Noeva.

CONFIDENTIAL · INTERNAL

VOL. 01 · DATA PROTECTION 2026

The data *discipline.*

Noeva's data protection and GDPR policy. The technical, legal and operational standards every byte of personal data on this companion is held to — and the standards every parent has the right to see in writing. Owned by the Data Protection & Security Architect; co-reviewed with the Child Safeguarding & Compliance Lead.

DOCUMENT	EDITION	STATUS	OWNER
Data Protection & GDPR Policy	Vol. 01 · 2026	Adopted · Pre-launch	DP & Security Architect

CONTENTS · ELEVEN SECTIONS

Inside this policy.

A working document. Adopted before any parent or Spark data is captured, reviewed every twelve months thereafter, and republished whenever the platform, the data flows, or the regulatory ground shifts beneath it.

SECTION 01 · STANDING

Purpose, scope *and standing.*

A data protection policy is not paperwork. It is the standard a regulator, a parent, or a future investor can hold us to — and the standard our own people are held to internally.

> Noeva holds children's data. That single fact raises the bar on every decision below — the technical controls, the contractual standards, the retention windows, the consent mechanics, and the audit trail. This policy makes that bar *operational.*

Purpose

The purpose of this policy is to translate UK data protection law — the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations, and the ICO Children's Code — into the specific controls, processes, named accountabilities, and lawful bases under which Noeva processes personal data. It is the policy a regulator can ask to see, the policy a parent can ask to see, and the policy any vendor or processor working with Noeva is required to meet.

Scope

This policy applies to every category of personal data Noeva processes, every person who processes it on Noeva's behalf, and every system, contract and third party involved in that processing. Specifically:

- → All personal data of parents who hold a subscription, have signed up to the waiting list, have enquired about Noeva, or have engaged with us in any other capacity.
- → All personal data of Sparks aged 6 to 18 enrolled on the companion through a parent account.
- → All employees, contractors and Noeva personnel whose own data we hold.

- → All processors — Lovable, Supabase, Stripe, our email provider, model providers, analytics vendors — to whom we entrust personal data under Article 28.
- → All marketing, analytics, customer-support and product-development activities that touch personal data, including the AI processing that powers the daily Moves and Anchors.

Standing and relationship to the Safeguarding Policy

This policy sits alongside the Noeva Safeguarding Policy Vol. 01. The two are designed to be read together. The Safeguarding Policy governs the duty of care to Sparks — content standards, AI guardrails, escalation procedures, parental authority architecture. This policy governs the data discipline underneath those decisions — lawful bases, retention, rights mechanics, technical controls, vendor risk, breach response. Where the two policies overlap, the more protective of the child applies. Where a conflict cannot be resolved at operational level, it is escalated within seventy-two hours to the Founder.

A NOTE ON REGISTER

Data protection language is precise *because the law is.*

Noeva's external voice is editorial. The voice in this policy is not. Terms like "controller," "processor," "lawful basis," "data subject," "supervisory authority," and "personal data breach" carry specific meanings in UK GDPR; this document uses them as defined in the legislation and is unembarrassed about doing so. Where a plain-English summary helps a parent or a member of the team, we provide it — but the legal term is the binding one.

SECTION 02 · THE LAW

The legal *ground.*

Five frameworks govern this policy. All are UK; some are new — the Data (Use and Access) Act 2025 reshaped material parts of the regime in 2026 and we incorporate those changes directly.

Noeva is a UK-based service. Its primary data subjects are UK-resident parents and Sparks. The frameworks below apply.

UK GDPR PRIMARY REGIME	The UK General Data Protection Regulation. The seven principles in Article 5 are the operating spine of this policy and are set out in Section 04. Material amendments introduced by the DUAA 2025 — particularly to Article 22 on automated decision-making and Article 25 on data protection by design — are incorporated throughout.
Data Protection Act 2018 DOMESTIC FRAMEWORK	The Act through which UK GDPR has effect, plus the domestic exemptions and conditions. Of particular relevance for Noeva: the recognition that children warrant specific protection in relation to their personal data, and the conditions governing processing of special category data.

