



Child Rights Impact Assessment (CRIA)

Subject: **LearnSphere Horizon Privacy Notice** · Assessed by: ChildSafe AI · Framework: UNCRC General Comment No. 25 (2021)

Assessment date: 29/09/2026 · Review due: 29/09/2027

OVERALL ASSESSMENT · UNCRC GENERAL COMMENT NO. 25

● **28/100 — RED — Non-Compliant**

Suspend pending remediation

LearnSphere Horizon fundamentally fails to align with General Comment No. 25 by subordinating the best interests, privacy, and developmental autonomy of child users to commercial engagement metrics and unchecked algorithmic processing. The systemic absence of a dedicated Child Rights Impact Assessment and child-tailored transparency mechanisms violates core obligations to safeguard minors in the digital environment. Pervasive commercial profiling, gamified retention nudges, and covert monitoring establish an environment characterized by systemic rights infringement rather than digital empowerment.

Article-by-Article Assessment

ARTICLE 2 · GC NO. 25

● **Non-discrimination**

25%

The platform provides no evidence of ex-ante algorithmic bias testing or fairness audits across its automated LearnerProfile and AI profiling systems, creating severe discriminatory risks for neurodivergent and SEND pupils. Profiling mechanisms such as writing pressure logging and reading velocity tracking inherently penalize children with physical or cognitive impairments without reasonable adjustments. Furthermore, automated sorting of older pupils into university marketing streams risks entrenching socioeconomic sorting without safeguards against algorithmic bias.

MITIGATIONS

- Conduct mandatory ex-ante algorithmic fairness and bias audits specifically evaluating impacts on SEND and neurodivergent pupils.
- Immediately cease the passive biometric capture of writing pressure and reading velocity that pathologizes atypical learning patterns.
- Implement human oversight and accessibility adjustments within all algorithmic routing, assessment, and classification algorithms.

ARTICLE 3 · GC NO. 25

20%

● Best Interests of the Child

Commercial objectives and platform engagement metrics are systematically prioritized over the best interests of child users, violating GC No. 25 paragraph 12. Deploying live high-risk algorithmic profiling and Wellbeing Pulse emotional tracking while operating without an ex-ante child-specific DPIA demonstrates an acute disregard for child welfare. Furthermore, Section 3.7 and Appendix A mandate non-consensual commercial consortium data sharing under legitimate interests, directly subordinating child rights to commercial revenue streams.

MITIGATIONS

- Complete and publish a dedicated child-specific Data Protection Impact Assessment prior to any further deployment of AI profiling.
- Halt all data sharing with commercial analytics consortia and eliminate reliance on legitimate interests for commercial processing of child data.
- Establish an institutional Best Interests Determination procedure embedded into platform governance and product change cycles.

ARTICLE 6 · GC NO. 25

● Right to Life, Survival and Development

26%

The deliberate deployment of persuasive design techniques—including daily login streaks, automated 7pm loss warnings, and AI-calibrated notifications—infringes upon children's holistic physical, mental, and emotional development. These gamified retention triggers are engineered to induce compulsive screen-time habits and evening platform engagement at the direct expense of healthy sleep patterns and restorative rest. In contrast to the positive escalation of safeguarding alerts via Section 3.4, the platform's overarching behavioral mechanics actively exploit developmental vulnerabilities for platform stickiness.

MITIGATIONS

- Eliminate all variable reward schedules, gamified daily streaks, and punitive loss-notification triggers across all age brackets.
- Implement automated hard screen-time boundaries and default night-time quiet hours (no notifications between 7pm and 8am).
- Introduce child-friendly digital wellbeing dashboards offering friction prompts to encourage healthy disengagement.

ARTICLE 8 · GC NO. 25

● Right to Identity and Privacy of Digital Identity

30%

Persistent LearnerProfile telemetry and behavioural profiling construct non-consensual algorithmic identities that follow students across their educational careers without their consent or remediation rights. Unverified date-of-birth self-declaration compromises identity integrity, while the absence of privacy-preserving age assurance leaves children under 16 subject to commercial data capture. Children are denied the agency to alter, contest, or separate their authentic identity from commercialized and algorithmic platform reputations.

MITIGATIONS

- Implement privacy-preserving, non-invasive age assurance mechanisms that avoid identity over-collection while verifying developmental thresholds.
- Grant children the unconditional right to reset, decouple, or delete behavioural LearnerProfile telemetry and algorithmic personas.
- Prohibit the persistent longitudinal aggregation of academic, behavioural, and biometric performance across academic years.

