



ChildSafe AI Compliance Report

Document: **LearnSphere Horizon Privacy Notice** · Generated: 29/09/2026, 10:02:54

HIGH RISK

28_{/100}

The LearnSphere Horizon Privacy Notice demonstrates an acutely deficient compliance posture with an overall high-risk score of 28/100 across both domestic and European child-safety frameworks. Primary critical exposures stem from the explicit failure to complete a mandatory child-specific Data Protection Impact Assessment under the UK Children's Code, compounded by the unlawful use of engagement-driven algorithmic notifications and daily streaks restricted by the EU KIDS Act. Continued inaction carries acute regulatory urgency, leaving the organization vulnerable to formal supervisory intervention, operational disruption, and severe statutory fines from the Information Commissioner's Office and European data protection authorities. As an immediate remediation priority, the organization must suspend all gamified, engagement-nudging features and execute a comprehensive, child-centric Data Protection Impact Assessment to establish lawful processing baselines.

Framework Assessment

FINDINGS

- Section 8.1 adheres to Standard 10 by strictly avoiding the collection of precise GPS geolocation, limiting geographic inference to city-level IP lookups solely for curriculum regionalisation. Additionally, Section 11.1 implements robust technical safeguards including TLS 1.3 encryption in transit, AES-256 at rest, and annual CREST-certified penetration testing, aligning with data security principles under Standard 1.
- Section 12.1 explicitly confirms that a child-specific Data Protection Impact Assessment has not been completed, relying instead on a generic organisational DPIA despite operating large-scale AI profiling and tracking emotional wellbeing. Under Standard 2 of the Children's Code and Article 35 UK GDPR, deploying high-risk algorithmic processing and automated profiling on child users prior to concluding and documenting a dedicated child DPIA is an acute compliance failure.
- Sections 7.1 and 7.3 contravene Standard 7 by defaulting all accounts to open peer visibility, continuous AI profiling, and third-party consortium sharing, while actively barring under-16 users from modifying privacy settings. Furthermore, Sections 3.2, 3.5, and 5.1 utilise exploitative nudge techniques under Standard 13—including automated 7pm streak loss warnings and AI-calibrated notifications designed specifically to inflate commercial daily active user metrics at the expense of child wellbeing.
- Section 10.2 facilitates covert surveillance by allowing parents to inspect historical emotional Wellbeing Pulse ratings and EngagementScore trends via FamilyView without notifying the child that monitoring is active. This directly violates Standard 11, which mandates that parental oversight mechanisms must respect children's developmental autonomy and provide transparent, age-appropriate indicators whenever parental monitoring features are accessed.
- Sections 14.1 through 14.3 violate Standard 14 by deploying the LearnPad connected tablet to harvest ambient classroom acoustic levels, writing pressure patterns, and reading velocity without distinct notice, separate consent, or child opt-out mechanisms. Integrating background physical-world surveillance by default without dedicated safeguards directly contradicts the requirement that connected devices used by children maintain the highest privacy settings by default.
- Section 3.7 and Appendix A mandate the sharing of pseudonymised behavioural datasets with commercial analytics consortia under legitimate interests without opt-out rights, subordinating the best interests of the child to commercial interests in breach of Standard 1 and Standard 9. Moreover, Sections 3.8 and 9.5 apply automated profiling to route students aged 16 and over into university marketing lists without human intervention, contravening profiling restrictions set out in Standard 12.
- Sections 13.2 to 13.4 fail Standard 15 by admitting that zero in-platform self-service privacy tools exist for children, restricting rights exercise to adult-oriented written DPO requests accompanied by proof of identity and an unlawful £10 administration fee. Section 13.3 further disenfranchises children under 16 by prohibiting them from exercising data rights independently, undermining the developmental empowerment required by the ICO.
- The privacy notice is drafted entirely in complex legalistic terminology without child-tailored, bite-sized, or age-stratified explanatory layers, contravening the transparency requirements of Standard 4. Additionally, Section 4.2 relies on non-compliant pre-ticked cookie categories and browwrap consent banners ('by continuing to use... you agree'), steering children away from data privacy contrary to PECR and ICO guidance.

