assessment, attendance and behaviour records; SEND and provision information; health and medical information; safeguarding and welfare records; parent or guardian contacts; staff identity and role; communications; documents and media; user activity, access and security metadata. Only data necessary for selected Services and documented purposes is in scope.
Special Category Data	May include health, disability, SEND-related health information, ethnicity where lawfully configured, and other sensitive information present in authorised safeguarding or welfare records. The Controller must document the relevant Article 9 and Data Protection Act 2018 condition.
Criminal offence data	May arise within authorised safeguarding records. The Controller must identify the lawful authority and Schedule 1 condition where required.

Required detail	Processing description
Retention	Controller's documented schedule during service; default live-system return or deletion within 30 days after termination instruction/export window; protected backup age-out within a maximum of 90 days, unless the executed Order Form or approved retention schedule sets a shorter compliant period.
School-enabled AI	Out of scope unless a signed capability schedule completes the specific fields required by clause 10.2.

Annex 2 - Technical and organisational measures

The following summary records the review position. The execution copy should link to the current reviewed security and continuity documents and must not add a precise control that has not been verified by its control owner.

A. Governance and people

- documented responsibility for data protection and security;
- confidentiality obligations for authorised personnel;
- role-appropriate security and data protection training;
- controlled access approval and prompt access removal;
- documented incident response, continuity and supplier-review processes; and
- Cyber Essentials certification, subject to the current certificate and renewal status supplied in the procurement pack.

B. Identity, access and data isolation

- authenticated staff access with multi-factor authentication;
- role-based access and least-privilege permissions;
- Supabase row-level security and tenant or school context controls;
- private storage for non-public documents; and
- administrative controls for user lifecycle and sensitive exports.

C. Hosting, encryption and application security

- primary database, authentication and file storage in the configured Supabase eu-west-2 London project;
- Vercel application hosting, server-side functions, static assets and edge delivery, without a blanket claim that every request executes in one country;
- provider-managed encryption at rest for hosted Customer Data and encrypted transport for data in transit;
- bounded request validation, same-origin protections and server-only credentials for relevant public APIs;
- appropriate security logging and restricted access to production systems; and
- controlled deployment, dependency review and vulnerability remediation processes.

D. Resilience, deletion and incident management

- protected backups and restoration capability appropriate to the service risk;

- continuity and incident-response procedures;
- live-system return or deletion within the clause 13 period;
- backup copies put beyond routine use and aged out within a maximum of 90 days, unless a shorter executed schedule applies; and
- investigation, containment, evidence preservation and phased breach notification.

E. Public API abuse prevention

- Upstash Redis is configured for shared public-API rate limiting in eu-west-2 London with no global read replicas;
- limiter identifiers are policy-specific HMAC-SHA256 tokens derived from an IP address and a server secret;
- raw IP addresses, form fields and pupil data are not intended to be placed in limiter keys;
- limiter keys expire shortly after the one-minute policy window; and
- expensive AI and PDF routes fail closed if the shared limiter is unavailable, while designated lead and directory routes may fail open with structured server logging.

F. AI controls

- public AI routes are separated from authenticated school capabilities;
- public Sensory generation accepts anonymous catalogue selections and rejects identity, school and free-text pupil context;
- public Echo uses bounded input fields and users are told not to include identifiers;
- current public Responses calls use `store:false`, without claiming Zero Data Retention;
- short-lived Student Radar process-memory caches are separate from provider retention;
- school-enabled AI requires a capability-specific written instruction, assessment and human review; and
- Student Radar will not opt Controller Personal Data into model training.

Annex 3 - Authorised providers and applicability

This table is aligned with the technical Sub-processor List version 1.5, reviewed on 11 July 2026. Provider contracts, locations and services can change, so the execution pack must include the then-current register and apply clause 8 change control.

