Compliance FAQ

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

1. Do you train AI on our pupil data?

No. Trellis does not fine-tune models, and no children's data is used to train any AI model (neither Trellis's nor Microsoft's). Azure OpenAI does not store the inputs or outputs for training, and data is not available to other customers. Quality improvement is through prompt engineering, model configuration, and (increasingly) analysis of what teachers change in drafts. A small evaluation access by up to five named, BPSS-vetted Trellis staff may review identifiable content under the DPA; that is not model training.

2. Where is data hosted?

Pupil and meeting data (including recordings, transcripts and generated documents) is stored at rest and processed in Microsoft Azure UK South, with backups in UK West. Application execution, speech transcription and document generation run in the UK. Staff identity and authentication data used by Microsoft Entra External ID is held in the EU; it does not include pupil data, recordings, transcripts or documents, and is covered by the UK's adequacy arrangements for the EEA, so this is not a restricted transfer.

3. Any US transfers of pupil data?

Not for the Trellis service pipeline. The DPIA states there are no restricted international transfers: routine storage and processing (including transcription and LLM inference) take place strictly in the UK. Microsoft is additionally certified to the UK Extension to the EU–U.S. Data Privacy Framework; the Trellis contract is with Microsoft Ireland Operations Limited.

5. Can parents/pupils see or object to recording?

Lawful basis, privacy notices, and how objections are handled are **controller decisions**. It is worth noting children and parents do not use Trellis directly. They keep their UK GDPR rights (access, rectification, erasure, objection), exercisable **through the controller** (the Trust). Trellis shows a **transparency statement** at the start of recording. Controllers can configure the system to **pause or cancel** recording if an objection is raised.

6. Who is the controller?

The **Trust / school** (or local authority) is the **data controller**. **Trellis Education Ltd** is the **data processor**. Microsoft Ireland Operations Limited is Trellis's sub-processor for the service.

7. How long do you keep data?

Data	Default
Personal data (recordings, drafts, related fields)	**60 days** (configurable per controller; in the DPA)
Intermediate transcripts	**14 days**
Audit logs	**7 years** (compliance evidence)

Earlier deletion is available on controller instruction. On contract end, personal data is permanently deleted from live systems other than the seven-year audit logs.

8. What if a teacher relies on a bad draft?

Trellis is **Human-in-Command**: the AI drafts only; the teacher must review and edit before use. The AI makes **no decisions** about children. Residual risk of an inaccurate draft after mitigation is scored **4** in the Trellis DPIA, with training and evaluation reinforcing review responsibility. Trusts should set acceptable-use rules so unedited AI text is never treated as a final plan or decision.

9. ISO 27001 / pen test?

Yes. Trellis is certified to **ISO 27001** (certificate **271956**, dated **23 April 2026**), covering the production service and supporting administrative systems. The service undergoes **annual third-party penetration testing**, with findings tracked to closure and re-validated.

10. Network / IP allowlisting and SSO?

Since 6 October 2026, Trellis no longer requires IP allowlisting for UK access. Users can access the sign-in page from any UK network, including home broadband. Access from outside the UK remains blocked unless the organisation has registered its IP ranges with Trellis. Additional security checks and rate limiting may apply to users accessing from unlisted IP addresses.

Trellis strongly recommends that organisations provide a regularly updated list of their egress IP addresses.

Sign-in is via Microsoft Entra. Until federation, accounts are held in the Trellis tenant with MFA enforced. Where SSO is federated, the Trust's authentication policy (including MFA) applies.

11. Breach notification?

Trellis will notify the controller without undue delay after becoming aware of a personal data breach, in accordance with the DPA. Microsoft separately notifies Trellis of qualifying Security Incidents without undue delay and, in any event, within 72 hours under the Microsoft DPA. The Trust remains responsible for assessing ICO and individual notification duties as controller. Audit logs support investigation.