

# Record of Processing (ROPA) + Breach Response — spelling.live

**Status:** Complete — keep current on any processing change. The ROPA satisfies UK GDPR Art. 30 record-keeping; the breach plan covers Art. 33/34. Not legal advice.

| Date       | Owner                                                                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2026-06-30 | Sole Trader: Spelling Live, <a href="mailto:support@spelling.live">support@spelling.live</a>                                                                   |
| 2026-10-14 | AK Shah Ltd (Manoj Shah, Director), <a href="mailto:support@spelling.live">support@spelling.live</a> - Resend added as a processor; controller details updated |

## Part A — Record of Processing Activities (Art. 30)

**Controller:** AK Shah Ltd (company number 17491910), trading as Spelling.Live, [support@spelling.live](mailto:support@spelling.live). Previously Mr Manoj Shah as a sole trader (ICO ref ZC173462); AK Shah Ltd holds its own ICO registration (ref ZC266285, registered name: Ak Shah Ltd). **DPO:** none (not required).

**Representative:** N/A (controller is UK-based).

### A1. Processing activities & purposes

| Activity                                                                                    | Purpose                                                                               | Lawful basis                                                                                                                |
|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Account & child-profile management                                                          | Run the service the parent set up                                                     | Contract                                                                                                                    |
| Spelling practice & progress tracking                                                       | Deliver/personalise learning; parent reports                                          | Contract / legitimate interests                                                                                             |
| AI features (sentences, hints, handwriting & worksheet reading, voice transcription, audio) | Generate learning content & feedback                                                  | Consent (optional features) / contract                                                                                      |
| Handwriting/formation analysis                                                              | Per-child writing feedback                                                            | Contract (part of the learning service); parent can toggle off per child                                                    |
| AI Spelling Coach tips (incl. per-child pattern personalisation)                            | Explain to a parent/child why a spelling mistake keeps happening and what to practise | Contract (part of the learning service); parent-initiated per word                                                          |
| Security, logging, abuse/credit metering                                                    | Protect the service                                                                   | Legitimate interests                                                                                                        |
| Progress/reminder emails                                                                    | Keep parents informed                                                                 | Legitimate interests (service-related communications to the parent who signed up; parent can disable reminders in settings) |

| Activity                                               | Purpose                                               | Lawful basis                                                                                                                           |
|--------------------------------------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Practice reminders on the parent's device (native app) | Remind a child to practise at a time the parent chose | Consent (parent switches it on per child; OS notification permission). Stored and scheduled on the device only - nothing is sent to us |
| Support feedback handling                              | Respond to users                                      | Legitimate interests                                                                                                                   |

## A2. Categories of data subjects & personal data

- **Parents:** email, account IDs, sign-in provider metadata, IP/device/server logs.
- **Children:** name/label, learning level, year group, practice activity, per-word stats, handwriting image thumbnails, transient voice input, report events.
- **Children — derived/inferred:** spelling-error pattern classifications (deterministic, from `spelling_report_events`), Skills Check feature profiles (`skills_checks.feature_profile`), and AI-generated coach tips personalised to that child's recurring patterns (`child_word_tips`). These are **inferences about a child's learning difficulties**, not just activity records, so they are RLS-scoped to the owning parent (or the child's own login), covered by account/child delete and by the data export, and never shared with another child. The non-personalised tip caches (`word_tips`, `mistake_tips`) are keyed on the word and the misspelling only, contain no child identifier, and are deliberately shared across learners.
- **Children — imported from Google Classroom (teachers only):** the pupil's Google Classroom user ID, stored as a dedupe key so a repeat import never duplicates a child (`child_external_identities`). No email or photo is requested or stored. Google Classroom is a data **source** authorised by the teacher, not a recipient of our data.
- **Children — imported from a school MIS via Wonde (teachers only):** the pupil's Wonde student ID, stored as the same dedupe key (provider `wonde`), plus the preferred name. Nothing else from the MIS is read. Wonde is a data **source** authorised by the school in the Wonde portal, not a recipient of our data.
- **Special category (Art. 9):** none intended (handwriting images are not biometric identification; voice is transient).

