Browne Jacobson

# New DfE AI guidance: A welcome start, but needs further development

26 June 2025 Claire Archibald

In June 2025, The Department for Education (DfE), supported by the Chiltern Learning Trust and the Chartered College of Teaching, published **support materials on the use of artificial intelligence (AI) in education settings**, described as a 'workbook' with slides and videos.

This welcome initiative aligns with the DfE's aim to boost school leaders' and teachers' confidence in using AI, hoping to unlock new workload approaches and time efficiencies. These materials supplement the earlier policy paper and generative AI product safety expectations guidance originally published in January 2025.

The government's message is clear: AI, when implemented safely and effectively, can transform education. Therefore, any additional DfE guidance is genuinely welcomed by the sector.

## The ‘how-to’ gap for using AI in schools

While the DfE's guidance sets out useful examples for AI's benefits while reminding practitioners of the risks, a gap remains. Their strategic vision hasn’t yet fully translated into the practical instructions schools need daily to reduce risk.

This 'how-to' gap shifts detailed risk assessment, policy development, and compliance onto already strained school resources. Without practical safeguards and comprehensive 'how-to' support, particularly for Data Protection Officers (DPOs), what’s presented as a potential game-changer could, without more comprehensive support, become a complex compliance challenge.

This article isn't just a theoretical discussion, it's about practical action. For time-strapped school staff, we outline below some key steps schools can take now to build safe and robust AI use.

## The UK government's pro-innovation AI strategy and its implications for education

The UK government's ‘pro-innovation’ AI approach aims to unlock economic potential and establish Britain as a global leader. This strategy prioritises innovation, avoiding excessive top-down regulation. AI is central to the government's broader strategy for economic growth and public service improvement, offering significant cost reduction and economic boosts.

Schools are key to this ambition, crucial for both AI adoption and development. It's a natural extension that the DfE promotes AI tools for educational excellence, viewing AI as a transformative force for improving lives and supporting the government's AI Opportunities Action Plan.

The government has clear aims to enhance learning, streamline administration, and contribute to a more efficient, technologically advanced education system that supports broader economic growth and prepares the future workforce.

Schools and academies must join on that mission, and it is vital that the sector supports and works with the government on the division of responsibilities for management of the risks that come in hand with AI opportunity. So, while avoiding top-down regulation is part of the strategy, that doesn’t mean that the risk burden should lie entirely with schools.

# Next steps to expand the DfE's guidance

The DfE, like all those navigating AI's rapid advancements, is on a learning curve. This initial guidance is a valuable start, but the next phase now offers an important opportunity to provide the actionable detail schools truly need.

The following areas represent key opportunities for the DfE to expand current guidance, moving from high-level principles to practical guidance that will genuinely empower schools to harness AI safely and effectively:

## Clarifying data protection terminology

Data protection can be confusing, so clear terms are crucial. Currently, the training offers high-level principles without necessary legal specificity, listing legal basis and missing an opportunity to explore them in more detail.

Phrases like "data protection must comply with GDPR" in the slides can be confusing. As a legal professional, I initially thought this was a typo. However, completing the accompanying Chartered Institute of Teaching certification confirmed it wasn't, as it appeared in a multiple-choice question.

The 'privacy' vs 'data protection' debate continues too. While 'privacy' is not defined in UK data protection laws, this Americanised terminology occasionally creeps into the guidance. The DfE could enhance understanding by providing clear, consistent definitions for key AI and data-protection related terms.

## Consent for children under 18 using online services

Schools need more detailed guidance on consent, especially for processing personal data of children under 18.

The Information Commissioner's Office (ICO) defines a child as under 18. For Information Society Services (ISS) offered directly to a child, UK GDPR Article 8 applies. If consent is the basis, a child must be at least 13 to consent themselves. For under 13s, parental consent is needed.

While the ICO's Children's Code clarifies schools typically aren't ISS when processing for educational purposes, an edtech service used in or by a school can be an ISS. Crucially, the distinction between an edtech provider’s status as a data controller or processor determines their ISS status, and this nuanced area needs further clarification. Without this, schools are inadequately informed about indirect responsibilities when procuring AI tools that are ISS and process children's data.

## Scrutinising terms and conditions

Terms and conditions (T&Cs) are the primary contractual mechanism for schools to understand and control how their data, especially pupil data, is processed by third-party AI vendors. Even after training, schools may still struggle to negotiate or understand these or data processing agreements.

Future guidance should equip schools with practical tools and templates to effectively review and negotiate T&Cs and provide example questions/checklists for vendor due diligence.

## Beyond personal data and intellectual property

While DfE guidance focuses on data protection and intellectual property, it largely overlooks broader confidential information. This is a significant oversight for schools, who handle much sensitive confidential information. Schools and academies often receive freedom of information requests and make use of the exemption in Section 36 of the Freedom of Information Act 2000, which allows the refusal of a request for information which, if released could ‘prejudice the conduct of public affairs’.

The DfE's focus on data protection and IP so far misses an opportunity for more comprehensive guidance on information governance in education. Without explicit guidance on safeguarding all information, schools might use AI tools for tasks like summarising internal reports, financial data, or sensitive meeting minutes.

Such actions could compromise security or integrity, or expose the school to cyber threats, regardless of personal data concerns. The DfE focus on AI for teaching and learning purposes may mean that use for governance, financial and strategic purposes may mean that schools inadvertently give away information which should be more closely guarded.