Data (Use and Access) Act 2025

MATERIAL AMENDMENTS

The DUAA, which entered into force during 2025 with further provisions taking effect in 2026, amends the UK GDPR and DPA 2018 in ways directly relevant to Noeva. Section 81 of the DUAA strengthens Article 25 by requiring online services likely to be accessed by children to give particular regard to children's higher protection matters when implementing data protection by design and by default. Section 80 replaces the previous Article 22 regime on solely automated decision-making with new Articles 22A-D, clarifying definitions and providing a more permissive framework for non-special-category processing accompanied by mandatory safeguards. The DUAA also introduces a new "recognised legitimate interests" lawful basis, refines the time limits for responding to data subject access requests (the "stop the clock" rule), and changes the international transfer test from "essentially equivalent" to "not materially lower." These changes are reflected in the relevant sections below.

PECR

MARKETING & COOKIES

The Privacy and Electronic Communications Regulations. Governs cookies, similar technologies, and electronic direct marketing. Noeva's cookie posture is set out in Section 09; our marketing posture is set out in Section 06. Noeva does not run advertising to children under any circumstances.

ICO Children's Code

STATUTORY CODE

The Age Appropriate Design Code. Fifteen standards governing information society services likely to be accessed by under-18s. Noeva conforms to all fifteen. The Code is currently under ICO review following the DUAA; this policy is updated when revised standards are issued.

This policy does not address regimes outside the UK directly. Where Noeva subsequently offers the service to a Spark or parent in another jurisdiction, the international transfer regime in Section 09 applies and the lead supervisory authority position is reassessed by the Data Protection & Security Architect.

SECTION 03 · ROLES

Controllers, processors *and roles.*

UK GDPR turns on who decides what happens to personal data. Here is what Noeva is under the law, what our vendors are, and who inside Noeva is accountable for what.

Noeva's position

Noeva is the **data controller** for all personal data processed in the delivery of the companion. We determine the purposes and means of processing — what data is collected, why, for how long, and what is done with it. Lovable, Supabase, Stripe, our email provider, and our model provider are **data processors** acting on our documented instructions under Article 28 contracts. We do not act as a processor for any other organisation.

Are we required to appoint a DPO?

Under UK GDPR Article 37, formal appointment of a Data Protection Officer is mandatory only in specific circumstances: where the controller is a public authority, where the core activities require regular and systematic monitoring of data subjects on a large scale, or where the core activities consist of processing special category data on a large scale. At current scale Noeva is not strictly required to appoint a DPO. The ICO's published view is that, given the sensitivities involved in processing children's data, organisations not strictly required to appoint a DPO should still nominate someone with clear responsibility for data protection compliance. We exceed that expectation: the Data Protection & Security Architect performs DPO-equivalent functions, and the position will be formalised as a statutory DPO at the scale milestone defined in Section 11.

Named accountabilities

Data Protection & Security Architect

POLICY OWNER · DPO-EQUIVALENT

Owns this policy end-to-end. Accountable for UK GDPR compliance, the Record of Processing Activities, the DPIA, the technical security posture, breach response, vendor risk, and the data subject rights process. The named contact for the ICO and for any data subject exercising rights. Reports to the Founder.

Child Safeguarding & Compliance Lead

JOINT REVIEW

Co-reviews this policy. Owns the children's-data overlay: ICO Children's Code conformance, parental consent design, and the children's higher protection matters obligation under DUAA s.81. Jointly accountable with the Architect for the DPIA.

Founder

FINAL SIGN-OFF

Final sign-off on this policy and every annual revision. Receives every Category-A breach notification. Holds the standing decision authority where commercial pressure and data protection are in tension — the data subject's interests prevail by default.

Strategic & Commercial Director

COMMERCIAL ALIGNMENT

Ensures pricing, growth, marketing, and partnership decisions are designed within this policy. Any campaign or partnership that introduces a new processing activity is reviewed against the policy by the Architect before launch.

All Noeva personnel

UNIVERSAL

Every person engaged by Noeva, paid or unpaid, reads this policy on day one, attests in writing that they have read it, and refreshes that attestation annually. Every person knows the process for reporting a suspected breach and is aware that no breach is too small to report.

SECTION 04 · PRINCIPLES

The seven *principles.*

Article 5 of UK GDPR sets out the seven principles that govern all processing of personal data. We do not paraphrase them. We apply them. Below: what each one means and how Noeva delivers on it.

