



90-Day Remediation Roadmap

Document: **LearnSphere Horizon Privacy Notice** | Generated: 29/09/2026 | ChildSafe AI v1.2.0 | Report ID: fe6a2f4b-2a99-4304-94d3-8f0e4f9771db

● Immediate Actions (0–30 Days)

Abolish DSAR Administration Fee and Remove Age Restrictions on Rights Exercise

Under Article 12(5) UK GDPR and Children's Code Standard 15, data subject rights must be provided free of charge, and competent children cannot be categorically barred from direct rights exercise. Section 13.2-13.4 must be revised immediately to eliminate the unlawful £10 fee and allow under-16s with sufficient developmental capacity to exercise their data rights independently. Compliance is verified when all fee requirements are deleted from public terms and a zero-cost intake process is active.

Legal

Low

UK GDPR

1-7 days

Halt Ambient Acoustic and Stylus Biometric Harvesting on LearnPad Devices

Under Children's Code Standard 14 and Article 5(1)(c) UK GDPR (Data Minimisation), connected hardware deployed to children must maintain the highest privacy settings by default. Engineering must deploy an immediate firmware update disabling background classroom acoustic sensing, stylus pressure pattern logging, and reading velocity telemetry across all LearnPad units referenced in Section 14. Good looks like total suspension of ambient audio and biometric telemetry pending distinct, unbundled consent workflows.

Engineering

Low

Children's Code

1-7 days

Decommission 7pm Streak Loss Push Warnings and Compulsive Nudge Mechanics

Under Children's Code Standard 13 and Standard 5, platforms must not deploy manipulative nudge techniques or variable reward structures that induce compulsive evening platform usage in minors. Product must disable automated 7pm streak loss notifications and AI EngagementBoost triggers documented in Sections 3.2, 3.5, and 5.1 designed to inflate daily active users. Success is achieved when time-pressured streak loss warnings and gamified engagement prompts are permanently eradicated from client and push notification architectures.

Product

Medium

Children's Code

7-14 days

Suspend Analytics Consortium Data Sharing and Automated 16+ University Profiling

Pursuant to Children's Code Standards 1, 9, and 12, children's personal data cannot be shared for commercial analytics under legitimate interests, nor automatically profiled for commercial marketing pipelines. Engineering must cut Section 3.7 and Appendix A telemetry feeds to commercial analytics consortia and halt automated algorithmic sorting of 16-17 year-olds into university marketing lists under Sections 3.8 and 9.5. Good looks like the complete deactivation of external commercial feeds and algorithmic marketing filters.

 CTO

 Low

UK GDPR

 7-14 days

Finalize and Integrate Child-Specific DPIA for AI Profiling and Emotional Tracking

Section 12.1 admits that high-risk AI profiling and Wellbeing Pulse tracking operate without a finalised child assessment, breaching Article 35 UK GDPR and Children's Code Standard 2. The DPO must conduct and document a comprehensive child-specific DPIA evaluating algorithmic risks, psychological impacts, and discrimination in automated LearnerProfile scoring. Full compliance requires published, DPO-approved mitigating controls and formal sign-off before AI features can lawfully proceed.

 DPO

 High

UK GDPR

 14-30 days

● Short-term Actions (31–60 Days)

Implement Active Oversight Transparency Indicators on FamilyView Parental Dashboard

Children's Code Standard 11 requires that parental monitoring tools respect children's developmental autonomy and provide visible indicators whenever monitoring features are accessed. Product and Engineering must redesign FamilyView (Section 10.2) to trigger an immediate, age-appropriate in-app visual indicator whenever a parent inspects Wellbeing Pulse or EngagementScore telemetry. Good looks like children having clear, real-time awareness of active parental inspection, eradicating covert digital surveillance.

 Product

 Medium

Children's Code

 31-45 days

Reconfigure Account Defaults to Maximum Privacy and Enable Settings for Under-16s

Under Article 25(2) UK GDPR and Children's Code Standard 7, platform settings must default to the highest level of privacy, and minors must be empowered to control their profiles. Engineering must reconfigure all user settings so that peer visibility, PeerSpace directory indexing, and continuous profiling (Sections 7.1 and 7.3) are disabled by default while unlocking settings controls for under-16s. What good looks like is zero default public exposure and unrestricted user ability to maintain strict privacy.