## Enhancing parental and community engagement

Robust community engagement is vital for schools, ensuring plans anticipate stakeholder concerns. While current guidance mentions parent involvement, it often describes a one-way exchange. Effective parental engagement will inevitably strengthen the home/school relationship. Additionally, children themselves have voiced concerns about generative AI, including bias and environmental impacts. Pupil voices should therefore be considered in AI adoption decisions.

The DfE's approach so far seems to suggest a top-down, informational model, not a collaborative two-way dialogue. This misses an opportunity to identify parental engagement as a strategic boost for innovation. Insufficient engagement can lead to distrust and resistance, potentially resulting in parents opting children out of AI activities or vocal opposition, hindering effective and equitable AI implementation.

Future DfE guidance should proactively advocate for genuine two-way dialogue, empowering schools to build deeper trust and ensure AI initiatives reflect community values and needs.

## AI and sustainability

The DfE guidance's brief mention of sustainability so far feels like a token gesture, suggesting the focus is on immediate operational risks (security, safety, compliance) while largely neglecting broader, long-term societal and environmental responsibilities of technology adoption. To truly support a forward-thinking approach, the DfE could integrate more comprehensive guidance on AI's ethical and environmental considerations, with a holistic understanding of responsible AI adoption.

## Practical steps for schools right now

While we await more comprehensive guidance from the DfE, schools are not left entirely without a compass. Ideally, schools should aim to put in place a comprehensive governance programme for AI, perhaps using the approach suggested by our Browne Jacobson six-step governance plan.

However, as a minimum starting point, drawing on principles of good data protection practice, sound governance, and community engagement, here are three practical steps schools can take to begin to govern AI:

**1. Engage effectively with the parent community: AI with, not to**

One of the most powerful and often overlooked steps a school can take is to bring parents and carers into the conversation. AI is a rapidly evolving area, and there can be understandable anxieties among parents about its use.

Rather than presenting AI as a fait accompli, schools should proactively engage with the parent community. This means having open and honest conversations, listening to concerns, even if you don’t have the answers, and involving parents in discussions about AI policy or specific AI tool implementations. When parents feel they are part of the process, rather than having AI 'done to' them, subsequent complaints and objections are much less likely.

**2. Complete a single, thorough project plan, DPIA, and AI risk assessment for your riskiest AI use**

The sheer volume of AI tools can feel overwhelming. Instead of trying to tackle everything at once, focus your efforts strategically. Identify the single riskiest or most impactful use of AI that your school is considering or is already using. For this chosen AI use, conduct a project plan, setting out the purpose and expected outcomes. Then complete a Data Protection Impact Assessment (DPIA).

This is a legal requirement under the UK GDPR when processing is likely to result in a high risk to individuals' rights and freedoms. An AI tool, particularly one involving pupil data, almost certainly triggers this. This DPIA for an AI tool should be robust, identifying potential data protection risks (e.g. data security, accuracy, bias, transparency, data minimisation) and setting out clear mitigation strategies. Bolster that DPIA by considering broader AI-specific risks and mitigations.

Treat this intensive exercise for one AI tool as a learning opportunity. The insights gained, challenges encountered, and solutions developed will be invaluable blueprints or templates for future AI projects.

**3. Read AI vendor terms and choose products where the provider acts as a processor, and inputs are not used further**

You really want to make sure any external provider is acting as a data processor in relation to any information input into the AI tool. This means they only process the data (including any inputs from your school) strictly under your school's instructions, and for your school's specified purposes.

This keeps your school firmly in control as the data controller, responsible for determining why and how the data is processed, and ensures the vendor acts purely as a service provider, adhering to your direction. If an AI provider positions themselves as a 'controller' for the data inputs, it means they are determining their own purposes and means of processing, which can significantly reduce the school's control and increase compliance complexities.

Further, a non-negotiable term for schools should be that inputs from your school (e.g., pupil work, teacher notes, sensitive school data) are not used by the AI product provider to train or improve their models, whether anonymised or not. Even 'anonymised' data can sometimes be re-identified, and allowing your confidential school information to be used to build vendor commercial products is not acceptable from a data protection or ethical standpoint. This needs to be explicitly stated and agreed in the contract.

## Conclusion

In summary, while the DfE guidance is a welcome and necessary first step in integrating AI into education, more is needed to offer the comprehensive, practical toolkits schools urgently require. As specialists in data protection, information law, and AI governance with practical experience advising education clients we know that schools need clearer, more in-depth, and truly actionable strategies.

In the meantime, adopting a pragmatic approach will stand schools on a firmer footing. This includes effective engagement with the parent community to ensure AI is done with them, not to them; undertaking a thorough project plan, DPIA, and AI risk assessment for the riskiest AI use as a crucial learning exercise; and scrutinising AI vendor terms.

Ultimately, effective AI integration in education, as always, lies in the granular details, many of which remain undefined in the current guidance. By taking these concrete steps now, schools can responsibly harness AI's potential while safeguarding their communities.

## Contact


Claire Archibald

Legal Director

claire.archibald@brownejacobson.com

+44 (0)330 045 1165


## Related expertise

AI regulation and governance

Artificial intelligence

Data protection and privacy

Data protection guidance for schools and trusts

Education law

Information law