01

Lawfulness, fairness and transparency.

Every processing activity sits on a clear lawful basis (Section 06). Privacy information is published, plainly written, and rewritten in age-appropriate form for Sparks.

02

Purpose limitation.

Data collected for one purpose is not repurposed without a fresh lawful basis. The companion is not a back door for ad-tech, market research, or model training.

03

Data minimisation.

We collect the minimum personal data necessary to deliver the companion. If we cannot articulate the product reason for a data point, we do not collect it.

04

Accuracy.

The Parent Portal lets parents correct any data point about themselves or their Spark. Inaccurate data is rectified without undue delay on request.

05

Storage limitation.

Each data category has a defined retention period in the schedule held with this policy (Section 09). Nothing is kept indefinitely without a recorded legal reason.

06

Integrity and confidentiality.

Technical and organisational measures are in place to protect personal data against unauthorised access, accidental loss, and destruction. The security floor is in Section 09.

07

Accountability.

We do not just comply. We can demonstrate that we comply. This policy, the RoPA, the DPIA, the breach log, the vendor register, and the consent records form the evidence base.

+

Children's higher protection matters.

The DUAA 2025 amendment to Article 25 requires online services likely to be accessed by children to give particular regard to children's higher protection matters. We treat this as an eighth principle in practice.

SECTION 05 · THE RECORD

What we hold *and what we don't.*

Article 30 of UK GDPR requires a written Record of Processing Activities. This section is the parent-readable summary; the full RoPA, including data flows and processors per activity, is held separately by the Data Protection & Security Architect.

What we hold about a parent

CATEGORY	PURPOSE	LAWFUL BASIS
Identity & contact	Name, email, account credentials	Performance of contract
Payment	Billing details processed by Stripe	Performance of contract
Account configuration	Subscription, preferences, parental control settings	Performance of contract
Support correspondence	Emails and messages with the Founder or support	Legitimate interest · contract
Marketing consent	Opt-in or opt-out status for non-service comms	Consent · legitimate interest
Operational logs	Sign-in events, security logs, error reports	Legitimate interest · legal obligation

What we hold about a Spark

CATEGORY	PURPOSE	LAWFUL BASIS
First name & age	To calibrate Moves and Anchors	Parental consent
Programme record	Completed Moves, Anchor engagement, progress	Parental consent
Reflect entries	The Spark's daily journal (private to the family)	Parental consent · explicit
Tune preferences	News-feed topic filters, intensity settings	Parental consent
Configuration history	Pauses, age corrections, settings changes by parent	Parental consent

What we do not hold

The data we deliberately do not collect matters as much as the data we do. We do not hold, and we do not currently intend to hold:

- → A Spark's last name, home address, or any other location data.
- → A Spark's school, year group, or any school-affiliated identifier.
- → Photographs, voice recordings, or biometric data of a Spark.
- → A Spark's contact details. The parent is the contact point.
- → Behavioural-profiling tags for advertising. We do not run advertising.
- → Any special category data (health, religion, ethnicity, sexual orientation, political opinion, trade union membership, genetic or biometric data) about a Spark — except where a Spark voluntarily references such information in a Reflect entry, in which case it is treated under the explicit-consent and additional-protection regime in Section 06.
- → A Spark's data after account closure, beyond the minimum financial and audit records required by law.

A NOTE ON REFLECT

Reflect entries are *processed locally to the family.*

The Spark's Reflect journal is the most sensitive surface in the companion. Reflect content is encrypted at rest, accessible only to the parent and (where the disclosure thresholds in the Safeguarding Policy are met) to the Child Safeguarding & Compliance Lead. Reflect content is never used to train any model, never shown to any third party, and never analysed at an individual level for product-development purposes. Aggregated, irreversibly anonymised signals — for example, that a particular Move prompts strong engagement on Reflect across the user base — may be used to improve the programme; individual entries are not.

SECTION 06 · BASES

Lawful bases *and consent.*

Every processing activity Noeva carries out is recorded against one of the six UK GDPR lawful bases — or, post-DUAA, the seventh: recognised legitimate interests. Below: which basis we use, where, and why.

Performance of contract

The primary lawful basis for processing parent personal data. The parent is the contracting party. Processing their identity, contact, payment, and account-configuration data is necessary to deliver the subscription. The contract is the user terms accepted at sign-up.