 Engineering

 High

Children's Code

 31-45 days

Implement Privacy-Preserving Age Assurance and 13-14 Mini-Account Safeguards

Relying on self-declared date of birth in Section 2.1 fails statutory age assurance duties under Children's Code Standard 3 and youth safety expectations under DUAA 2025. Engineering must integrate zero-knowledge, privacy-

preserving age assurance mechanisms at onboarding and enforce restricted 'mini-accounts' with a mandatory one-hour daily usage cap for 13-14 year-olds. Good looks like robust age verification without identity data retention and automated hard limits on junior screen time.

 CTO

 High

DUAA 2025

 45-60 days

Overhaul Tracking Consent Architecture and Abolish Browwrap Cookie Mechanics

Under Regulation 6 of PECR and Article 4(11)/7 UK GDPR, tracking cookies require granular, affirmative consent rather than pre-ticked boxes or browwrap banners ('by continuing to use... you agree'). Engineering must deploy a compliant Consent Management Platform across all domains that unchecks all non-essential trackers by default and gives 'Reject All' equal visual prominence in Section 4.2. Full compliance ensures no telemetry or tracking scripts run prior to positive, explicit opt-in.

 Engineering

 Medium

UK GDPR

 45-60 days

Deploy Child-Accessible In-Platform Self-Service Rights Management Tools

In accordance with Children's Code Standard 15 and Article 12(2) UK GDPR, data controllers must actively facilitate the exercise of data subject rights through intuitive, age-appropriate interfaces. Product must build a self-service 'Privacy Hub' within student profiles enabling users to directly download, review, rectify, or request deletion of LearnerProfile telemetry and Wellbeing records. What good looks like is a one-click, child-friendly rights dashboard that renders formal legalistic requests unnecessary.

 Product

 Medium

Children's Code

 45-60 days

Ongoing Actions (61–90 Days)

Publish Age-Stratified, Multi-Layered Child Privacy Notices

Under Children's Code Standard 4 and Article 12(1) UK GDPR, privacy information directed at children must be transparent, concise, and presented in developmental, age-appropriate language. Legal must dismantle the existing legalistic text and launch a tiered transparency portal featuring bite-sized summaries, illustrated infographics for ages 13-15, and layered technical explanations for ages 16-17. Good looks like demonstrable child comprehension verified through user testing and integrated contextual help widgets.

 Legal

 Medium

Children's Code

 61-75 days

Establish Algorithmic Bias Auditing and Human Review for LearnerProfile Scores

Article 22 UK GDPR and Children's Code Standard 12 prohibit subjecting children to automated decisions or algorithmic profiling that produce discriminatory or detrimental effects on educational progression. The CTO must institute automated bias auditing pipelines and enforce mandatory human review by qualified educators before any AI-generated

LearnerProfile score impacts academic evaluations. Success is documented by quarterly bias audit logs, transparent model explainability, and logged human intervention checkpoints.

 61-75 days

Institute Recurring Best Interests of the Child Assessment (BICA) Governance

In accordance with Article 3(1) UNCRC and Children's Code Standard 1, commercial and engagement objectives must remain subordinate to the best interests of child users. The DPO must embed a mandatory BICA review stage into the platform's product development lifecycle, requiring formal risk assessment for any proposed algorithmic trigger, gamification mechanic, or sensor integration. Good looks like an institutional governance gate where no engineering sprint containing child-facing features proceeds without signed DPO clearance.

 75-90 days

Audit and Restructure Third-Party Vendor Data Processing Contracts

Articles 28 and 44-49 UK GDPR require rigorous controller oversight and statutory guarantees regarding downstream data processors handling children's data. Legal must review and renegotiate all contracts with hardware partners, cloud hosting providers, and educational research partners to contractually bar secondary analytics monetization and enforce UK adequacy mechanisms. Full compliance is attained when an active processor register is established with verified child-safeguarding audit clauses.

 75-90 days

90-Day Gantt Timeline



ACTION	d0	d7	d14	d21	d30	d45	d60	d75	d90
Publish Age-Stratified, Multi-Layered C...									
Establish Algorithmic Bias Auditing and...									
Institute Recurring Best Interests of the...									
Audit and Restructure Third-Party Ven...									

⚠️ This roadmap was auto-generated by ChildSafe AI for guidance purposes only and does not constitute legal advice. Consult a qualified DPO before implementing changes.