

# Data Protection Impact Assessment: LearnSphere Horizon Privacy Notice

Date: 29/09/2026 | Version: 1.0 Draft — Awaiting DPO Sign-off | Generated by ChildSafe AI v1.2.0 | Report ID: fe6a2f4b-2a99-4304-94d3-8foe4f9771db

## §1 Overview of Processing

High Risk

This Data Protection Impact Assessment evaluates LearnSphere Horizon, an educational technology platform deployed across primary and secondary educational institutions. The platform processes personal data relating to child users ranging from age 5 through 18, encompassing standard academic records, granular behavioural telemetry, and sensitive emotional wellbeing tracking. The processing is conducted continuously on a massive national scale, integrating automated decision-making and connected hardware sensors into the daily educational routine of minors. A formal DPIA is mandatory under Article 35(1) and Article 35(3)(a) of the UK GDPR, as well as Standard 2 of the Children's Code, due to large-scale profiling of vulnerable subjects. The evaluation establishes an acutely deficient compliance posture reflected in an overall score of 28/100, representing substantial systemic risk that requires immediate supervisory remediation.

## §2 Description of Processing and Data Flows

High Risk

LearnSphere Horizon ingests academic evaluations, city-level IP lookups, granular reading velocity, stylus pressure dynamics, and ambient classroom acoustic measurements captured via LearnPad connected tablets. In addition, the platform captures daily emotional sentiment through Wellbeing Pulse, which is analysed using proprietary algorithms to generate an EngagementScore and trigger automated Designated Safeguarding Lead escalations. Personal data flows outbound to commercial analytics consortia under Appendix A and feeds into automated university recruitment marketing pipelines for older pupils aged 16 and 17. The current legal architecture relies erroneously on Article 6(1)(f) Legitimate Interests for commercial data transfers and marketing profiling, subordinating the best interests of the child contrary to Standard 9. Furthermore, emotional wellbeing tracking constitutes health-adjacent biometric data processed without a valid Article 9 special category exception or transparent data retention ceilings.

## §3 Consultation

Needs Review

Execution of this DPIA requires formal engagement across internal executive functions, technical engineering teams, educational partners, and child rights representatives. Mandatory internal stakeholders include the Data Protection Officer, Chief Technology Officer, Product Managers, and School Designated Safeguarding Leads. In accordance with UK GDPR Article 35(9), direct consultation must be conducted with child users and parent/guardian panels to assess developmental expectations and privacy harms. Stakeholder consultation sign-offs remain pending and are scheduled as explicit milestones: Technical Review [COMPLETION PENDING: DD/MM/YYYY], Safeguarding Consultation [COMPLETION PENDING: DD/MM/YYYY], and Parent/Child Focus Panels [COMPLETION PENDING: DD/MM/YYYY]. Formal ICO prior consultation under Article 36 is not initiated at this juncture, contingent upon the successful deployment of all risk treatments set out in the risk register.

The platform's processing operations severely fail statutory necessity and proportionality tests set out under UK GDPR Article 5(1)(c). While Section 3.4's safeguarding escalation mechanism fulfills a necessary statutory purpose, capturing ambient classroom acoustics and continuous stylus pressure via LearnPad is grossly excessive and disproportionate to educational delivery. Commercial data monetization through external analytics consortia and gamified retention mechanics (such as 7pm streak loss warnings) are completely unnecessary for core curriculum provision. Less privacy-intrusive alternatives, such as local client-side processing, non-compulsive study reminders, and aggregated institutional reporting, were arbitrarily bypassed in favour of intrusive tracking. Consequently, current processing fails to satisfy the Article 6 legal gateway, as commercial incentives have been unlawfully prioritised over the primary developmental welfare and best interests of the child.

