Data Retention and Deletion Schedule

Clarity for Education

Version 1.1

Reviewed: 11 July 2026

Current external retention and deletion schedule, based on the reviewed service implementation and supplier register. School-controlled retention and executed agreements remain separate.

Document control	Detail
Organisation	SENDlink LTD, trading as Student Radar
Company number	16602655
Document owner	Student Radar Data Protection Lead
Version	1.1
Technical review date	11 July 2026
Next review	On a material change to data, providers, contracts or retention controls, and no later than 11 July 2027
Status	Current external retention and deletion schedule, based on the reviewed service implementation and supplier register. School-controlled retention and executed agreements remain separate.
Contact	dpo@studentradar.com

1. Purpose and scope

This schedule records how long SENDlink LTD intends to keep the principal information used by Student Radar, why it is needed and what happens at the end of the period. It covers:

- Customer Data processed for schools and trusts in the authenticated platform;
- public website enquiries and requested outputs;
- public Echo and Sensory Profiler working data;
- browser storage used by public tools;
- security, rate-limit and measurement data; and
- supplier administration records.

The subscribing school or trust is normally the controller for pupil, parent/carer and school-staff data in the authenticated platform. It remains responsible for its statutory school-record retention and for issuing lawful instructions to Student Radar. This supplier schedule does not replace the controller's retention schedule.

An executed Data Processing Agreement or Order Form may set a more specific requirement. A shorter lawful instruction will be followed where technically and legally possible. A longer period requires a documented controller instruction, legal obligation or legal hold; data is not kept indefinitely just in case it becomes useful.

2. Retention principles

Student Radar applies the following principles:

- **Purpose first:** every period must relate to a current operational, contractual, security or legal purpose.
- **Minimum necessary:** personal data is deleted or anonymised when the purpose ends unless a documented exception applies.
- **Clear trigger:** periods run from a defined event, such as termination, last meaningful contact or incident closure.
- **Separation of roles:** the school's statutory record period is not automatically copied into the processor's platform retention.

- **Provider transparency:** provider-controlled retention is stated as such and is not presented as a Student Radar technical deletion guarantee.
- **Review rather than default extension:** a record is not retained merely because the system can hold it.
- **Secure disposal:** live records are removed from the relevant system; encrypted backups age out under their lifecycle; browser data can be cleared by the user.

3. Retention schedule

3.1 Authenticated platform and Customer Data

Information	Purpose	Standard period / trigger	End-of-period action	Status and qualification
Live Customer Data, including pupil, SEND, attendance, assessment, health and safeguarding records	Deliver the capabilities selected by the controller	Subscription term plus up to 30 days after termination, unless the controller gives an earlier or different documented instruction or a legal hold applies	Provide the agreed export opportunity, then delete from live systems	Current public and contractual position. The school must retain any authoritative or statutory records it still requires.
Parent/carer and school-staff Customer Data	Communications, authorised access and selected platform workflows	Subscription term plus up to 30 days after termination, subject to controller instructions	Delete from live systems	Covered by Customer Data offboarding rather than a separate, indefinite period.
Authentication and access records tied to an active school account	Secure access, account administration and incident investigation	Active account; account data is included in Customer Data offboarding. Security events retained under the audit schedule below where necessary	Disable access promptly; delete account data on offboarding; retain only the necessary security record	School must notify Student Radar of leavers and access changes.
Platform audit events	Accountability, investigation and support for controller obligations	13 months from the event; longer only for a documented incident, dispute, legal obligation or hold	Delete or irreversibly aggregate; record any exception	Current policy period. Applied through scheduled or manual lifecycle review; exceptions are recorded.
Database backups containing Customer Data	Disaster recovery	Rolling provider lifecycle; up to 90 days after termination for data to age out	Automatic expiry under the backup lifecycle	Backups are not a separate archive. If a backup is restored, applicable deletion instructions must be reapplied.
Wonde connection credentials and mappings	Operate the authorised MIS connection	While the connection and customer service are active	Revoke/disconnect and delete in accordance with the integration offboarding process	No claim is made that Wonde retains nothing beyond its own contract and logs; see the current Sub-Processor List and provider terms.

The school is responsible for deciding how long it must retain SEND, safeguarding, attendance, assessment and other education records in its authoritative systems. Ending the Student Radar subscription does not remove that responsibility.

