DPIA Summary

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

1. What Trellis is

Trellis is an AI scribe for SEND/ASN administration. A teacher records a relevant meeting in the Trellis web app or native iPad app. Trellis transcribes the recording with Microsoft Azure Speech, then drafts plans and minutes with Azure OpenAI from the transcript and any further inputs the teacher provides (for example pastoral notes, or student and parent views). The teacher reviews and edits every draft before it is used. **Trellis makes no decisions about any child.**

2. Why a DPIA is needed

Trellis processes special category data about children with additional support needs (including health-related and pastoral notes), and it uses generative AI. Under UK GDPR, that combination means a Data Protection Impact Assessment is appropriate. Trellis, as processor, maintains a full DPIA to support each controller. The trust or school, as controller, should still decide why it needs its own DPIA and complete one.

3. Roles

Party	Role
Trust / school (or local authority)	**Data controller** – decides purpose, lawful basis, privacy notices, and staff policy
Trellis Education Ltd	**Data processor** – processes only on the controller's documented instructions
Microsoft (Azure)	Sub-processor – hosts the service pipeline and processes children's data in the UK

4. What data is processed

Children's data (includes special category under Article 9): names, support needs, health-related notes, pastoral notes, and recordings of Team Around the Child and equivalent meetings, plus transcripts and generated drafts.

User (teacher/staff) data (ordinary personal data): name, work email, school and organisation, Entra identity identifiers, and operational records (activity and audit logs, error logs, survey and feedback responses). This is treated separately from children's data throughout Trellis's DPIA and DPA.

Children are not direct users. Teachers and staff enter and use the data on behalf of the controller.

5. Lawful basis

Trellis does not decide the lawful basis. That is solely for the controller. Trellis can provide technical descriptions of the processing to support the trust's privacy notice and DPIA. Typical education bases are for the trust's DPO to confirm, not for Trellis to assert.

6. Where data lives

Pupil and meeting data in the Trellis service pipeline is stored at rest and processed in Microsoft Azure in the United Kingdom (UK South, with backups in UK West). Staff identity and authentication data used by Microsoft Entra External ID (name, work email, unique ID, and sign-in/sign-out logs) is held in the EU under the UK's adequacy arrangements for the EEA. No pupil data, recordings, transcripts or generated documents are held in Entra.

7. Key security controls

Drawn from Trellis DPIA v2.8 and Security Overview v2.3:

- **Identity:** Microsoft Entra External ID (OpenID Connect). MFA enforced for Trellis-managed accounts; where SSO is federated, the controller's own authentication policy (including MFA) applies. SSO roll-out through autumn term.
- **Network:** Web application firewall with UK geo-restriction and additional security controls. UK access is not restricted to pre-approved IP addresses; overseas access requires registered IP ranges. Admin tools and database have no public route (audited VPN only).
- **Encryption:** Client-side encryption of audio chunks before upload; TLS everywhere; encryption at rest in Azure UK.
- **Database:** Per-user Row-Level Security (fails closed); least-privilege roles; shared trust-boundary layer for permission checks and audit.
- **Malware:** Microsoft Defender for Storage scans every upload before the pipeline continues.
- **Residency:** Pupil and meeting data is stored and processed in Azure UK South, with backups in UK West. Microsoft Entra External ID holds staff identity/authentication data in the EU; no pupil data is held there.
- **Audit:** Append-only audit log (actor, action, entity, IP, user agent, trace ID); seven-year retention as compliance evidence.
- **Retention scrub:** Every personal-data record carries a PII expiry; continuous scrub deletes expired audio/documents and overwrites identifying fields.
- **Assurance:** ISO 27001 (certificate **271956**, dated **23 April 2026**); annual third-party penetration testing; staff with production access BPSS-vetted (DBS or Disclosure Scotland).

8. AI guardrails

- **Human-in-Command:** Trellis drafts; the teacher (or other education professional) always reviews, edits, and decides whether and how content is used. The AI never makes decisions or takes autonomous action about a child.
- **No training or fine-tuning** on customer or children's data (neither Trellis's nor Microsoft's). Quality improvement uses prompt engineering, model configuration and controlled evaluation; customer data is not used to train the underlying AI models.'

- Evaluation of a small number of identifiable recordings/transcripts/drafts is limited to no more than five named, BPSS-vetted Trellis staff under DPA instructions; increasingly evaluation uses in-app editing data instead.

9. Retention defaults

Category	Default	Notes
Personal data (recordings, drafts, related fields)	**60 days**	Configurable per controller; recorded in the DPA
Intermediate transcripts	**14 days**	For quality assurance and accuracy checking
Audit logs	**7 years**	Compliance evidence (Annex 1 of the DPA)

Controllers can instruct earlier deletion. On termination, personal data is permanently deleted from live systems other than the seven-year audit logs.

10. Sub-processors

Sub-processor	Children's / pupil data?	Location / transfer note
Microsoft (Microsoft Ireland Operations Ltd)	Yes – Azure compute/storage, Speech, OpenAI and Defender. Entra External ID holds staff identity/authentication data only; no pupil data.	Pupil/meeting data: UK South, with UK West backups. Entra staff identity/authentication data: EU under UK EEA adequacy; not a restricted transfer.

11. Top residual risks (after mitigation)

Risk = Likelihood (1–5) × Severity (1–5). Scores of 1–3 Low; 4–6 Medium; 7+ High.

Following mitigation, every residual risk listed in Trellis's DPIA evaluates to 6 or under. The controller retains responsibility for determining its own acceptance of residual risks when adopting the platform.

Risk (condensed)	Residual (L×S)	Residual risk level
Inaccurate or poorly worded draft misrepresenting a child's needs	1 × 4 = **4**	Medium
Speaker mis-attribution in transcript/draft	1 × 4 = **4**	Medium
Unauthorised access via compromised login	1 × 4 = **4**	Medium
Retention failure (data kept too long)	1 × 3 = **3**	Low
Function creep (use beyond agreed scope)	2 × 3 = **6**	Medium
Bias or discriminatory wording in AI output	1 × 4 = **4**	Medium

Mitigations centre on Human-in-Command review, training, MFA/SSO, WAF security controls and UK geo-restriction, RLS, retention scrub, purpose limitation in the DPA, and two-monthly ML evaluation. The trust still owns acceptance of residual risk for its own DPIA.

12. Further documentation

Full documents for information governance review:

- **Trellis DPIA v2.8** (October 2026)
- **Trellis Security Overview v2.3** (October 2026)

Contact: andy@trellis.scot (Andy Bell, CEO, Trellis Education Ltd)