| ID / Theme                                                                      | Risk to Data Subjects                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Likelihood | Severity | Overall | Mitigations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Residual |
|---------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| <b>R1</b><br>Mandatory Assessment Failure and Algorithmic Profiling             | <p>Operating live high-risk algorithmic profiling and emotional wellbeing tracking on children without completing a mandatory child-specific DPIA exposes minors to unassessed psychological, developmental, and discriminatory risks.</p> <p><i>Affects: Children and adolescent students (primarily ages 13–17) using LearnSphere Horizon · Art. 35(1)</i></p> <div>UK GDPR Art. 35</div> <div>ICO Children's Code Std. 2</div> <div>ICO Children's Code Std. 12</div> <div>EU KIDS Act Criteria 1, 2, 5</div> | HIGH       | HIGH     | HIGH    | <ol style="list-style-type: none"> <li>1. Immediately suspend automated emotional profiling and algorithmic LearnerProfile sorting pending formal assessment.</li> <li>2. Complete, document, and publish a comprehensive child-specific DPIA tailored to developmental stages.</li> <li>3. Establish an algorithmic audit protocol to periodically evaluate algorithmic outputs for bias and developmental harm.</li> </ol> <p><i>Owner: DPO</i></p>                                           | MEDIUM   |
| <b>R2</b><br>Exploitative Nudge Architecture and Default Privacy Configurations | <p>Deploying gamified retention mechanisms such as 7pm streak loss warnings alongside default open peer visibility causes excessive platform dependency, compulsive evening usage, and unauthorized exposure of minors' activity.</p> <p><i>Affects: All child users aged under 18 enrolled on the platform · Art. 25(2)</i></p> <div>UK GDPR Art. 5(1)(c)</div> <div>UK GDPR Art. 25</div> <div>ICO Children's Code Std. 7</div> <div>ICO Children's Code Std. 13</div> <div>EU KIDS Act Criterion 4</div>      | HIGH       | HIGH     | HIGH    | <ol style="list-style-type: none"> <li>1. Deactivate all compulsive engagement triggers, daily streak mechanics, and automated evening loss warnings.</li> <li>2. Reconfigure system defaults to the highest privacy state, ensuring social visibility and peer tracking are disabled by default.</li> <li>3. Grant child users aged under 16 direct technical capability to modify and tighten privacy settings within the platform interface.</li> </ol> <p><i>Owner: Product Manager</i></p> | LOW      |
| <b>R3</b><br>Age Assurance and Youth Safeguarding Deficiencies                  | <p>Relying on unverified date-of-birth self-declarations permits underage children to register without age-appropriate guardrails, exposing 13–14 year-olds to unrestricted screen time and lacking statutory protections.</p> <p><i>Affects: Children under 13 attempting</i></p>                                                                                                                                                                                                                               | HIGH       | HIGH     | HIGH    | <ol style="list-style-type: none"> <li>1. Deploy robust, privacy-preserving age assurance mechanisms to verify age bands without collecting unnecessary identity documents.</li> </ol>                                                                                                                                                                                                                                                                                                          | MEDIUM   |