Parental consent — the basis for Spark data

The Spark is not the contracting party and is not deemed competent to consent on their own behalf to the processing involved in delivering a learning companion. The lawful basis for processing Spark data is therefore **consent**, given by the parent on the Spark's behalf at enrolment and capable of being withdrawn at any time through the Parent Portal. Consent is:

- → **Specific:** the parent consents to defined processing activities, not to a generic "we may use your child's data for stuff" clause.
- → **Informed:** the parent is given clear, plainly written privacy information before consent is collected.
- → **Freely given:** consent is not a precondition of any service we could deliver without that processing; the option not to consent is genuine.
- → **Unambiguous:** consent is captured through a clear affirmative action — a positive tick of an unticked box, not silence or inactivity.
- → **Recorded:** the date, mechanism, and content of each consent is logged and retrievable.
- → **Revocable:** withdrawing consent is as easy as giving it. A single action in the Parent Portal withdraws consent and triggers the deletion flow.

Special category data

Where a Spark's Reflect entry references information that meets the Article 9 definition of special category data — health, religious belief, sexual orientation, ethnicity, and so on — that data is processed on the basis of **explicit parental consent** obtained at enrolment, and on the further condition that the data is held under the additional technical protections set out in Section 09. The default position is that we treat any unprompted Spark disclosure as potentially special category and apply the same protections regardless of strict legal classification.

Legitimate interests

A small set of processing activities sit on the legitimate-interests basis, with the necessary balancing test recorded in the RoPA. These include security logging, fraud prevention, support correspondence, and limited service-improvement analytics conducted on pseudonymised data. The test is applied conservatively where children's data is concerned: where the balance is finely poised, we fall back to consent.

Legal obligation

A narrow set of processing activities sit on legal-obligation: retention of financial records for HMRC purposes (six years plus the current year, per the Tax Consultant's standing advice), response to lawful information requests from regulators or law enforcement, and notification of personal data breaches to the ICO.

Recognised legitimate interests

The DUAA 2025 introduced a seventh lawful basis: "recognised legitimate interests," which permits processing for a defined set of public-interest purposes (national security, safeguarding of vulnerable individuals, responding to emergencies) without the standard balancing test. Noeva does not currently rely on this basis as a routine matter; the safeguarding-related activities for which it might apply are themselves grounded in consent or legitimate interest under our current architecture. The basis is recorded here for completeness and would be used only where a clearly defined recognised-legitimate-interest situation arose.

Marketing

Marketing communications to parents — beyond service messages required to deliver the subscription — sit on consent or, in the case of existing customers, on the soft opt-in

available under PECR for products and services similar to those already purchased. Marketing communications are never sent to Sparks under any basis.

SECTION 07 · RIGHTS

Data subject *rights.*

Eight rights under UK GDPR. How a parent or Spark exercises each one, what we do, how long it takes, and the DUAA 2025 changes that apply.

> Rights are not a defensive position. They are a parent's *operational power* over the data we hold. We design the Parent Portal so most rights can be exercised in two clicks, without contacting support — that is the standard the law sets and the standard a parent expects.

THE RIGHT	HOW WE DELIVER IT
Right to be informed ARTICLES 13-14	The privacy notice published at noeva.live, in a parent version and an age-appropriate Spark version. Material processing changes trigger an updated notice and, where required, fresh consent.
Right of access ARTICLE 15 (DSAR)	A parent can request a copy of all personal data Noeva holds about them and their Spark. We respond within one calendar month of identity verification. Under the DUAA "stop the clock" rule, the response window pauses where we have reasonably requested further information from the requester and resumes when that information is supplied. We carry out "reasonable and proportionate" searches as required by the DUAA.
Right to rectification ARTICLE 16	Most rectification can be self-served through the Parent Portal. For data not editable in the portal, written request to *privacy@noeva.live* is rectified within one calendar month.