## A3. Recipients (processors / sub-processors)

| Recipient | Role                   | Data               | Location                                                                                                                                                                                      | Safeguard                           |
|-----------|------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| Vercel    | Hosting/infrastructure | IP, logs, requests | <b>Serverless (Node) functions:</b> EU — Frankfurt ( <code>fra1</code> ); <b>Edge Functions + static assets:</b> global edge network (executed nearest the request; most API routes are Edge) | DPA with SCCs Accepted (2026-06-30) |

| Recipient    | Role                     | Data                                                                                                                             | Location                             | Safeguard                                                                                       |
|--------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|-------------------------------------------------------------------------------------------------|
| Supabase     | Database, storage, auth  | All stored personal data                                                                                                         | <b>EU — Ireland (AWS eu-west-1 )</b> | In the EEA (UK adequacy); <b>DPA with SCCs</b> also accepted (2026-06-30) for US support access |
| OpenAI       | AI text/vision/voice/TTS | Practice text, handwriting images, voice                                                                                         | US                                   | <b>DPA with SCCs</b> Accepted (2026-06-30)                                                      |
| Google Cloud | TTS/Vision/Gemini        | Text, audio, images (incl. Write it handwriting images for Cloud Vision reading - no name, ID or expected word, from 2026-10-04) | US/global                            | <b>DPA with SCCs</b> Accepted (2026-06-30)                                                      |
| Anthropic    | Support-feedback triage  | Feedback text                                                                                                                    | US                                   | <b>DPA with SCCs</b> Accepted (2026-06-30)                                                      |

| Recipient | Role                                                                          | Data                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Location                                | Safeguard                                 |
|-----------|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|-------------------------------------------|
| PostHog   | Product analytics, feature flags, session replay (churn analysis)             | Anonymous profile UUID, event names with numeric/boolean properties only. Parent/tutor account email ( <code>parent_email</code> person property, adult data) for genuine parent logins only. No child names, practice words, or free-text, except the site-search term typed on the public help/blog/resources pages (not in the app), scrubbed and withheld when it contains an email, phone number or web address ( <code>js/site-search.js</code> ). Session replay masks all displayed text and all typed inputs by default; only parent-facing static UI (sign-in, add-child copy) is unmasked — no child name/practice word/handwriting is captured. | EU<br>( <code>eu.i.posthog.com</code> ) | DPA<br>Accepted<br>(2026-06-30)           |
| Resend    | Transactional email (progress reports, reminders, account and teacher emails) | Recipient name and email address, email subject and body as sent                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | US                                      | DPA with SCCs<br>Accepted<br>(2026-10-13) |

Canonical AI list is maintained in `data/ai-subprocessors.json` and reviewed on a recurring schedule ( `npm run check-vendor-terms` ).

## A4. International transfers

**Policy: choose the EU option wherever a provider offers one.** Supabase, PostHog and Vercel's function region are all set to EU. Where a service is inherently global (a CDN / edge network) or US-only (the AI vendors), that is stated plainly below rather than implied away.

**Data at rest is in the EEA.** The two stores that hold personal data are both EU-hosted: Supabase (database, storage, auth) in AWS `eu-west-1` (Ireland) and PostHog (analytics) on its EU Cloud instance. Transfers to the EEA are covered by the UK's adequacy regulations, so no SCC reliance is needed for either.

**Compute is EU-configured but not EU-only.** Vercel's function region is set to Frankfurt ( `fra1` ), which governs Serverless (Node) functions. It does **not** pin Edge Functions: those execute at the point of presence nearest the request, and most of the API — including every route handling child

practice data — is `runtime: "edge"`. So request handling (IP, request content in memory) can occur outside the EEA even though nothing is stored outside it.