RECOMMENDATIONS

- Immediately complete, publish, and integrate a dedicated child-specific Data Protection Impact Assessment (DPIA) addressing AI profiling, LearnerProfile algorithms, and emotional wellbeing tracking pursuant to Children's Code Standard 2 and Article 35 UK GDPR.
- Reconfigure all platform default settings to the highest privacy level by default in accordance with Standard 7, disabling public streaks, peer group indexing, and consortium data sharing unless voluntarily activated by the user.
- Dismantle engagement-maximising nudge techniques under Standards 5 and 13, including streak loss push warnings and AI EngagementBoost triggers, aligning platform design with child wellbeing rather than commercial renewal metrics.

- Deploy child-accessible, in-platform self-service rights management tools pursuant to Standard 15 and Article 12(2) UK GDPR, removing the unlawful £10 fee and permitting under-16s with sufficient competence to exercise their rights directly.
- Redesign FamilyView parental controls under Standard 11 to introduce visible, real-time indicators when monitoring is active, and immediately disable ambient sound recording on LearnPad hardware to comply with Standard 14.

ICO CHILDREN'S CODE STANDARDS ASSESSMENT

Standard	Finding	Score
● Std 1: Best interests of the child	Subordinates children's privacy to commercial metrics by calibrating engagement algorithms for school licence renewals (Section 3.2) and sharing data with commercial consortia (Section 3.7).	30/100
● Std 2: Data protection by design and default	Violates privacy-by-default standards by enabling peer visibility, tracking, profiling, and connected device data syncing automatically upon registration (Sections 7.1 and 14.3).	25/100
● Std 3: Age appropriate application	Distinguishes age tiers (under 13, 13-15, 16+) but relies on unverified self-declared age (Section 2.1) and enforces an arbitrary barrier denying under-16s direct control of their rights.	50/100
● Std 4: Transparency	Notice provides comprehensive disclosures but lacks child-friendly formatting and uses browwrap terms stating access implies acceptance of the privacy notice (Section 1.4).	50/100
● Std 5: Detrimental use of data	Leverages behavioural data to maximise daily session lengths and screen time via EngagementBoost nudges (Sections 3.2 and 5.2), contrary to child health and wellbeing guidance.	30/100
● Std 6: Policies and community standards	Maintains clear safeguarding commitments in Section 3.4 by integrating automated risk alerts with school Designated Safeguarding Leads in compliance with KCSIE 2024.	80/100
● Std 7: Default settings	Directly breaches Standard 7 by defaulting all accounts to public peer profiles, active behavioural profiling, and push notifications with under-16s unable to change them (Sections 7.1 and 7.3).	25/100
● Std 8: Data minimisation	Collects non-essential data including ambient classroom audio (Section 14.1) and response latency, retaining profile data for 36 months after school departure (Section 6.1).	30/100
● Std 9: Data sharing	Mandates data sharing with commercial analytics consortium members and partner universities without student opt-out rights or consent (Sections 3.7, 3.8, and Appendix A).	30/100
● Std 10: Geolocation	Section 8.1 adheres to Standard 10 by strictly avoiding the collection of precise GPS geolocation, limiting geographic inference to city-level IP lookups solely for curriculum regionalisation.	85/100

Standard	Finding	Score
● Std 11: Parental controls	Section 10.2 violates requirements by allowing parents via FamilyView to covertly monitor emotional wellbeing pulse histories and activity patterns without notifying the child.	35/100
● Std 12: Profiling	Profiling is switched on by default (Section 7.1), cannot be disabled without severe service degradation (Section 9.4), and is used to drive targeted university outreach (Section 3.8).	25/100
● Std 13: Nudge techniques	Deploys gamified streak warnings and AI-calibrated EngagementBoost notifications designed to manipulate children into maintaining daily platform use (Sections 3.5 and 5.2).	25/100
● Std 14: Connected toys and devices	Section 14.2 enables automatic syncing of LearnPad device telemetry and ambient audio without separate consent, child notification, or student controls to disable sync.	30/100
● Std 15: Online tools	Provides no in-platform self-service tools for children to exercise rights (Section 13.4) and unlawfully restricts under-16s from submitting requests directly (Section 13.3).	30/100