Right to erasure ARTICLE 17 · "RIGHT TO BE FORGOTTEN"	A parent can delete their account at any time through the Parent Portal. Deletion triggers a 30-day cooling-off window during which the parent can reverse the decision; after 30 days, all parent and Spark personal data is irreversibly deleted except for the minimum financial and audit records required by law. The parent receives written confirmation of completion.
Right to restrict processing ARTICLE 18	A parent can pause the companion for any duration through the Parent Portal — during pause, the underlying data is retained but processed only to the minimum extent necessary to enable resumption. Granular restriction requests beyond pause are handled within one month.
Right to data portability ARTICLE 20	A parent can export the full record of Spark progress, Reflect entries, and account data in a structured, machine-readable format (JSON) directly from the Parent Portal. No request to support is required.
Right to object ARTICLE 21	Where we rely on legitimate interests, a parent can object to that processing. Objection is handled within one month. Where the objection relates to marketing, processing stops immediately and unconditionally.
Rights relating to ADM UK GDPR ARTICLES 22A–D · DUAA 2025	Where any decision Noeva takes is based solely on automated processing and produces legal or similarly significant effects, the parent is informed, can make representations, can obtain human intervention, and can contest the decision. The detail is in Section 08.

How a parent exercises a right

- → **Self-service:** the Parent Portal handles access (download), rectification, restriction (pause), portability (export), erasure (delete), and marketing objection. Two clicks is the design target.
- → **Direct request:** *privacy@noeva.live*, monitored daily by the Data Protection & Security Architect, for any right not available in the portal.
- → **Identity verification:** we verify the requester is the account-holder before disclosing personal data. We are not entitled to ask for more than is reasonable. Excessive ID demands are a recognised anti-pattern and we avoid them.

→ **No fee:** the first request of any kind is free. Manifestly unfounded or excessive repeated requests may incur a reasonable fee or be refused — a decision recorded with reasons by the Architect.

Complaints to the ICO

Every parent has the right to complain to the Information Commissioner's Office if they believe Noeva has not handled their personal data correctly. We say so plainly in the privacy notice and provide the ICO's contact details (*ico.org.uk* · 0303 123 1113). We encourage parents to raise concerns with us first so we can put things right, but the ICO route is theirs at any point and we do not impede it.

SECTION 08 · AUTOMATION

Automated decisions *and AI.*

The DUAA 2025 rewrote Article 22 of UK GDPR. Below: what the new Articles 22A–D mean, what the model on Noeva actually does to Spark data, and the safeguards we apply.

What the law says now

Before the DUAA, Article 22 of UK GDPR gave data subjects a general right not to be subject to a decision based solely on automated processing — including profiling — that produced legal or similarly significant effects, save in narrow exceptions. Since the DUAA, the regime is set out in new Articles 22A–D. The principal changes:

- → The prior consent / contract / authorised-by-law conditions on solely automated significant decisions now apply *only* where special category personal data is involved. For other personal data, controllers may carry out such processing on any appropriate lawful basis, including legitimate interests.
- → Wherever solely automated significant decision-making takes place, mandatory safeguards apply: the data subject must be informed; must be able to make representations; must be able to obtain human intervention; and must be able to contest the decision.
- → A "significant decision" is defined and a "solely automated" process is clarified — meaningful human involvement breaks the "solely" classification.

What Noeva's AI actually does

The model on Noeva generates the four daily Moves and the three Anchors. It calibrates content to a Spark's asserted age and observed engagement. It produces curated entries in the Tune feed. It does not, at any point, take decisions that produce legal or similarly significant effects on a Spark or a parent. It does not:

- Issue qualifications, grades, certifications, or judgments that bear on a Spark's educational future.
- Decide whether a Spark is admitted to anything, eligible for anything, or excluded from anything.

- Set pricing, allocate offers, or determine commercial terms for a parent.
- Profile a Spark for advertising, content recommendation outside the programme, or third-party use.
- Process special category data for any decision-making purpose.

On the basis of this assessment, the Article 22A–D regime is not currently triggered as a routine matter on Noeva. The Architect maintains this assessment in writing and reviews it whenever the model's role changes.

Safeguards we apply anyway

Even though the strict ADM regime does not currently apply, we adopt its safeguards as good practice on the principle that any significant complaint about AI behaviour deserves a human response.

01 **Transparency.**

The privacy notice explains, in plain language, that the model generates the daily Moves and Anchors and calibrates them to a Spark's age and phase. The parent knows what the model is doing.

02 **Representation.**

A parent or Spark can flag any model output as inappropriate, inaccurate or unwelcome through the in-product report mechanism. Flagged content is reviewed within twenty-four hours by a human; see the Safeguarding Policy Section 09 for the response window.