Transfers outside the UK/EEA therefore arise from three things, all covered by DPAs with Standard Contractual Clauses (see A3):

- **Edge request handling** — Vercel Edge Functions run at the nearest global PoP.
- **AI calls in flight** — request content is sent to OpenAI, Google and Anthropic in the US, processed, and returned; it is not stored there under our API configuration (no-training stance, see `data/ai-subprocessors.json`).
- **Vendor support/operations access** — Vercel and Supabase are US companies whose staff may access infrastructure for support.

All provider DPAs accepted by the controller (confirmed 2026-06-30).

## A5. Retention

Automated via `purge_expired_data()` (daily cron, dry-run by default): usage 14m · email log 12m · feedback + screenshots 12m · challenge data 90d · **handwriting thumbnails 90d (image only; scores kept)** · dormant unconfirmed accounts 12m. On-demand erasure via in-app account/child delete. Unused-account sunsets (email warning + keep link first): no child → deleted day 30 after signup; no sign-in or practice for 6 months → deleted 30 days after the warning, children included (`sunset-childless`, `sunset-inactive`; armed only after queue review).

## A6. Technical & organisational measures

Supabase RLS (owner-scoped), private storage buckets, JWT auth, service-role keys server-side only, owner-only child erasure, credit metering, child-safe AI guardrail, retention automation, self-service rights tooling.

---

## Part B — Personal Data Breach Response (Art. 33/34)

**Goal:** assess any suspected breach and, if it meets the threshold, report to the **ICO within 72 hours** of becoming aware, and tell affected individuals if high risk. Children's data raises the likelihood that notification is needed.

### B1. If you suspect a breach

1. **Contain** — revoke keys/sessions, take the affected route offline, stop the leak.
2. **Record** time discovered, what happened, data and people affected (especially children), likely cause. Start a log immediately.
3. **Assess risk** — what data, how many, could it harm the child/parent (identity, safety, distress)?

### B2. Decide & notify

- **Report to the ICO within 72 hours** if there's a risk to people's rights/freedoms. ICO breach line / online form. Better to report and stand down than miss the window.

- **Tell affected parents without undue delay** if the breach is **high risk** — plain language: what happened, likely impact, what you're doing, what they can do.
- If a **processor** (Vercel/Supabase/AI provider) caused it, they must inform you; capture their incident report.

### B3. After

Fix root cause, record lessons learned, update this plan and the DPIA if the processing or risk changed. Keep a breach register (even for non-reportable ones).

**Key contacts:** ICO — [ico.org.uk](https://ico.org.uk) / 0303 123 1113. Controller — [support@spelling.live](mailto:support@spelling.live).

#### Processor status & security contacts:

| Provider     | Status page                                                           | Security contact                                                   |
|--------------|-----------------------------------------------------------------------|--------------------------------------------------------------------|
| Vercel       | <a href="https://vercel.com/status">vercel.com/status</a>             | <a href="mailto:security@vercel.com">security@vercel.com</a>       |
| Supabase     | <a href="https://status.supabase.com">status.supabase.com</a>         | <a href="mailto:security@supabase.io">security@supabase.io</a>     |
| OpenAI       | <a href="https://status.openai.com">status.openai.com</a>             | <a href="mailto:security@openai.com">security@openai.com</a>       |
| Google Cloud | <a href="https://status.cloud.google.com">status.cloud.google.com</a> | <a href="mailto:security@google.com">security@google.com</a>       |
| Anthropic    | <a href="https://status.anthropic.com">status.anthropic.com</a>       | <a href="mailto:security@anthropic.com">security@anthropic.com</a> |
| PostHog      | <a href="https://status.posthog.com">status.posthog.com</a>           | <a href="mailto:security@posthog.com">security@posthog.com</a>     |
| Resend       | <a href="https://resend-status.com">resend-status.com</a>             | <a href="mailto:security@resend.com">security@resend.com</a>       |

Spelling.Live is operated by AK Shah Ltd (company number 17491910, England and Wales; ICO registration ZC266285). Rendered 2026-10-14 from the maintained source; the current version is always at <https://spelling.live/for-schools/trust>.