3.2 Public enquiries and requested outputs

Information	Purpose	Standard period / trigger	End-of-period action	Status and qualification
Demo and contact enquiries	Respond to the request, arrange a walkthrough and document the commercial conversation	Review 12 months after the last meaningful contact if no customer relationship begins	Delete, or record a specific current reason and new review date	Current policy period. Supplying an enquiry is not consent to unrelated marketing. Manual review applies where no automated lifecycle is available.
Pathfinder applications	Assess and administer the funded programme and communicate the outcome	Unsuccessful/inactive application: review 12 months after the programme decision or last meaningful contact. Successful application: move necessary records into the customer/contract record	Delete unnecessary application detail; retain contractual records under the contract schedule	Priorities/free-text must not contain pupil or safeguarding case details.
Sensory Profiler PDF access email and optional role	Unlock and support the requested PDF	Review 12 months after capture if no customer relationship or continuing support need exists	Delete from the enquiry store	The sensory selections and generated profile are not stored with the enquiry. The email is not stored in the browser; only a session boolean is kept.
Inclusion-funding estimate request	Deliver the requested estimate and support the enquiry	Review 12 months after the last meaningful contact if no customer relationship begins	Delete contact/enquiry record; provider delivery metadata follows provider terms	School and local-authority context is business information; the form must not contain pupil data.
Compare business-case PDF request	Render the visitor's requested PDF	Request lifecycle only	Discard after response; response uses Cache-Control: no-store	The route does not persist the request body. School name, roll, setting and decision note are not placed in the shareable URL or analytics.
School-directory lookup query	Return public GIAS school matches	Request lifecycle only in the Student Radar route	No application record created; response uses Cache-Control: no-store	Hosting and database providers may still create bounded technical/security logs under their controls.

3.3 Public Echo

Information / storage	Purpose	Period	End-of-period action
Tapped phrase and ordered button labels/vocalisations sent to Student Radar and OpenAI	Interpret the visitor's request	Request lifecycle; Student Radar may cache the generated text and audio in volatile process memory for up to 10 minutes	Cache entry expires or disappears earlier when the process restarts; no database write by this route
Generated short utterance sent to OpenAI audio speech	Produce speech requested by the visitor	Provider request lifecycle; default provider abuse-monitoring logs may be retained for up to 30 days	Provider expiry under its API controls

Information / storage	Purpose	Period	End-of-period action
OpenAI Responses application state	Generate the interpretation	The request sends store:false, so Responses application-state storage is not requested	No blanket ZDR claim: default abuse-monitoring retention may still be up to 30 days
Echo localStorage preferences and acknowledgement	Remember language/display choices, default board version, optional shared context and that the AI notice has been seen	Until the user clears site data, a relevant app update replaces it, or the browser removes it	Cleared through browser/site settings
Echo IndexedDB (aac-board-db)	Store board sets, boards and assets for the requested AAC and offline functionality	Until the user removes a board or clears site data	Deleted by the app action or browser/site-data controls
Echo Cache Storage and service worker	Cache application assets for offline/fast operation	Until replaced by an app/service-worker update or cleared by the user/browser	Old versioned assets removed by the service-worker lifecycle or site-data controls
Echo session scroll state	Restore navigation position	Browser-tab/session lifecycle	Browser clears session storage

Echo fields are user controlled. Visitors must not enter names, medical or safeguarding details, or other identifying content. Browser-stored custom board or shared-context content may be personal if the user puts personal information in it.

3.4 Public Sensory Profiler

Information / storage	Purpose	Period	End-of-period action
Generic domain, pattern and behaviour selections in browser session storage	Carry selections from the questionnaire to the output route	Current browser-tab/session; removed when the visitor selects Start a new profile	Browser/session deletion or explicit removal
Anonymous catalogue selections sent for generation	Generate the requested profile	Request lifecycle; validated output may be held in volatile process memory for up to 10 minutes	Cache expiry or earlier process restart; no profile database write
OpenAI Responses application state	Generate the profile text	The request sends store:false	No blanket ZDR claim: provider abuse-monitoring logs may still be retained for up to 30 days
Signed PDF content	Authenticate that PDF content is the unchanged server-generated result	HMAC-SHA256 signature expires after 10 minutes	Expired signatures are rejected; the visitor must generate again
PDF rendering request and PDF	Produce the download	Request/response lifecycle only; response uses Cache-Control: no-store	Discard after response
PDF-access marker in session storage	Avoid asking for the email again in the same browser session	Current browser-tab/session	Browser clears session storage

The generation API rejects name, school, SEND status, year group, setting, self-advocacy and free-text fields. If a school later attaches a downloaded PDF to an identifiable pupil record, that copy is controlled and retained by the school under its own schedule.