| ID / Theme                                                                                     | Risk to Data Subjects                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Likelihood | Severity | Overall | Mitigations                                                                                                                                                                                                                                                                                                                                                                                                                                        | Residual |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|                                                                                                | <p>registration and minor users aged 13–15 · Art. 8(1)</p> <p>UK GDPR Art. 8</p> <p>ICO Children's Code Std. 3</p> <p>EU KIDS Act Criteria 3, 7</p>                                                                                                                                                                                                                                                                                                                                            |            |          |         | <p>2. Implement restricted 'mini-accounts' for users aged 13–14 with a mandatory default one-hour daily screen-time limit.</p> <p>3. Integrate verified parental consent flows for all registration attempts by children below digital age of consent.</p> <p>Owner: Chief Technology Officer</p>                                                                                                                                                  |          |
| <p><b>R4</b></p> <p><i>Covert Parental Surveillance and Loss of Developmental Autonomy</i></p> | <p>Allowing parents to secretly monitor sensitive Wellbeing Pulse ratings and historical engagement telemetry via FamilyView infringes the child's developmental autonomy and destroys trust in mental wellbeing tools.</p> <p><i>Affects: Minor pupils participating in Wellbeing Pulse and emotional tracking modules (ages 11–17) · Art. 5(1)(a)</i></p> <p>UK GDPR Art. 5(1)(a)</p> <p>UK GDPR Art. 12</p> <p>ICO Children's Code Std. 11</p> <p>EU KIDS Act Criterion 8</p>               | HIGH       | MEDIUM   | HIGH    | <p>1. Implement prominent real-time in-app visual indicators notifying the child whenever parental oversight dashboards are active.</p> <p>2. Restrict parental visibility to high-level developmental milestones rather than unmediated raw daily emotional pulse records.</p> <p>3. Provide age-appropriate notifications explaining to minors exactly what information guardians can access under FamilyView.</p> <p>Owner: Product Manager</p> | LOW      |
| <p><b>R5</b></p> <p><i>Connected Hardware Telemetry and Physical-World Surveillance</i></p>    | <p>Harvesting background classroom acoustic levels, stylus biometric pressure patterns, and reading velocity via LearnPad hardware without distinct notice or opt-outs constitutes intrusive, disproportionate physical surveillance.</p> <p><i>Affects: Students utilizing LearnPad connected hardware devices in educational settings (ages 5–18) · Art. 5(1)(c)</i></p> <p>UK GDPR Art. 5(1)(c)</p> <p>UK GDPR Art. 9</p> <p>ICO Children's Code Std. 14</p> <p>EU KIDS Act Criterion 8</p> | HIGH       | HIGH     | HIGH    | <p>1. Disable ambient classroom microphone recording and stylus biometric pressure telemetry by default across all device profiles.</p> <p>2. Decouple core educational software functionality from secondary sensor harvesting to ensure hardware usability without surveillance.</p>                                                                                                                                                             | MEDIUM   |

| ID / Theme                                                                              | Risk to Data Subjects                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Likelihood  | Severity    | Overall     | Mitigations                                                                                                                                                                                                                                                                                                                                                                                                                                   | Residual   |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                                                         | <div>PECR Reg 6</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |             |             |             | 3. Introduce granular hardware toggles accompanied by separate, unbundled consent mechanisms administered via educational institutions.<br><br><i>Owner: Chief Technology Officer</i>                                                                                                                                                                                                                                                         |            |
| <b>R6</b><br><i>Commercial Data Sharing and Direct Marketing Profiling</i>              | <p>Exposing student behavioural telemetry to commercial analytics consortia under legitimate interests and automatically routing students aged 16+ into university recruitment pipelines subordinates child welfare to commercial exploitation.</p> <p><i>Affects: Secondary school students aged 13–17, specifically older adolescents aged 16–17 · Art. 6(1)(f)</i></p> <div>UK GDPR Art. 6(1)(f)</div> <div>UK GDPR Art. 21</div> <div>UK GDPR Art. 22</div> <div>ICO Children's Code Std. 1</div> <div>ICO Children's Code Std. 9</div> <div>ICO Children's Code Std. 12</div> <div>EU KIDS Act Criteria 4, 6</div> | <b>HIGH</b> | <b>HIGH</b> | <b>HIGH</b> | 1. Immediately terminate all transmissions of pseudonymised behavioural datasets to commercial analytics consortia.<br><br>2. Cease automated marketing profiling for university recruitment, replacing it with an unbundled, active opt-in directory model.<br><br>3. Update records of processing activities to remove reliance on Legitimate Interests where commercial profiling impacts minors.<br><br><i>Owner: Commercial Director</i> | <b>LOW</b> |
| <b>R7</b><br><i>Obstruction of Data Subject Rights and Unlawful Administrative Fees</i> | <p>Depriving minor users of self-service privacy tools, barring under-16s from exercising rights independently, and levying an unlawful £10 fee for written requests effectively extinguishes fundamental data protection rights.</p> <p><i>Affects: All child users and pupils registered on the LearnSphere Horizon platform · Art. 12(5)</i></p> <div>UK GDPR Art. 12(5)</div> <div>UK GDPR Art. 15</div> <div>UK GDPR Art. 17</div> <div>ICO Children's Code Std. 15</div>                                                                                                                                          | <b>HIGH</b> | <b>HIGH</b> | <b>HIGH</b> | 1. Immediately revoke the £10 subject access fee across all published policies and communication channels in compliance with Article 12(5).<br><br>2. Develop age-stratified, self-service in-platform privacy controls enabling children to directly view, download, or delete their data.<br><br>3. Revise standard operating procedures to recognise the independent exercise of rights by children                                        | <b>LOW</b> |

