



CHILTERN
LEARNING
TRUST

Artificial Intelligence Policy 2025–2026

Approved by the Board of Trustees: July 2025

Review date: July 2026

Contents

1. Introduction
2. Responsibilities
3. Ethics and Product Safety
4. Data Protection
5. Intellectual Property
6. Safeguarding and Online Safety
7. Academic Integrity
8. Monitoring, Training and Review
9. Associated Documents and Roles

1. Introduction

Artificial Intelligence (AI) is reshaping education. From reducing workload and personalising learning to generating insights and supporting inclusion, AI offers real promise. But it also brings

serious risks around safeguarding, data privacy, bias, misuse, academic integrity, over-reliance and legal compliance.

Chiltern Learning Trust (CLT) is proud to be leading nationally in this space, having co-developed the **DfE's Safe and Effective Use of AI in Education** training programme. This policy provides our internal framework for the **safe, ethical and effective** use of AI across all CLT schools.

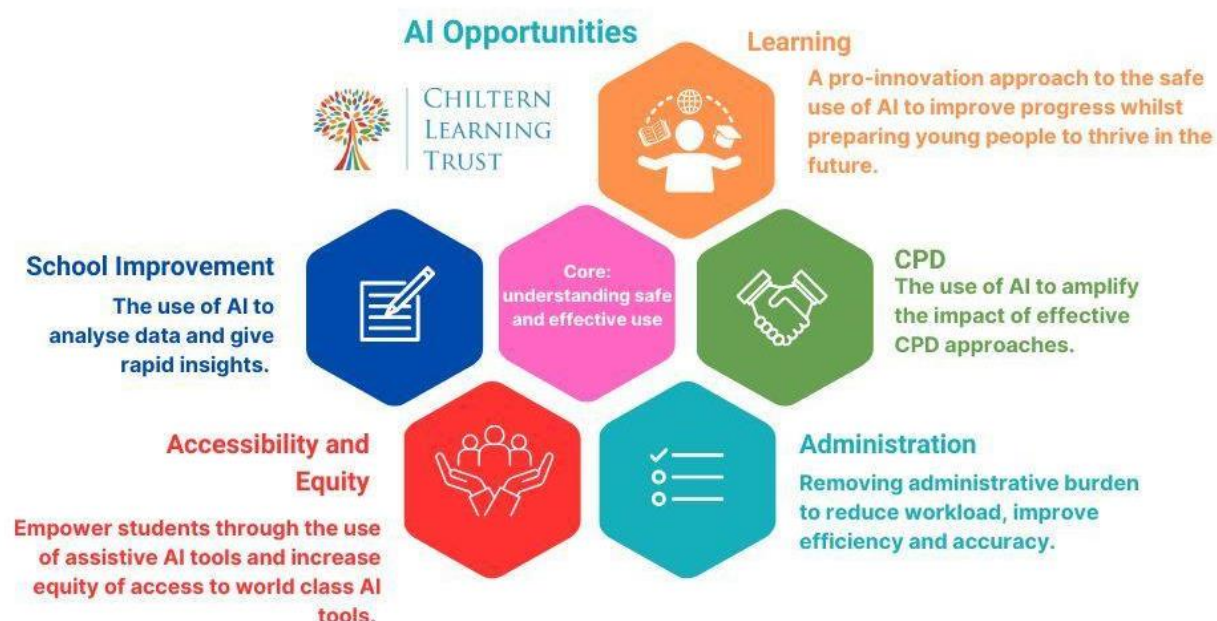
2. Responsibilities

Using AI safely in education requires shared understanding and clarity of roles.

- **School staff:** Use only trust approved AI tools in line with this policy, data laws and only in approved ways in line with training on AI, referring to the trust 'Approved AI tool register'. School staff must always be transparent about their use of AI and if unsure about a particular use, they should seek clarification from their Technology for Learning Lead in School.
- **School leaders:** Set clear expectations for use and ensure staff receive CPD on the safe and effective use of AI through a visit by the Trust EdTech Lead and by using the DfE materials. The Trust EdTech Lead will deliver a programme throughout the autumn term for school leadership to support the development of a school AI action plan in each school which will include risk mitigation and a curriculum approach to help prepare students for a world increasingly driven by AI, helping them to understand where it can support their learning and where it might hinder their learning.
- **The Trust EdTech Lead supports schools to:**
 - Develop AI strategies
 - Embed AI literacy in curriculum
 - Access CPD and implementation support

This policy applies to all employees, contractors, volunteers associated with the Trust schools. All staff should be aware of the evolving potential for AI to save workload in their practices in the role of assistant rather than replacement whilst being sure to use AI in a way that is commensurate with safeguarding and data safety regulations.