Provider	Status and purpose	Data and processing position	Location and transfer note
Supabase, Inc.	Core platform database, authentication, file storage and backups	Controller Personal Data required for selected Services	Primary project configured in eu-west-2 London. Provider support, resilience and onward processing remain subject to current contractual terms.
Vercel, Inc.	Core application hosting, server-side functions, static assets and edge delivery	Request and response data, sessions and technical logs as necessary to serve the application	No blanket one-country execution claim. Applicable transfer safeguards and deployment configuration govern processing.
Wonde Ltd	Direct MIS integration where enabled for the Customer	Configured pupil and staff data supplied from the Customer MIS	UK provider position, subject to the current Wonde agreement and Customer configuration. Student Radar makes no other direct MIS integration claim unless expressly stated in the Order Form.

Provider	Status and purpose	Data and processing position	Location and transfer note
Upstash, Inc.	Shared public-API rate limiting and abuse prevention	Policy-specific HMAC-SHA256 IP token and request count; no raw IP, form field or pupil data is intended in the key	Redis configured in eu-west-2 London with no global read replicas. Provider support access is governed by its DPA and transfer terms.
OpenAI, L.L.C.	Conditional, for a public visitor-triggered request or a separately authorised school-enabled capability	Public contexts are outside this DPA. School data is processed only under a signed capability schedule. No blanket tokenisation or ZDR claim applies.	General API domain; no UK-only claim. Restricted transfers require an approved mechanism and assessment. Default abuse-monitoring logs may retain content for up to 30 days unless approved controls apply.
Resend, Inc.	Conditional transactional email	Recipient address, message content and delivery metadata where the workflow is enabled	EU or US processing may occur under current provider safeguards. Unnecessary pupil data must not be included in email.
Twilio, Inc.	Conditional SMS delivery for Connect	Recipient phone number, message content and delivery metadata	EU or US processing may occur under current provider safeguards. SMS is a separately authorised Pass-through Cost.
Functional Software, Inc. (Sentry)	Conditional error and performance monitoring where configured	Technical diagnostics; configuration is intended to exclude Personal Data, subject to operational review	Provider processing and support may involve a Restricted Transfer under applicable safeguards.

Annex 4 - Article 28 execution checklist

The execution owner should confirm each item before issuing a signature copy. This checklist mirrors the minimum controller-processor contract elements identified by the ICO.

Article 28 requirement	Location in this draft	Execution check
Subject matter and duration	Clause 3; Annex 1	Order Form and Annex 1 agree on term and exit periods.
Nature and purpose	Annex 1	Only selected Packages and lawful purposes are listed.
Personal Data and Data Subjects	Annex 1	Categories match the Customer's actual configuration and DPIA.
Controller rights and obligations	Clause 4	Lawful basis, Article 9/10 condition, transparency and retention owner are identified.
Documented instructions, including transfers	Clauses 4 and 5	Order Form and capability schedules are complete; unlawful-instruction process retained.
Confidentiality	Clause 5.1; Annex 2A	Personnel and contractor commitments verified.
Article 32 security	Clause 6; Annex 2	Control owners verify each precise statement and current evidence.

Article 28 requirement	Location in this draft	Execution check
Sub-processors	Clause 8; Annex 3	Current register attached; notice, objection and flow-down terms approved.
Data Subject rights assistance	Clause 11	Operational route and contacts confirmed.
Breach, DPIA and consultation assistance	Clauses 7 and 12	Incident contact and the without-undue-delay notification route confirmed.
Return or deletion	Clause 13; Annex 1	Controller choice, 30-day live deletion and maximum 90-day backup age-out confirmed or replaced by a shorter executed schedule.
Information, audit and inspection	Clause 14	Evidence pack and audit process approved.
Processor's direct obligations	Clauses 5, 8, 14 and 15	Records, cooperation and statutory responsibility retained.

Primary ICO source: What needs to be included in the contract?

International transfer source: ICO international transfers guidance

Review note

This review template deliberately removes the older pack's consent-gated analytics wording, blanket tokenisation and de-identification promises, OpenAI Zero Data Retention claim, universal UK-only processing statement, obsolete AI feature list, unverified fixed logging claims and unsupported control assertions. Legal counsel, the data protection owner and the relevant technical control owners should approve the execution copy and capability schedules before signature.