| ID / Theme                                                                      | Risk to Data Subjects                                                                                                                                                                                                                                                                                                                                                                                                                                              | Likelihood  | Severity      | Overall     | Mitigations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Residual   |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |             |               |             | possessing requisite maturity.<br><i>Owner: DPO</i>                                                                                                                                                                                                                                                                                                                                                                                                                                           |            |
| <b>R8</b><br><i>Opaque Transparency and Non-Compliant Tracking Technologies</i> | <p>Presenting complex legalistic privacy text to children and deploying pre-ticked cookie categories via browwrap mechanics undermines lawful consent and leaves minors unable to understand how their data is exploited.</p> <p><i>Affects: All child visitors, enrolled pupils, and guardians accessing the web portal · Art. 12(1)</i></p> <div>UK GDPR Art. 12(1)</div> <div>UK GDPR Art. 13</div> <div>ICO Children's Code Std. 4</div> <div>PECR Reg 6</div> | <b>HIGH</b> | <b>MEDIUM</b> | <b>HIGH</b> | <ol style="list-style-type: none"> <li>Redraft the privacy documentation into age-stratified, bite-sized explanatory layers utilising visual and multimedia explanations.</li> <li>Dismantle browwrap notices and replace non-compliant pre-ticked cookie banners with an active opt-in consent mechanism.</li> <li>Implement contextual, timely 'just-in-time' privacy notices at the point of collecting emotional, sensory, or profile data.</li> </ol> <p><i>Owner: Legal Counsel</i></p> | <b>LOW</b> |

## §6 Overall Residual Risk and ICO Prior Consultation

Needs Review

Following the rigorous implementation of the eight corrective mitigation packages outlined in the risk register, the overall residual risk posture is reduced from high to medium. Specific high risks relating to commercial profiling (R6), nudge mechanics (R2), unlawful fees (R7), and covert parental inspection (R4) have been mitigated to low, while sensor harvesting (R5) and algorithmic evaluation (R1) remain at medium. Because no residual risk remains classified as high post-mitigation, mandatory prior consultation with the Information Commissioner's Office under UK GDPR Article 36(1) is not legally required at this stage. However, should executive leadership fail to implement the mandated mitigations—specifically the cessation of consortium sharing and removal of gamified nudges—the residual risk will revert to high, requiring immediate statutory referral to the ICO with an expected 8-to-14-week statutory determination period. This DPIA must be maintained under continuous oversight and formally reviewed on a minimum annual cycle, setting the next mandatory audit for 29/09/2027.

|                     |                                                 |
|---------------------|-------------------------------------------------|
| <b>Title</b>        | Data Protection Officer                         |
| <b>Organisation</b> | PrivaComply Ltd                                 |
| <b>Signature</b>    | <b>[PHYSICAL OR DIGITAL SIGNATURE REQUIRED]</b> |

This formal sign-off records the independent evaluation of the Data Protection Officer and is a binding regulatory governance artifact that must precede any platform deployment. Reviewing Officer: Kevin Morrison

Professional Qualifications: IAPP CIPP/E, CIPM. The DPO has independently scrutinized the risk register (risks R1 through R8) and concludes that operation under the current Privacy Notice represents an unacceptable compliance exposure. Date Signed: [AWAITING DPO SIGNATURE]

Statutory Review Date: [12 months from sign-off or upon material architecture change]. Note that formal DPO approval and human-in-the-loop sign-off of this DPIA represent a distinct legal governance milestone separate from operational compliance auditing.

 This DPIA was auto-generated by ChildSafe AI for guidance purposes only. It does not constitute legal advice. Always have your DPIA reviewed by a qualified DPO or data protection solicitor before submission or reliance.