ARTICLE 12 · GC NO. 25

● Right to Be Heard and Participate

18%

The platform completely suppresses children's agency and participation by explicitly forbidding users under 16 from modifying privacy settings or exercising data subject rights. Rectification, erasure, and access rights are locked behind adult-oriented legalistic barriers, including mandatory identity documentation and an unlawful £10 fee, disenfranchising the child's evolving capacities. The total absence of student feedback loops or representation in platform governance violates the core mandate of GC No. 25 regarding children's digital participation.

MITIGATIONS

- Introduce intuitive, age-appropriate, in-app self-service privacy controls enabling children to configure their settings and exercise data rights.
- Abolish unlawful administrative fees and bureaucratic identity verification hurdles for rights requests submitted by or on behalf of children.
- Establish a standing Youth Advisory Board to review platform features, terms, and privacy interfaces on an ongoing basis.

ARTICLE 13 · GC NO. 25

● Freedom of Expression and Information

42%

While PeerSpace technically affords collaborative communication opportunities, mandatory algorithmic content recommendation and persistent profiling constrain children's autonomous exploration and diversity of expression. Children cannot opt out of algorithmic personalization or social visibility defaults without sacrificing fundamental access to mandatory educational resources. This creates an echo-chamber effect that shapes their informational access based on automated tracking rather than autonomous intellectual inquiry.

MITIGATIONS

- Provide an accessible, single-click toggle for a strictly non-personalized, chronological view across all educational feeds and PeerSpace forums.
- Ensure full access to core educational content and curriculum materials remains unaffected if a pupil disables social tracking and profiling.
- Publish transparent, child-comprehensible explanations of how educational algorithms curate and prioritize learning resources.

● Right to Privacy

Section 10.2 facilitates unlawful covert surveillance by permitting guardians to secretly inspect historical Wellbeing Pulse ratings and EngagementScore metrics without child notification. Privacy is further eroded by Section 14 LearnPad hardware harvesting ambient classroom audio, stylus pressure biometrics, and reading velocity by default without consent or toggles. Default-open visibility and commercial tracking consortia partnerships fundamentally compromise the private digital sphere protected by Article 16.

MITIGATIONS

- Implement clear, real-time, age-appropriate visual transparency indicators whenever parental FamilyView monitoring is active.
- Disable all hardware sensor collection (ambient acoustic levels, stylus pressure, reading velocity) by default, requiring explicit opt-in.
- Configure all child accounts to the highest privacy settings by default, restricting peer visibility and external data flows.

● Access to Appropriate Information

The privacy notice violates Article 17 and GC No. 25 transparency standards by relying exclusively on dense legalistic text with zero age-stratified or multimodal explanatory layers. The service steers children into privacy-invasive defaults through manipulative browwrap consent notices and pre-ticked cookie categories in violation of basic transparency duties. Children are deprived of accessible information necessary to make informed developmental choices about their personal data and rights.

MITIGATIONS

- Draft and publish layered, child-friendly privacy notices using plain language, infographics, and short explanatory video summaries for distinct age cohorts.
- Dismantle browwrap banners and pre-ticked tracking cookies, replacing them with granular, unbiased privacy choices.
- Deploy in-context, just-in-time privacy prompts whenever sensitive data or emotional wellbeing tracking is initiated.

● Protection from Violence, Abuse and Exploitation

Section 3.4 demonstrates positive harm-prevention through automated escalation of severe safeguarding risks to school Designated Safeguarding Leads. However, this protective mechanism is severely counteracted by structural commercial exploitation, including automated routing of 16-17 year-olds into university marketing funnels and commercial data sharing. Furthermore, default public peer visibility on PeerSpace exposes child users to peer abuse, harassment, and unauthorized contact without adequate boundary controls.

MITIGATIONS

- Immediately terminate all automated commercial profiling and third-party recruitment pipelines targeting 16-17 year-old pupils.
- Enforce strict default-closed privacy settings on PeerSpace, ensuring peer interaction is limited to vetted classroom groups.
- Strengthen the Designated Safeguarding Lead workflow with independent human-in-the-loop oversight to avoid false positives and discriminatory intervention.

👥 STAKEHOLDER CONSULTATION ASSESSMENT

There is zero documented evidence of participatory consultation or co-design with children, parents, or pedagogical experts regarding data processing, algorithmic nudges, or platform interface governance. Children are entirely disenfranchised from governance, actively barred under age 16 from configuring privacy settings or independently exercising basic data protection rights.

Generated by **ChildSafe AI** · childdsafe-ai.privacomply.co.uk

This CRIA requires review by a qualified professional before formal use.

UNCRC: ohchr.org · GC No. 25: [Download PDF](#)