

AI READINESS

Introducing AI safely and practically in schools

A decision guide for choosing use cases, products and safeguards before moving from informal experimentation to approved school use.

SLT	DPOs	DSLs	Digital leads
-----	------	------	---------------

HOW TO USE THIS BRIEFING

Use this briefing to structure an AI working group, product review, staff pilot or decision about learner-facing access.

If you only read one page

Start with the decision, then use the rest of the briefing to test evidence and plan implementation.

THE CORE DECISION

Start with a defined educational or operational need, then decide what data, users and safeguards are appropriate. A popular tool or attractive demonstration is not yet an implementation plan.

Why this matters now

Use is already happening

Staff and pupils may use consumer AI before a school has agreed approved tools, data rules, training or support.

Guidance is maturing

DfE has guidance for AI use in education and product safety standards, including expectations for learner-facing filtering.

Risk depends on the use case

A staff drafting assistant and a pupil-facing tool have different safeguarding, data, accuracy, supervision and assessment risks.

What good looks like

- A small set of approved use cases linked to school priorities
- Clear staff and pupil rules for personal, special-category and safeguarding data
- Product review covering contracts, retention, training use and sub-processors
- Age-appropriate filtering, monitoring, supervision and reporting
- Human review of outputs and no uncritical automated decision-making
- A controlled pilot with success, risk and stop criteria

A sensible first action

- Form a working group including education, safeguarding, IT and data protection.
- Collect current use cases before selecting a platform.
- Classify the data each use case might process.
- Start with a limited staff pilot and record what is learned.

SCHOOL REALITY

Where sensible plans often become difficult

These are common implementation problems in schools. They are not signs of failure; they are reasons to make dependencies, evidence and ownership visible.

Shadow use

Blocking every tool may hide activity, while unrestricted use can expose school data and create inconsistent practice.

Product claims

Enterprise controls, education terms, data residency, model training and safety features vary between products and licences.

Safeguarding context

Learner-facing AI can generate dynamic, personalised content that needs suitable filtering, supervision and reporting.

Quality and accountability

Outputs can be inaccurate, biased or unsuitable. Staff remain responsible for professional decisions and checking work.

Warning signs to investigate

- A product is chosen before the use case and data are understood
- Staff paste identifiable pupil, HR or safeguarding information into consumer tools
- The supplier cannot explain retention, training use or sub-processors
- Learner access is introduced without age, filtering and supervision decisions
- No human-check or escalation process exists for harmful or inaccurate output
- The pilot has no owner, success measure, review date or stop condition

LEADERSHIP PRINCIPLE

Ask for enough technical detail to support a decision, but keep the outcome expressed in school terms: learning, safeguarding, continuity, workload, cost and accountability.

DECISION FRAMEWORK

Questions that turn reassurance into evidence

Use the third column to agree what the school should be able to see, retain and review. Evidence should be current, understandable and linked to an owner.

DECISION AREA	LEADERSHIP QUESTION	EVIDENCE TO REQUEST
Purpose	What specific problem will the tool address, and is AI necessary?	Defined use case, user group, expected benefit and alternative
Data	What personal, special-category, safeguarding or confidential data could be processed?	Data-flow map, input rules, lawful-basis review and DPIA decision
Supplier	How are prompts, outputs and accounts stored, used, transferred and deleted?	Contract, DPA, privacy terms, sub-processors and retention
Identity	Can school accounts, SSO, MFA, roles and leavers be controlled?	Licence capability, access design and administrator roles
Safety	What filtering, monitoring, age controls and reporting exist for the intended users?	Product safety response and school safeguarding assessment
Quality	How will errors, bias, copyright and unsuitable outputs be checked?	Human-review rules, staff guidance and incident route
Assessment	How will permitted and non-permitted pupil use be explained and detected?	Curriculum and assessment guidance with consistent communication
Pilot	What would make the school expand, change or stop the use?	Success measures, risk indicators, feedback and review date

How to use the table

Do not expect every item to be perfect before acting. Record the current position, the risk or service impact, the agreed action, the owner and a realistic target date. Review high-impact gaps first.

IMPLEMENTATION ROUTE

Move in controlled, visible stages

The sequence matters: establish the current position, prove the important controls or user journeys, then embed review into normal school governance.

FIRST 30 DAYS Govern current use	- Identify existing tools and practical use cases - Publish interim rules for data, checking and approved access - Assess priority products and decide whether a DPIA is needed
DAYS 31-90 Run a controlled staff pilot	- Configure identity, licensing, retention and administrator controls - Train users on safe prompting, verification and reporting - Measure time saved, quality, incidents and support demand
BEFORE WIDER USE Scale only with evidence	- Complete safeguarding and product-safety checks for learner use - Update policies, privacy information, curriculum and assessment guidance - Review suppliers, risks and controls at agreed intervals

Measures leaders can follow

01 Approved use cases	02 Users trained	03 Data or safety incidents	04 Quality and time-saving evidence
-------------------------------------	--------------------------------	---	---

KEEP THE PLAN REALISTIC

Align major changes to exams, census, payroll, admissions, safeguarding reviews and the limited windows available for disruptive work. Build support and rollback into the plan, not after it.

LEADERSHIP CHECKLIST

What to confirm before closing the review

A completed checklist is useful only when exceptions, evidence and actions are recorded. Use it as a review prompt rather than a compliance certificate.

☐ The use case and intended benefit are defined	☐ SSO, MFA, roles and leavers are controlled
☐ Education, DSL, DPO and IT roles are represented	☐ Learner-facing safety features are assessed
☐ Approved and prohibited data are explained	☐ Human checking is mandatory for important outputs
☐ DPIA screening is recorded	☐ Staff and pupil guidance is consistent
☐ Supplier terms and sub-processors are reviewed	☐ The pilot has success and stop criteria
☐ Retention, deletion and model-training use are understood	☐ The review date and accountable owner are set

Minimum evidence pack

01 Use-case register	02 AI product assessment	03 DPIA decision
04 Configuration record	05 Training and guidance	06 Pilot evaluation

Decision record

Record what was reviewed, who contributed, the evidence considered, any limitations, the decision made, actions and owners, and the next review date. This gives future leaders and suppliers a clear starting point.

ABOUT OPSWISE

School-focused support, security and planning

OpsWise helps schools make technology decisions in context - joining technical delivery with safeguarding, data protection, budget, supplier and operational needs.

How OpsWise can help

- AI readiness and product comparison
- DPIA, data-flow and supplier review support
- Identity, licensing and security configuration
- Pilot design, implementation and governance

What an initial discussion covers

- What is happening now
- Which outcome matters most
- What evidence is already available
- A proportionate next step, even if that is not a managed service

A PRACTICAL NEXT STEP

Turn the questions into a clear school IT plan.

OpsWise can help a school move from informal AI use to a proportionate, documented approach that joins educational value with safeguarding, data protection and technical control.

hello@opswise.co.uk | 0203 907 6865

www.opswise.co.uk

86-90 Paul Street, London EC2A 4NE

Authoritative sources

[DfE: Generative AI in education](#)

[DfE: Generative AI product safety standards](#)

[DfE: Filtering and monitoring core standard](#)

[ICO: AI and data protection guidance](#)

[ICO: When a DPIA is needed](#)

Guidance checked 19 August 2026. Always consult the latest authoritative version. This briefing provides general information and a decision framework; it is not legal advice, certification or a guarantee of compliance or outcomes.