Some of the key opportunities that the trust have identified are listed below:



3. Ethics

In line with the Beijing Consensus from UNESCO and DfE Guidance on the ethics of AI, our Trust recognises the transformative potential of AI in education, as well as the risks and challenges, particularly concerning ethical considerations.

The Department for Education's (DfE) guidance on Generative AI in education (June 2025) underscores the importance of adhering to ethical standards, emphasising the potential biases and inequalities that could emerge through the use of AI. Some of these issues include:

- The risks of AI tools being biased against particular groups and perpetuating biases, as well as the possibility of outputs being biased due to the prompt or instruction containing bias.
- AI creating factually incorrect materials.

To mitigate these risks, our Trust is committed to:

- Providing regularly updated guidance and CPD to all staff to help them recognise and understand the underlying biases that can influence AI, equipping them to identify and address potentially harmful content, misinterpretations and misuse.
- Tools that are not approved by the trust may be blocked on the network.

It is important that teachers:

- Use only trust approved tools as listed in the 'Approved AI tool register'. These tools meet the **DfE Product Safety Expectations, this includes the need for additional safety features to be built in, and for the AI model not to train on prompts or uploaded materials.**
- If anyone in a school is thinking of adopting a new AI tool, the Trust EdTech Lead should be consulted via the 'Tech for Learning Leader' before a DPIA is also completed. If approved by the Trust EdTech Lead, the tool will be placed on the 'Approved AI tool register'.
- It is important to be transparent about how you're using AI, if unsure about a particular use, check with your technology for learning leader.
- AI should not be used solely to support any key decision making and special consideration should be given to the use of AI for marking and feedback, AI can often seem convincing when it comes to marking, but its effectiveness in this area is not yet proven. The process of marking and providing feedback provides opportunities for teachers to understand a pupil's/student's work more closely and risks being bypassed when completed solely by AI.

Student use of AI

There are a range of risks associated with students using AI tools. The use of any AI tool directly with students will need to be approved by the Trust EdTech Lead, as well as the headteacher in the school, and must meet the DfE's product safety expectations, particularly with regard to safeguarding.

4. Data Protection

AI tools may process or store data, often on external servers. **Any processing of personal data must comply with UK GDPR.**

- Personal data should not be input into any AI systems that will learn from the input, consult the 'Approved AI tools register' for tools that are approved for this purpose. Using tools that are unapproved for this purpose risks data breaches, which should be reported instantly in line with the Data protection policy.

AI systems often learn and evolve based on the data provided, raising significant data protection concerns. Staff must not input any school data into AI systems that aren't secure, for example the freely available version of ChatGPT.

In compliance with the General Data Protection Regulation (GDPR), our policy states that:

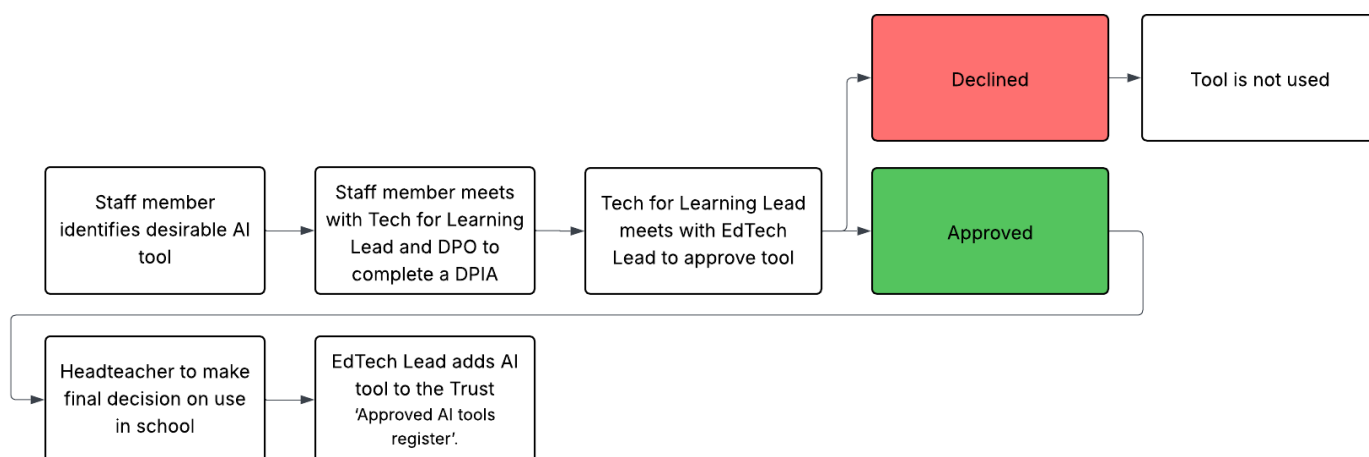
- Any AI tool used within the school environment must be approved by the Trust EdTech Lead as well as going through the DPIA process.
- No sensitive student data should be input into any AI system. For example, student ethnicity, health records or special educational needs.