03 **Human intervention.**

Customer support is human-led. Any parent who wants a human to review what the model has been generating for their Spark can request that review and it is performed by a named member of the team.

04 **Contestability.**

A parent who disagrees with how the model has calibrated to their Spark — content too easy, too hard, too sensitive — can override settings through the Parent Portal and the change takes effect on the next day's Moves.

Training data

Spark and parent personal data is not used to train any model — neither the model Noeva uses, nor any third-party model accessed via Noeva. This is set out contractually with each model provider as an explicit opt-out under their standard terms, and is verified at vendor onboarding and at annual review. Where a provider does not offer a contractual opt-out from training, they are not used. This is non-negotiable.

CHILDREN'S HIGHER PROTECTION MATTERS

Article 25 carries a heavier load *where a child is the data subject.*

DUAA section 81 amends Article 25 of UK GDPR to require online services likely to be accessed by children to have particular regard to children's higher protection matters when implementing data protection by design and by default. In operational terms, this means three things at Noeva. First, every default setting is the most protective for a child. Second, every product decision that creates a new processing activity touching a Spark is screened by the Child Safeguarding & Compliance Lead before deployment. Third, the DPIA explicitly tests every processing activity against children's higher protection matters and the residual risk for each is recorded. This is not a compliance exercise. It is how a service that takes its child users seriously is actually built.

SECTION 09 · THE FLOOR

Security, retention *and transfers.*

Where data lives, how long it lives, what protects it, and what happens when it crosses a border. The technical and organisational floor beneath everything above.

Security: technical and organisational measures

Noeva's security posture is owned by the Data Protection & Security Architect and is operationalised against UK GDPR Article 32 (security of processing), the OWASP Top 10, NIST Cybersecurity Framework, and ISO 27001 as the reference standard. The current baseline:

Technical

- Row Level Security enabled on every Supabase table containing parent or Spark data; RLS policy reviewed at every schema change.
- Encryption in transit (TLS 1.2 minimum) for every connection.
- Encryption at rest for all stored personal data, including Reflect entries.
- API keys rotated on a published schedule; any keys created before November 2025 audited and replaced.
- Two-factor authentication on every administrative account, the domain registrar, and any vendor admin portal.
- Security headers configured and tested against securityheaders.com and Mozilla Observatory.
- DMARC, SPF and DKIM configured on every sending domain.
- Vulnerability scanning and dependency audit at every deployment.
- Backups taken daily, encrypted, retained on a tested schedule, restorable.

Organisational

- Access to personal data is granted on the principle of least privilege and reviewed quarterly by the Architect.
- Joiner / leaver process: access granted on the first day of an engagement and revoked on the last, with documented confirmation.
- Every Noeva person reads this policy on day one and refreshes annually.
- Annual penetration test or equivalent third-party security review, scaled to the size of the user base.
- Incident response plan tested at least annually through a tabletop exercise.
- Vendor security review at onboarding and annually thereafter; right to terminate written into every contract.
- Clean-desk and secure-disposal practices for any printed material containing personal data.

Retention schedule

Each category of personal data has a defined retention period. Where the law sets a minimum, we hold to the minimum. Where the law is silent, we apply the shortest period consistent with the purpose. The schedule:

CATEGORY	RETENTION	REASON
Parent account data	Duration of subscription + 30 days	Performance of contract; reversibility window after closure.

Spark account data	Duration of subscription + 30 days	Parental consent basis; deleted on account closure.
Reflect entries	Default: duration of subscription. Configurable shorter rolling window (90 days).	Highest-sensitivity surface; default favours retention for the family's benefit, parent may shorten.
Marketing data (consent given)	Until consent withdrawn + 30 days	Consent basis; withdrawal triggers prompt deletion.
Waiting-list data	12 months from last engagement	Legitimate interest; refreshed by ongoing engagement.
Financial records	6 years + current year	Legal obligation under HMRC retention requirements (Tax Consultant standing advice).
Security & access logs	12 months	Legitimate interest in security and forensics; deleted on schedule.
Breach records	Indefinitely	Article 33(5) UK GDPR; required for accountability.
Consent records	Until consent expires + 12 months	Accountability evidence.
Support correspondence	3 years from last contact	Reasonable period for resolution and reference.