3.5 Security, abuse prevention and marketing measurement

Information	Purpose	Standard period / trigger	Qualification
Upstash public-API rate-limit keys	Prevent automated abuse and enforce per-route limits	A little over two minutes after the one-minute sliding window	Key is a policy-specific HMAC-SHA256 value derived from the request IP. Raw IP and form data are not sent to Upstash.
Hosting/security logs, which may include IP address and request metadata	Threat detection, incident investigation and service operation	Provider/account-controlled operational period; reviewed against need and provider settings	This schedule does not invent a single fixed Vercel log period that is not verified in the implementation review. Request bodies must not be deliberately logged by public routes.
Public API error logs	Diagnose route failures	Operational log period	Current routes log bounded error types/codes, not form values or public-tool request bodies.
Vercel Web Analytics visitor identifier	Produce anonymous, aggregated traffic measurement	Automatically resets after 24 hours	No cookie; not associated with an individual or IP address in Student Radar analytics reports.
Web Analytics aggregate data and custom events	Understand page use and approved non-personal funnel steps	Retained under the current Vercel plan and account controls	Query strings and fragments are removed. Custom properties are allowlisted and exclude names, emails, school names, notes and query strings.
Vercel Speed Insights data	Measure route and Core Web Vitals performance	Retained under the current Vercel plan and account controls	Vercel describes data points as anonymous and not tied to a visitor or IP address.

3.6 Corporate, contract and incident records

Information	Purpose	Standard period / trigger	End-of-period action
Executed agreements, Order Forms, DPAs and material contract correspondence	Contract administration, audit and legal claims	Agreement term plus six years, unless a longer legal hold applies	Secure deletion at expiry
Invoices and accounting records	Accounting and statutory record-keeping	Six years from the relevant accounting period or longer where applicable law requires	Secure deletion at expiry
Security and personal-data incident record	Evidence decisions, notifications, remediation and learning	Six years after closure, subject to legal hold and necessity review	Secure deletion or irreversible aggregation at expiry
Procurement evidence and policy version history	Demonstrate which assurance statement applied at a given time	Current version plus superseded versions needed for accountability and contract history	Retain a controlled archive; do not publish superseded files as current

4. Deletion and offboarding procedure

1. **Confirm scope and authority.** Verify the customer, affected systems, controller instruction, legal holds and required export.
2. **Restrict access where appropriate.** Disable accounts and connections that no longer require access.

3. **Export or return.** Make Customer Data available in the format and window agreed in the executed contract.
4. **Delete live data.** Remove Customer Data from live systems after the applicable export/offboarding window.
5. **Revoke integrations.** Disconnect Wonde and other customer-specific provider access.
6. **Allow backup ageing.** Backups expire under the documented maximum lifecycle. If a backup is restored, deletion instructions are reapplied.
7. **Record completion.** Keep a minimal deletion record identifying the customer, scope, authoriser and completion date. A deletion confirmation can be provided where agreed.

A deletion confirmation describes the scope and systems actually completed. Provider systems and protected backups follow their verified lifecycle rather than an invented per-record deletion promise.

5. Early deletion, restriction and legal holds

Personal data should be deleted earlier where it is no longer needed and no contractual or legal reason remains. For Customer Data, the school normally decides whether an individual rights request requires deletion or restriction and sends the documented instruction to Student Radar.

A legal or safeguarding hold must record:

- the data and people covered;
- the legal or safeguarding reason;
- the person who authorised it;
- the start and review dates; and
- the event that ends the hold.

Held data must be restricted to the hold purpose. It must be deleted or returned to the normal schedule when the hold ends.

6. Monitoring and review

The Data Protection Lead owns this schedule. Each system owner must be able to show how its period is applied. A manual review is acceptable where the volume and risk make it proportionate, but it must be recorded. An automated period must not be described as implemented until it has been tested.

The schedule is reviewed:

- after a provider, data-flow or contractual change;
- after a relevant incident or rights request;
- before a new AI or tracking capability is enabled; and
- at least annually.

7. Related documents and sources

- Student Radar Privacy Notice
- Student Radar Cookie, Client Storage and Telemetry Notice
- 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 Appropriate Policy Document - Supplier Statement
- Student Radar Data Protection Impact Assessment - Supplier Information and School Template
- Executed Customer Data Processing Agreement

- ICO, Storage limitation
- ICO, Retention audit framework
- Vercel, Web Analytics privacy and compliance
- Vercel, Speed Insights privacy and compliance

8. Version history

Version	Date	Change
1.0	21 February 2026	Withdrawn. It included consent-cookie, blanket AI and provider-retention claims that did not match the current implementation evidence.
1.1	11 July 2026	Rebuilt around role-specific Customer Data offboarding, verified public-tool lifecycles, browser storage, short-lived HMAC rate-limit keys, cookieless telemetry and explicit implementation qualifications.