FINDINGS

- Section 3.4 integrates automated risk detection within Wellbeing Pulse entries and PeerSpace communications that proactively escalates potential harm to school Designated Safeguarding Leads under statutory frameworks. This mechanism aligns with the positive duty under Criterion 9 to actively prevent child harm and provide structured intervention pathways.
- Sections 3.2, 3.5, and 5.1-5.2 employ engagement-driven algorithmic notifications, daily login streaks, and automated 7pm loss warnings designed explicitly to maximise daily active users for commercial licence renewal. These mechanisms directly breach Criterion 4, which strictly prohibits variable reward systems, gamified streaks, and engagement triggers engineered to induce compulsive use in minors.
- Section 2.1 relies entirely on self-declared date of birth for registration and grants unverified independent accounts to children aged 13 and over. This contravenes Criteria 3 and 7, which explicitly rule out self-declaration, mandate privacy-preserving age assurance, and require restricted 'mini-accounts' with a mandatory one-hour daily screen-time cap for ages 13–14.
- Sections 3.1, 7.1, and 9.3 mandate algorithmic content recommendations, social visibility, and persistent LearnerProfile tracking by default, denying students the ability to opt out without forfeiting core platform access. This directly violates Criterion 6 and Criterion 8, which forbid default algorithmic personalisation for under-18s and require strictly opt-in profiling.
- Section 12.1 admits that high-risk AI profiling and emotional tracking are deployed while a child-specific Data Protection Impact Assessment is still 'in preparation' and only a general organisational assessment exists. This constitutes an immediate failure of Criteria 1, 2, and 5, which make ex-ante Child Safety Assessments and documented safety-by-design conformity an absolute legal prerequisite before live deployment.
- Section 10.2 enables covert parental surveillance via the FamilyView dashboard, allowing guardians to inspect sensitive Wellbeing Pulse emotional histories and EngagementScores without notifying the child. This design undermines the child's right to digital privacy and fails to provide age-appropriate transparency or transparency indicators to the minor.
- Section 14.1-14.3 mandates default ambient sound capture, stylus pressure biometric logging, and reading speed tracking via LearnPad hardware without explicit consent or individual disabling controls. This non-essential sensor data harvesting infringes data minimisation principles and defaults-by-design obligations under Criterion 8.
- Sections 3.7, 3.8, and 9.5 automatically profile students aged 16-17 for university recruitment without prior human review and share behavioural telemetry with a commercial analytics consortium under legitimate interests. This practice conflicts with Criterion 4 and 6 safeguards against commercial profiling and exploitative algorithmic sorting of minors.

RECOMMENDATIONS

- Complete and publish an ex-ante Child Safety Assessment (CSA) and risk conformity audit evaluating algorithmic profiling, emotional data processing, and child harm risks in accordance with EU KIDS Act (COM(2026) 681) Articles 1, 2, and 5.
- Eliminate prohibited addictive design features under COM(2026) 681 Article 4, specifically decommissioning daily login streaks, automated streak-loss warning notifications, and AI-timed EngagementBoost triggers.
- Implement zero-knowledge privacy-preserving age assurance under Article 7 to replace self-declared age, enforcing managed mini-accounts with an automated one-hour daily screen-time cap for users aged 13-14.
- Reconfigure all platform default settings to privacy-protective states under Article 8, ensuring AI-driven content feeds, PeerSpace directory visibility, and Consortium data sharing are strictly opt-in rather than pre-enabled.
- Deactivate ambient sound detection and unconsented hardware telemetry in the LearnPad integration (Section 14) to uphold statutory data minimisation and eliminate covert monitoring practices.

⚠️ **Legal Disclaimer:** This report is generated by AI for guidance purposes only and does not constitute legal advice. It must not be used as a substitute for assessment by a qualified data protection solicitor or registered DPO. Any decisions taken on the basis of this report must be reviewed and signed off by a competent professional.

Framework versions assessed: childrenscore · eukidsact.

Framework criteria last reviewed: August 2026. Regulatory frameworks are subject to change. Always verify analysis against the most current published guidance from the ICO, Ofcom, DfE and European Commission before taking compliance action.

⚠️ **Emerging regulation — ICO EdTech Code:** The ICO published its 'EdTech Examined' report on 24 June 2026, following audits of 28 EdTech providers which identified 596 compliance recommendations. The ICO is now working with the Department for Education and devolved authorities on a new EdTech Code of Practice. Once enacted, this will introduce mandatory compliance requirements for EdTech providers. UK GDPR criteria in this report already incorporate the ICO's EdTech Examined findings. Monitor ico.org.uk for code development updates.