DPIA template: Maintained school (governing body)

Template, 15 October 2026. Sendix AI Ltd (the processor) has written this to save you time. It is not legal advice: your DPO decides. Sendix's own sections of the DPIA (v0.3, approved 9 October 2026, and the Scotland addition, approved 12 October 2026) are available on request from privacy@sendix.ai. Fill in every **[bracket]**.

1. Who is the controller, and who signs

Controller	The school's governing body. For a maintained school the governing body is the controller for pupil records it holds, even though the local authority maintains the EHCP itself. If your local authority has told you it is the controller for this processing, use its own DPIA process instead.
Who signs this DPIA	The governing body: the chair of governors, or the headteacher or business manager if the governing body has delegated this to them in writing. The school's DPO gives advice and records it.
Who signs the DPA with Sendix	The governing body signs the DPA in the Sendix app, or authorises the headteacher or business manager to sign it.
Controller name and address	**[name, address]**
Controller ICO registration	**[number]**
Controller DPO	**[name and contact]**
Processor	Sendix AI Ltd, SC883770, ICO ZC264381, privacy@sendix.ai

2. What the processing is

- **Purpose.** Staff upload EHCPs. Sendix flags wording that is too vague to deliver or review, cites the basis for each flag, and (for EHCPs and IEPs) suggests wording from evidence already in the file. A member of staff accepts, edits or rejects every suggestion. Nothing is decided automatically.
- **Plans in scope: [EHCPs]**. **Volume:** about **[number]** plans a year. **Users: [number]** staff in SENCO or SEND lead roles. No other staff can see plan text.
- **Data.** Plan text about a pupil's needs, outcomes and provision, which is special category data. Before storage, Sendix removes the pupil's name, UPNs, NHS numbers, postcodes and dates, and discards EHCP health and social care sections (C, D, G and H). Other names are replaced with roles where possible; this is best-effort, so treat the stored text as personal data.
- **Where.** Microsoft Azure UK South (app, database, backups) and Amazon Bedrock in AWS London (the AI model, which sees extracts only and keeps no inputs or outputs). Pupil data is stored and processed in the UK.

3. Lawful basis

- **Article 6:** 6(1)(e) public task, to carry out the school's duties under the Children and Families Act 2014 and the SEND Code of Practice 2015.
- **Article 9:** 9(2)(g) substantial public interest, with Data Protection Act 2018, Schedule 1, paragraph 6 (statutory and government purposes). Your Appropriate Policy Document covers this processing: **[reference]**.

Necessity. Sendix supports a review you already carry out. Only the parts of the plan the review needs are kept, identifiers are removed first, and staff decide every change.

4. Consultation and transparency

- **DPO** consulted on **[date]**; advice in section 7.
- **Families** told through your privacy notice, updated on **[date]** using Sendix's insert (available on request). **[Edit if you also consulted a parent forum.]**
- Maintained schools are public authorities for freedom of information. The school consults Sendix before releasing anything Sendix supplied in confidence.

5. Risks and measures

Risk	Sendix's measures	Your measures	Residual risk
Someone outside your school reads plan text	Per-school access checked in code and tested every build; MFA for SENCO and SEND lead accounts; UK hosting; independent penetration test completed before the first school's real data	Remove leavers promptly; staff keep MFA	**[Low / Medium]**
Re-identification from stored text	Identifiers removed; health and social care sections discarded; best-effort name redaction	Upload the plan only, not assessment packs or chronologies	**[Low / Medium]**
A suggestion is wrong and is relied on	Every flag cites its basis; suggestions use only evidence in the file; staff decide every change	Staff check each finding before acting on it	**[Low]**
Data kept too long	A daily job deletes records when your retention period ends; backups within 35 days	Set your retention period in Sendix: **[days]**	**[Low]**
Breach at Sendix	Notice to you within 24 hours (DPA clause 7.1)	Your breach procedure covers processors	**[Low / Medium]**

6. Your own measures

Measure	Owner	Done
Privacy notice updated	**[role]**	**[date]**
Appropriate Policy Document updated	**[role]**	**[date]**
Retention period set in Sendix	**[role]**	**[date]**
Staff briefed (upload the plan only; use roles, not names, in notes)	SEND lead	**[date]**
Review after the first term	SEND lead and DPO	**[date]**

7. Sign-off

	Name and role	Date
Measures approved, for the controller	**[see section 1: who signs]**	
Residual risks accepted	**[as above]**	
DPO advice (and whether it was followed)	**[DPO]**	
Next review	After the first term, then yearly, and when Sendix notifies a change	