Submitting controller details

Name of controller	
Subject/title of DPO	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Project Aim and Processing Summary

The project implements *Willow*, an AI-powered digital teaching assistant that supports teachers by generating post-lesson activities and providing insights on student progress, while offering students personalised, interactive learning. This involves processing student data (e.g., names, academic records, assignments, test results, chat interactions), as well as limited staff and parent contact data, through collection, storage, analysis, and retrieval.

Need for DPIA

A DPIA is required as the processing involves children's personal and potentially sensitive data, systematic monitoring of student interactions, and the use of AI technologies, which present potential high risks to individuals' rights and freedoms under the UK GDPR.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Nature of the Processing

Willow processes personal data strictly on behalf of the school, acting as data processor. Data is collected from the school's authorised users (teachers, students, and where applicable, parents/guardians) via the Willow platform. The data includes student identifiers, academic records, assignment submissions, test results, and chat-based learning interactions, along with staff and parent contact details, such as email addresses.

Data is used to deliver personalised AI-powered educational support, generate assignments and learning tasks, provide progress insights, and enable secure communication between teachers and students and the technology platform. All personal data is encrypted in transit and at rest. Willow

and its AI providers necessarily process readable content to provide the service, subject to access, contractual, and security controls. Data is stored securely on approved cloud infrastructure (e.g., Google Cloud) and retained only for as long as necessary to deliver services. The school selects the retention period; the school-selected default in this template is deletion or anonymisation after 12 months of inactivity, unless the school selects a different period.

The primary source of the data is the school, which remains the data controller. Willow does not collect data from external sources. Limited sharing occurs with authorised sub-processors (e.g., hosting providers, AI model providers such as OpenAI/Anthropic) under contract, solely to support functionality and in compliance with the UK GDPR.

High-Risk Processing

The processing involves the use of children's personal and potentially sensitive data, systematic monitoring of student behaviour and interactions, and the application of AI technologies. These factors may be considered high risk under the UK GDPR and therefore necessitate appropriate safeguards and a DPIA.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Scope of the Processing

Willow processes student, staff, and parent/guardian data (e.g., names, contact details, academic records, assignments, test results, chat interactions, and usage logs). Special Category Data may be processsed for the purposes of making provisions for students with Special Educational Needs or Disabilities (SEND). No criminal offence data is intentionally collected, though students may disclose sensitive information (e.g., self-harm, bullying, harm to others) in chat, which is encrypted and flagged to the appropriate teacher/school safeguarding lead.

Data is processed continuously as part of daily educational use, retained only as long as necessary, and anonymised or deleted according to the retention period selected by the school. The school-selected default is **12 months of inactivity** unless the school selects a different period. The processing affects students, staff, and parents/guardians authorised by the school, covering the school population in the UK. Data is hosted in the United Kingdom or another compatible data jurisdiction on secure cloud infrastructure, with appropriate UK GDPR transfer safeguards where applicable.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Context of the Processing

Willow processes data under the instruction of the school, which remains the data controller. The relationship with individuals is educational in nature: teachers use Willow as a support tool, while students engage with it as part of their learning. Parents/guardians may in the future have access to analytics/ through their own portal.

Students, including children and therefore a vulnerable group, form the primary data subjects. They have limited direct control over how their data is processed, but the school exercises oversight and determines lawful basis and purpose.

The service involves novel elements, specifically, the use of AI-driven interactions in a classroom environment and for students to use at home. This raises potential concerns around accuracy, bias, and safeguarding, which are mitigated by content filters, risk alerting, and teacher oversight. Willow addresses these through GDPR compliance, strong security measures, and safeguarding policies.

Willow is not yet a signatory to an approved certification scheme, the technology aligns its practices with the UK GDPR, the Children's Code, and statutory guidance such as Keeping Children Safe in Education (KCSiE).

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Purposes of the Processing

Willow processes personal data to deliver its core educational functions as an AI-powered assistant. The objectives are to:

- **Support teachers** by automatically generating post-lesson tasks, quizzes, and exercises, and by providing clear insights into student progress.
- **Enhance student learning** through personalised, adaptive conversations that reinforce classroom content and build engagement.

For teachers, the effect is reduced administrative workload, freeing more time for direct teaching. For students, the effect is a more tailored and engaging learning journey, with opportunities for reinforcement at their own pace. For schools, the effect is greater visibility into learning outcomes and wellbeing indicators.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Given the involvement of children's data and the use of novel AI technologies, Willow recognises the importance of consultation in assessing privacy risks.

- **Individuals' Views**: Children's views should be sought in an age-appropriate and proportionate way where practicable, for example through school-led pupil voice,

facilitated user testing, or consultation with student representatives. Where direct consultation is not practicable or appropriate, the school should record a specific justification in this DPIA, taking account of age, vulnerability, safeguarding, and burden. Views from teachers, safeguarding leads, and parents/guardians may supplement, but should not automatically replace, children's views. Feedback should also be collected from teachers and administrators during implementation and ongoing use.

- **Internal Stakeholders**: The school's Data Protection Officer (DPO) and safeguarding team should be involved in reviewing the DPIA, alongside senior leadership responsible for teaching and learning.
- **Processors and Sub-Processors**: Willow may consult with its hosting and AI sub-processors (e.g., cloud service providers) to confirm security and compliance measures. Processors are contractually bound to support data protection obligations.
- **Expert Input**: Willow plans to engage with necessary cybersecurity and data protection experts to further improve existing technical safeguards to ensure appropriate protections for vulnerable groups.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Lawful basis: Processing is carried out on behalf of schools under their public task to deliver education; safeguarding may also rely on vital interests.

Purpose alignment: Data processing is necessary to generate learning activities, insights, and safeguarding alerts—objectives that cannot be achieved effectively without it.

