Key Risks and Mitigations

Trellis · Based on DPIA v2.8 and Security Overview v2.3 · October 2026

Risk register

Scoring (Trellis DPIA v2.8): Likelihood (1–5) × Severity (1–5). 1–3 Low; 4–6 Medium; 7+ High.

Residuals below are after mitigation. Trellis's DPIA assesses all residual risks as 6 or below. These are Trellis's residual assessments; each controller should consider and accept residual risk in its own DPIA.

Risk	Category	Key mitigations	Residual (L×S)
Inaccurate / poorly worded draft misrepresents a child's needs	Accuracy / Fairness	Human-in-Command review; in-app editing; schema validation; training; two-monthly ML evaluation	**1 × 4 = 4**
Speaker mis-attribution discloses or misrecords a remark	Accuracy	Teacher review of transcript/draft; no auto-send to families; Azure Speech diarisation; training guidance	**1 × 4 = 4**
Unauthorised access via compromised login	Confidentiality	Entra MFA (Trellis tenant) / controller MFA policy if federated; WAF security controls + UK geo-restriction; RLS; least privilege; audit log	**1 × 4 = 4**
Social-engineering credential compromise (controller side)	Confidentiality	MFA; WAF security controls; least-privilege RBAC; SSO federation; Trellis recommends controller phishing awareness	**1 × 4 = 4**
Personal data kept longer than controller allows	Storage limitation	Configurable retention (default 60 days); PII expiry; continuous scrub; API filters expired data; deletion logged; quarterly scrub review / alerts	**1 × 3 = 3**
Function creep beyond original scope	Purpose limitation	DPA/DPIA scope; document types enabled per controller; no integrations without request; mandatory DPIA + controller sign-off on purpose change	**2 × 3 = 6**
Bias / discriminatory wording in AI output	Fairness / Accuracy	Two-monthly evaluation; Teacher Strategy Group; diverse samples; teacher awareness; no fine-tuning; escalate systematic patterns before promotion	**1 × 4 = 4**
Parent objects: not properly informed about recording	Transparency	Transparency statement at start of recording; controller can pause/cancel on objection; accessible explainer in development	**1 × 2 = 2**
Service outage delays plan creation	Availability	Revert to manual drafting; zone-redundant gateway/containers; Azure SLAs; retries; HA roadmap for DB/broker	**2 × 2 = 4**

Risk	Category	Key mitigations	Residual (L×S)
Sub-processor (e.g. Microsoft) breach exposes data	Confidentiality / Integrity	Azure compliance; **client-side audio encryption**; private endpoints; Microsoft DPA 72-hour Security Incident notification	**1 × 5 = 5**
Trellis staff recognises someone during evaluation	Confidentiality	≤5 named BPSS-vetted staff; need-to-see; MFA + audited access; geographic distance; recusal policy	**1 × 2 = 2**
Staff (user) data in audit logs over-retained or misused	Storage / Confidentiality	Dedicated write-only audit role; no meeting content; used only for security/accountability/support; 7-year retention documented in DPA	**1 × 2 = 2**
Management Panel small numbers re-identify staff users	Purpose / Fairness	Access control; controller policy/training; Trellis docs: metrics for system management, not individual performance management	**3 × 2 = 6**

Full narrative and initial scores: Trellis DPIA v2.8, Step 6.