Browne Jacobson

AI adoption in schools: Meeting ICO expectations

04 March 2025   Claire Archibald and Dai Durbridge

We've compiled insights to support schools in the use of artificial intelligence (AI), focusing on the expectations of the Information Commissioner's Office (ICO) regarding the adoption of AI in educational settings.

In a keynote speech the Information Commissioner, John Edwards indicated that one of the key priorities for ICO engagement related to the use of AI. He asserted that organisations must ensure that *"any automated decision-making must be thoroughly tested, and risk assessed."*

But what does good testing and risk assessment look like?

During their workshop Choosing AI and doing it safely, ICO staff, Clara Clark Nevola and Kimberly Mai gave helpful detail about how organisations can do this. They considered some of the key questions that organisations, including schools, should ask when working to procure AI solutions.

Some of these questions are a vital step in procurement decision-making processes and should not be skipped over in the eagerness to get started with new technology. They flagged the tools the ICO have available, such as the AI and data protection risk toolkit.

They also share tips on how to investigate key risks with external providers and some of the questions that could be posed both during procurement, and on an ongoing basis.

Schools must:

1. Clearly understand roles and responsibilities, and consider carrying out a DPIA

Schools should clearly understand whether the AI provider acts as controller or processor in relation to personal data shared. Responses from the vendor regarding this question will be highly indicative of the vendor's understanding of the law and their responsibilities.

All projects should be screened to consider if a Data Protection Impact Assessment (DPIA) is required. Top tip: if children's personal data is going to be processed in the tool, or you are using it to carry out any HR processes, then that is almost certainly a high-risk processing activity, meaning a DPIA isn't just advisable, it's a legal requirement.

Regardless of whether it's a legal requirement, carrying out a DPIA is an ideal way to demonstrate that risk assessments have been carried out, as ofsted will also want to see evidence of this.

2. Clarify with the vendor whether personal data will be used to train the model

Technology tools always need constant refinement and improvement. When it comes to generative AI, this has an increased risk, where information provided by the controller may be fed back into the model to improve its functionality, including future outputs.

This could lead to individual's data being used in a way that has not been foreseen, or in an unlimited way, and leaves individuals in a position where it is difficult for them to be able to exercise their rights.

3. Confirm how information will be held securely

Schools are responsible for ensuring that any personal data shared with external vendors can be held securely. This means that vendors must be able to satisfactorily answer questions about information security. Vendors who merely answer that their information is held "encrypted, so in compliance with the GDPR" will not be giving sufficient detail in this sort of response.

Schools should ask for evidence of security tests and their results. Where pupils will be using tools, schools should be particularly interested in how models respond to "Jailbreaking" attempts. Jailbreaking presents both a safeguarding and a data protection risk, so vendors should be able to explain and share their testing results.

4. Ensure transparency and fairness for data subjects

Schools must explain to data subjects where AI is used, and their rights in relation to such processing, particularly if the processing is made automatically, without human input. For example, if AI tools are used as part of selecting candidates for shortlisting in a recruitment process, this automated processing must be open to challenge by the candidate, who can ask for a human review of the decision.

Schools must understand that they cannot hand over responsibility for AI decision-making to the vendor and that they retain overall oversight and accountability.

Schools should:

1. Engage at an early stage with your data protection officer (DPO) and stakeholders

The expertise of the DPO should be properly engaged at the earliest stage of an AI project. By engaging with the DPO at the outset, they can offer to contribute to procurement decisions, potentially finding one vendor to be less risky from a data protection point of view than another.

You should take any questions from the DPO and other stakeholders to the vendor as part of the due diligence process. This is an ideal opportunity to work with several vendors before committing to a spend with them. Not only the answers given, but the ability and willingness of the vendors to enter such discussions can then be a factor in final procurement decisions. Any statements of assurance should be queried and verified.

Wider stakeholder groups also have important information to add, so consider consulting with a wide range of users, from staff to students and their parents. Take time to understand their concerns, as they may provide useful information to include in due diligence processes.

2. Look for bias and discrimination and mitigations

Sadly, discrimination and bias are human attributes and generative AI models have been built on such human flaws. AI can amplify risks in relation to this. For example, an image generator may consistently produce white men as examples of CEOs, or young black men as criminals, or a CV scanning tool may show bias towards those educated in Russell Group universities.

Rather than avoid such issues, schools should actively engage with vendors to explore where those issues may surface and what mitigations have been put in place.

3. Carry out tests and seek feedback

Going 'live' on a system does not mean that schools need to launch AI to all users simultaneously. A responsible AI vendor will support a staged rollout of a system, enabling careful testing and feedback before all users can access the tool. This allows any unforeseen issues to be addressed at an early stage.

Time to act

Whether your school is preparing its first foray into AI tools, or whether existing Edtech tools have already been fitted with an 'AI upgrade', the ICO and Ofsted have made it clear that this change requires careful risk assessment and planning.

There's a wide market out there full of vendors eager to offer their wares. Schools are in a strong position to challenge vendors and are free to choose from those that not only offer a solution to their AI problem, but can also engage with and answer data protection, security, and discrimination risk questions.

Further support

Our expert team are here to help. Get in touch or check out these resources for the support you need to deploy AI safely in your school.

- AI governance support pack
- Education procurement support pack
- Data protection officer helpline

Key contacts

Claire Archibald

Legal Director

claire.archibald@brownejacobson.com

+44 (0)330 045 1165

Dai Durbridge

Partner

dai.durbridge@brownejacobson.com

+44 (0)330 045 2105

Related expertise

AI regulation and governance

Artificial intelligence

Data protection and privacy

Data protection guidance for schools and trusts

Education law

HR services for schools and academies