International transfers

Personal data is held in the UK or in jurisdictions designated by the Secretary of State as offering an adequate level of protection. Where a transfer is made to a third country without such designation — currently relevant for some sub-processors of our vendors — appropriate safeguards under Article 46 apply, principally the UK International Data Transfer Agreement or the UK Addendum to the EU Standard Contractual Clauses, supported by a transfer risk assessment. Under the DUAA 2025 the standard for international transfer protection has

been clarified from "essentially equivalent" to "not materially lower" than UK standards; we apply that revised test. The transfer register is held with the RoPA.

Cookies and similar technologies

Noeva's cookie posture is set out in the cookie notice at noeva.live. Strictly necessary cookies are used without consent on the basis of the PECR exemption. All other cookies — analytics, functional, and any third-party — are deployed only after explicit consent given through the cookie banner, with equal prominence to "Accept" and "Reject all." There are no advertising cookies on Noeva.

SECTION 10 · THE CHAIN

Processors, vendors *and the chain.*

Article 28 of UK GDPR governs the relationship between a controller and any third party that processes personal data on their behalf. Every vendor that touches Noeva data meets the Article 28 standard.

Noeva engages a small number of processors. Each is engaged under a written contract that meets the Article 28(3) requirements: documented processing only on Noeva's instructions; confidentiality obligations on the processor's personnel; appropriate security; sub-processor controls; assistance with data subject rights; assistance with security, breach notification and DPIA obligations; deletion or return of data at the end of the engagement; and information and audit rights.

The processor register

PROCESSOR	ROLE AND CONTROLS
Lovable PLATFORM HOST	Hosts the Noeva web application and Parent Portal. Bound by Article 28 data processing terms. The Architect maintains awareness of Lovable's published security advisories — including CVE-2025-48757 and related Supabase RLS findings — and verifies that Noeva's specific configuration is not affected. Long-term: as Noeva approaches the scale milestone in Section 11, the Architect will reassess whether continued reliance on a low-code platform host for sensitive child data remains the right architecture.

Supabase DATABASE & AUTH	Underpins data storage and authentication for the companion. RLS enabled on every table; policy reviewed by the Architect at every schema change. Article 28 terms in place. UK / EU data residency configured.
Stripe PAYMENTS	Processes parent payment data. Stripe holds full card data; Noeva does not. PCI-DSS compliance is Stripe's responsibility under the engagement; Noeva receives only the minimum required transaction metadata.
Email provider TRANSACTIONAL & MARKETING	Sends parent-facing transactional and (consent-based) marketing communications. Article 28 terms in place. List hygiene maintained by the Architect; bounces and complaints monitored.
Model provider AI CONTENT GENERATION	Generates Moves, Anchors, and the Tune feed. Spark and parent data is not used for model training under contractual opt-out. Inputs are minimised: the model sees only the personal data necessary to perform the immediate generation (age, programme state), not durable Spark identifiers.
Analytics PRODUCT QUALITY	Pseudonymous, aggregated product analytics used to monitor companion quality. No advertising SDKs. No profiling. Article 28 terms in place. Data minimisation reviewed at each integration change.

Sub-processors

Each processor's own sub-processors are recorded in the register and subject to the same Article 28 standards by contractual flow-down. Noeva is notified in advance of any proposed new sub-processor and retains the right to object.

Onboarding and review

No vendor processes Noeva personal data until: (a) an Article 28 contract is in place; (b) the Architect has completed a security and data-protection review of the vendor; (c) the vendor is added to the register and the RoPA is updated; (d) where the engagement is high-risk, a vendor-specific DPIA section has been completed. Vendors are reviewed annually thereafter, and at any material change to their service.

A NOTE ON AI PROVIDERS SPECIFICALLY

The opt-out from model training *is the entry ticket.*

A model provider that cannot or will not contractually exclude Noeva data from being used to train, fine-tune, or improve their models is not a viable processor for us. This standard is applied at first contact and is non-negotiable. The contractual position is verified annually, and any change in the provider's standard terms triggers an immediate review by the Architect.

SECTION 11 · WHEN THINGS GO WRONG

Breach response, governance *and review.*

What constitutes a breach, who finds out and when, the audit trail that proves it, and the review cycle that keeps this policy alive.