Alternatives: Manual methods exist but are less efficient and scalable.

Preventing function creep: Scope is limited to education and safeguarding; enforced through contracts, access controls, and regular reviews.

Data quality & minimisation: Data comes directly from schools and is limited to what is necessary. The school selects the retention period; the school-selected default in this template is deletion/anonymisation after 12 months of inactivity unless the school selects a different period.

Information for individuals: Clear privacy information is provided via schools for students, staff, and parents.

Supporting rights: Willow assists schools in fulfilling GDPR rights requests (access, rectification, erasure, etc.).

Processor compliance: Sub-processors are bound by GDPR-compliant contracts and due diligence.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
1. Data breach → Unauthorised access to student data, risk of exposure of children's personal information	Low	High	Medium
2. Inaccurate or biased AI outputs → Imperfect or misleading suggestions, risk of incorrect insights for students.	Medium	Medium	Medium
3. Sensitive disclosure by students in chat → Students may share unintended sensitive or wellbeing information.	Medium	Medium	Medium
4 Service downtime or technical failure → Disruption to teaching flow, reliance on alternative manual methods.	Low	Medium	Low
5. False safeguarding alerts → Incorrect alerts may cause unnecessary intervention, distress, stigma, or disproportionate disclosure.	Medium	High	High
6. Missed safeguarding alerts → Harmful or concerning content may not be flagged, delaying human safeguarding action.	Medium	High	High
7. Adult disclosure → Staff, parents/guardians, or other adult users may enter sensitive personal or safeguarding information beyond what is necessary.	Medium	High	High
8. Special-category or criminal-offence information → Chat or school data may include health, SEND, safeguarding, or alleged/offence-related information, increasing privacy and compliance impact.	Medium	High	High
9. Prompt injection → Malicious or manipulative inputs may cause the AI to ignore instructions, expose data, or produce unsafe outputs.	Medium	High	High

10. Vendor transfers → Hosting or AI vendors may process data outside the UK or change processing locations, creating transfer and transparency risks.	Low	High	Medium
11. Age assurance → Incorrect or incomplete age information may result in inappropriate settings, notices, or safeguards for children.	Low	High	Medium
12. Over-reliance on AI → Staff or students may place undue reliance on generated content, insights, or alerts, leading to poor educational or safeguarding decisions.	Medium	High	High

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Data breach	- Maintain encryption in transit and at rest; Willow and its AI providers necessarily process readable content to provide the service. - Regular penetration testing and vulnerability scanning. - Enforce multi-factor authentication, strict role-based access, and appropriate logging. - Annual data protection audits.	Mitigated	Low	Strong
Inaccurate or biased AI outputs	- Ensure teacher-in-the-loop oversight (no automated decisions). - Periodically evaluate AI outputs for accuracy, bias, and regression. - Provide clear guidance that outputs are advisory and require appropriate human review.	Mitigated	Low	Strong
Sensitive disclosure by students in chat	- Real-time safeguarding alerts routed to designated staff. - Configurable filters to detect sensitive keywords. - Staff training on responding to flagged disclosures.	Mitigated	Low	Strong
Service downtime or technical failure	- Maintain the 99% service uptime commitment. - Maintain regular backups and appropriate failover and recovery procedures.	Mitigated	Low	Strong

False safeguarding alerts	- Require human review of safeguarding alerts before consequential action, subject to the school's safeguarding procedures. - Tune and test alert thresholds against representative scenarios and record false positives for review. - Give designated staff sufficient context and clear escalation guidance.	Mitigated	Medium	Strong
Missed safeguarding alerts	- State clearly that automated alerts do not replace staff safeguarding duties or direct reporting routes. - Regularly test detection against representative safeguarding scenarios and investigate missed cases. - Maintain visible routes for students and staff to raise concerns directly with the school.	Mitigated	Medium	Strong
Adult disclosure	- Provide clear notices and acceptable-use guidance for staff and parents/guardians, discouraging unnecessary sensitive disclosures. - Apply data minimisation, access controls, and appropriate retention to adult-entered content. - Route safeguarding-relevant disclosures to designated staff where the school has configured that workflow.	Mitigated	Low	Strong
Special-category or criminal-offence information	- Minimise collection and avoid soliciting this information unless necessary for the school's purposes. - The school documents the applicable Article 9 and, where relevant, Article 10 condition and limits access and retention. - Apply enhanced access controls, audit logging, and appropriate handling of safeguarding records.	Mitigated	Medium	Strong
Prompt injection	- Treat user prompts and model outputs as untrusted; isolate system instructions and restrict tool and data access to the minimum required. - Test prompt-injection and jailbreak scenarios and monitor anomalous requests. - Do not allow model output to trigger consequential actions without appropriate human review.	Mitigated	Medium	Strong
Vendor transfers	- Maintain an up-to-date sub-processor list, contractual data-processing terms, and documented processing locations. - Use UK hosting or a compatible data jurisdiction and apply appropriate UK GDPR transfer safeguards where required. - Review vendor location or sub-processor changes before use and notify schools in line with contractual commitments.	Mitigated	Low	Strong
Age assurance	- Use school-managed account or roster data for age or cohort rather than inferring age from conversation content. - Apply age-appropriate defaults and notices based on school-provided age bands. - Require the school to verify account allocation and review edge cases.	Mitigated	Low	Strong

Over-reliance on AI	- Keep teachers and relevant staff in the loop and do not make solely automated decisions about students. - Train users on model limitations and require human verification of important educational or safeguarding outputs. - Reinforce that AI outputs and alerts support, rather than replace, professional judgment and established school processes.	Mitigated	Medium	Strong

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:	n/a	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	n/a	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	DPO	The DPO should also review ongoing compliance with DPIA