# Data protection impact assessment for an AI tool

The ICO's seven steps, phrased as the questions to answer, with the AI-specific prompts built in. One completed copy per tool, linked from its row in the Approved Tools Register. The DPIA belongs to the school as controller: whoever proposes the tool drafts it, the DPO advises and that advice is recorded, and a named senior leader decides.

Tool, proposer, date: [name and version of tool] · [person introducing it] · [DPO advising] · [date started]

## Step 1: the need

What is proposed, in two or three sentences, and why a DPIA is required. For an AI tool used with pupils' data the answer is usually that AI is an innovative technology and children are vulnerable data subjects, which together meet the ICO's high-risk test. If you conclude no DPIA is needed, record why here and stop: the record is the point.

## Step 2: the processing

What data goes in (list it exactly). Where it is processed and stored. Who can see it. How long it is kept. What comes out. Whether inputs train the supplier's models. Whether names can be left out (use pseudonyms or candidate numbers where possible). Every "to confirm" here becomes a written question to the supplier from the vendor question bank before you continue.

## Step 3: consultation

Who was asked (the staff who will use it; a route for pupil and parent views where the tool is pupil-facing), what they said, and what changed as a result. If nobody was consulted, say why.

## Step 4: necessity and proportionality

The purpose in one sentence. The lawful basis (public task, usually, for a state school's core work). What the tool does not need: name what you are withholding (names, whole cohorts, indefinite retention). Whether the same benefit could come with less, or with no tool at all.

## Step 5: risks

For each risk, likelihood and severity. Always walk the AI list: inputs used for training; hallucinated statements entering records; biased outputs affecting some pupils more than others; data leaving the UK; a safeguarding disclosure inside pupil work reaching the tool before the DSL; the tool changing under you (model, features, terms); a decision with a legal or similarly significant effect on a person made without meaningful human involvement.

## Step 6: measures

For each risk: what you will do, who does it, and the risk that remains. Typical measures: pseudonymised inputs, a person reviewing every output before it reaches a pupil, contract clauses (no training, UK or EU processing, retention, deletion on exit), register conditions narrowing the use, and review triggers.

## Step 7: sign-off and outcomes

| | |
|---|---|
| The DPO's advice | [recorded in full; if not followed, the reasons] |
| Decision and decision-maker | [approved / approved with conditions / declined] · [name and role] · [date] |
| Residual risk | [low / medium / high] |
| Carried into the register entry and the privacy notice | [what] |
| Review date and triggers | [date]; a model or feature change, new terms, an incident or complaint, any new use |

If a high risk remains after the measures, the school must consult the ICO before the processing starts (UK GDPR Article 36); the ICO says it responds within eight weeks, or up to fourteen in complex cases. In practice the finding is usually "not like this": narrow the use, reconfigure, or choose another tool.