What is a personal data breach

Under Article 4(12) UK GDPR, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes the obvious — a system compromise, a database leak, a lost laptop — and the less obvious — a misdirected email containing personal data, a verbal disclosure to the wrong party, a configuration change that exposes data we expected to be private. All are breaches. The Architect is empowered to declare a breach without external sign-off.

The breach protocol

01

Detect and contain.

Any suspected breach is reported to the Architect immediately by any Noeva person, processor, or member of the public who notices it. The Architect's first action is to contain — to stop the loss, isolate the affected systems, revoke credentials, take whatever immediate step prevents further harm.

02

Assess severity.

The Architect assesses, within hours: the nature of the breach, the data categories and approximate number of data subjects affected, the likely consequences for those data subjects, and the technical and organisational measures already in place. Where Sparks are affected, the Child Safeguarding & Compliance Lead is engaged immediately.

03 **Notify the ICO.**

Where the breach is likely to result in a risk to the rights and freedoms of natural persons, the Architect notifies the ICO within 72 hours of becoming aware of it, using the ICO's online breach report. Where information is incomplete at 72 hours, an initial report is made and supplemented.

04 **Notify affected parents.**

Where the breach is likely to result in a high risk to data subjects, the affected parents are notified directly and without undue delay — in plain language, describing what happened, what data was affected, what we have done, and what they can do. We do not gild the lily.

05 **Document.**

Every breach is logged in the breach register, regardless of whether notification thresholds are met. The log is retained indefinitely and is the evidence base for our Article 33(5) accountability obligation.

06 **Review and remediate.**

Within fourteen days of a Category-A breach the Architect, the Safeguarding Lead and the Founder conduct a post-incident review. Lessons are translated into policy or control changes. The review is recorded.

The Record of Processing Activities

The RoPA, required by Article 30, is maintained by the Architect. It records, for each processing activity: the controller, the purpose, the categories of data subjects and personal data, the recipients (including processors and sub-processors), any international transfers and the safeguards applied, the retention period, and a general description of the technical and organisational security measures. The RoPA is reviewed quarterly and at every material change.

The DPIA

A Data Protection Impact Assessment, conducted under Article 35, accompanies this policy. The DPIA is mandatory in Noeva's case under the Article 35(3) criteria: processing of personal data of children at scale on the basis of new technologies (an AI model generating the daily experience). The DPIA documents data flows, identifies risks, sets out mitigations, records residual risk and the decision-maker for each, and is reviewed alongside this policy on the

annual cycle and at every material change to data processing. The Child Safeguarding & Compliance Lead is the joint signatory.

Scale milestone for formal DPO

The Architect performs DPO-equivalent functions at present. We will appoint a statutory DPO — either internal or fractional — at the earlier of (a) reaching 500 Founding Families on the companion, or (b) any material change in processing that meets the Article 37(1) mandatory-appointment threshold. The appointment process is initiated three months before either trigger.

Review cycle

- → **Scheduled review:** every twelve months. Architect drafts; Safeguarding Lead co-reviews; Founder signs off.
- → **Regulatory change:** within sixty days of an ICO guidance update, an Ofcom Codes change, or new statutory provisions affecting the regime.
- → **Material product change:** before release. Any new feature affecting personal data processing is reviewed against this policy by the Architect; the Architect can hold a release.
- → **Vendor change:** within thirty days. Architect updates the register and the RoPA.
- → **Post-breach:** within fourteen days of any Category-A breach.

Audit trail and public availability

Every revision of this policy, every RoPA update, every consent capture, every DSAR and its response, every vendor onboarding, and every breach is recorded and retained. The audit trail is held by the Architect and is available, on request, to the Founder, to the ICO, and — within applicable confidentiality limits — to a parent who has raised a concern about the handling of their own or their Spark's data. A parent-facing version of this policy and the full privacy notice are published at noeva.live and linked from every page footer.

Kate Bell

FOUNDER · FINAL SIGN-OFF

Data Protection & Security Architect

POLICY OWNER · DPO-EQUIVALENT

Child Safeguarding & Compliance Lead

JOINT REVIEW · CHILDREN'S DATA

Steve Pratt

STRATEGIC & COMMERCIAL DIRECTOR