west sussex county council

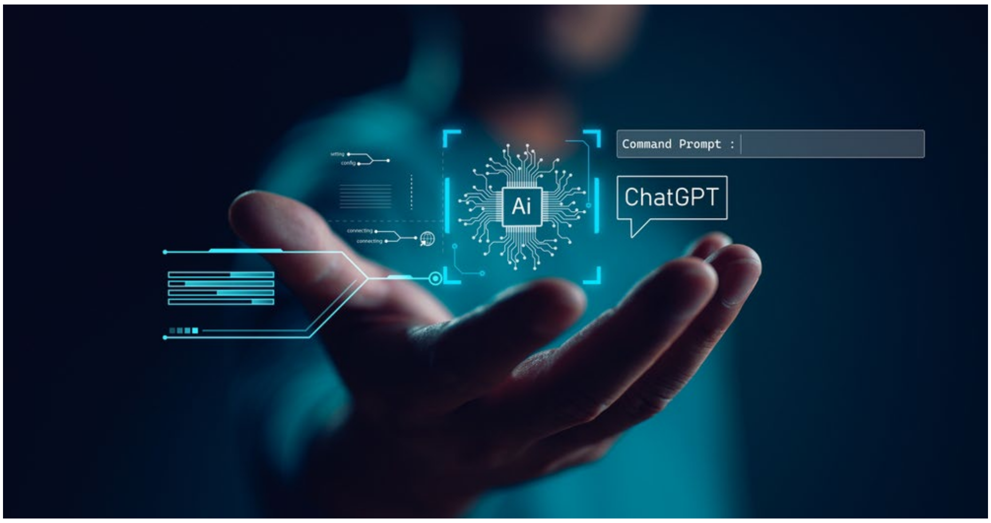
SERVICES FOR SCHOOLS
and other educational settings

# AI Tools: protecting personal data

## Protecting personal data when using AI tools in educational settings

By Lisa Hickman, Education Business Communications Manager

The Department for Education (DfE) recognises that there are benefits to using AI in schools. My colleague, Stephen, explores some of these in his article on integrating AI into education. Whist AI can provide many benefits, these must be considered alongside the need to manage any risks to avoid sharing personal data. Following recent enquiries from schools it might be helpful to consider the following when using AI in schools. We have also provided some sources of useful information that may be of further help to schools.



### What is generative AI and how does it work?

Generative artificial intelligence (AI) has the technological ability to create new content, text, images, music, audio, and videos. It works by:

- storing and learning from the information it is given
- creating believable content from that information.

Understanding how the technology works will help in assessing how to utilise its benefits and consider the steps you need to take in order to protect personal data processed in your school.

### Benefits of using generative AI

It is easy to see the benefits the generative AI tools can provide in speeding up tasks we are required to undertake.

Examples might include:

- analysing, structuring, and writing text from documents, data or meeting recordings
- turning prompts into audio, video and images
- managing repetitive tasks
- reducing errors when transcribing meeting minutes

The DfE recognises that, when used appropriately, generative AI has the potential to:

- reduce workload across the education sector
- free up teachers' time, allowing them to focus on delivering excellent teaching.

**What are the risks of using Generative AI**

Whilst the benefits can be appealing, it is important to understand the risks, which can include:

- inaccuracy in the information produced
- that the content and language used is inappropriate.
- a risk of bias
- that information is taken out of context and without permission
- that information is out of date or unreliable
- that personal data is not sufficiently protected
- that the technology is being used to deceive, Scam emails are a common example of this.

So, how do schools navigate this complex area whilst utilising the potential efficiencies this type of technology can provide?  How can they protect the rights and freedoms of individuals and comply with data protection requirements expected of organisations?

**Risk management**

The deployment of an AI system to process personal data needs to be driven by evidence that there is a problem, and a reasoned argument that AI is a sensible solution to that problem, not merely by the availability of the technology. Organisations must be able to evidence that you couldn't possibly accomplish the processing of personal data in a less intrusive way, using existing tools. For content that is produced using generative AI, organisations need to ensure professional judgement is used to check the quality and content of the documents, data etc being produced.

Schools are their own data controllers and their DPOs are accountable for understanding those risks, or seeking advice on those risks. The Information Commissioner's Office (ICO) guidance is that organisations must ensure that their processes capture the use of AI to identify the risks at the earliest possible stage and complete a Data Protection Impact Assessment (DPIA). The DPIA looks at the data, context, method of processing and whether it persists beyond its intended use – i.e. transcribing a meeting.

The ICO has produced guidance around the use of AI and how to approach it – Guidance on AI and data protection. The ICO has also created an AI toolkit which can be a useful resource and includes a video explaining how organisations can mitigate the risk of using AI whilst utilising its benefits.

The DfE advises that schools and colleges should:

- protect personal and special category data in accordance with data protection legislation
- not allow or cause intellectual property, including pupils' work, to be used to train generative AI models, without appropriate consent or exemption to copyright
- review and strengthen their cyber security by referring to the cyber standards – generative AI could increase the sophistication and credibility of attacks
- ensure that children and young people are not accessing or creating harmful or inappropriate content online, including through generative AI - keeping children safe in education provides schools and colleges with information on:
    - what they need to do to protect pupils and students online
    - how they can limit children's exposure to risks from the school's or college's IT system
- refer to the filtering and monitoring standards to make sure they have the appropriate systems in place.

**Data Privacy**

Data protection legislation sets out organisations responsibilities for protecting personal and special category data. Being aware of these when using generative AI tools is key. Avoiding the use of this data when using generative AI tools or if it is necessary to use personal and special category data, the school must ensure it is complying with GDPR legislation and their own policies.

The DfE reminds us that "education institutions should also be open and transparent, ensuring the data subjects (pupils) understand their personal or special category data is being processed using AI tools.".

**Where can I find out more?**

- Guidance on AI and data protection | ICO
- DfE Publication: Generative Artificial Intelligence In Education
- ChatGPT and LLMs: what's the risk
- the principles for the security of machine learning

More information about:

- personal data
- special category data