- All staff members are required to participate in routine data protection training, which includes best practices in handling and interacting with AI platforms.

Key Principles:

- Personal data includes names, assessment records, and anything identifiable
- Lawful processing must have a clear basis; the most common of these are: public task, legitimate interest, or consent.
- Schools must not input personal or sensitive data into generative AI systems without approval from the EdTech Lead, DPIA, and Data Protection Officer (DPO).
- AI systems must not store or learn from personal data, to avoid this only trust approved AI tools should be used, as listed on the 'Approved AI tools register'.
- Schools must ensure data retention, deletion and storage policies are adhered to.

The process for AI tools is outlined below:



5. Intellectual Property

Separate from data protection, **intellectual property (IP)** refers to the ownership of original work, including student work.

Requirements:

- Teachers must not input student work into an unapproved AI tool (for example ChatGPT or some free plagiarism checkers), as the work produced may be the student's intellectual property and may be retained by the AI system.
- Staff should not share or upload copyrighted material into AI systems unless rights are held.
- AI systems are trained on a range of data, some of which may be copyrighted, we should avoid sharing widely work generated by AI.

- The DfE acknowledge that the legal landscape is evolving around copyright and AI and suggests some mitigation measures that we must all follow:
 - You should avoid public sharing (such as on school or college websites) of any content largely created by a generative AI tool, as there is potential for the output to resemble or contain copyrighted material.
 - Do not share AI-generated resources widely. For example, if you generate an image using AI, you should avoid placing it on your school or college website. Another example that should be avoided is publishing a policy created by an AI tool that used input from another school's policy without permission

6. Safeguarding and Online Safety

AI creates new online safety risks: deep-fakes, impersonation, fake chatbots, inappropriate outputs. The safety of our students remains paramount. There are particular risks within the digital realm where AI is utilised. While AI can be a powerful educational tool, its misuse can lead to serious consequences.

To support SLT to mitigate these risks, there will be a series of workshops for SLT members focusing on the evolving risks of AI and mitigations that can be taken. This will include the development of an AI action plan for each school.

- Any concerning behaviour or material generated by or encountered within AI platforms must be immediately reported, following the school and trust safeguarding procedures as well as Keeping Children Safe in Education Guidance.

Teachers should:

- Consider the constantly changing safeguarding risks brought about and follow the trust safeguarding policies
- Ensure tools used with students are age-appropriate, meet the DfEs product safety expectations and are approved for use in your school.
- Follow *Keeping Children Safe in Education policy* and school safeguarding procedures paying particular attention to any updates with regards to safeguarding and escalate concerns promptly
- If you encounter or generate any concerning behavior or material on AI platforms, you must report it immediately according to the school's safeguarding procedures.

7. Curriculum

Understanding AI's role, potential, and limitations in our world is crucial for students. To support this we commit to developing a curriculum that will integrate critical thinking skills and foundational knowledge about AI.

We commit to:

- Ensure that knowledge remains at the core of our curriculum to enable the critical judgment of AI-generated outputs.
- Develop opportunities within existing subjects to critically evaluate information, particularly content generated by AI, to equip students with the skills needed to discern misinformation and inaccuracies.
- Develop strands within the Computing and PSHE curriculum that addresses emerging concerns around content that could be generated by AI as part of Online Safety education and equip students with the skills needed to build healthy attitudes to AI.
- In all exams, the school will follow the JCQ guidance on AI in assessments.

Through this policy, our Trust is committed to harnessing the benefits of AI in an ethical, safe, and informed manner, preparing our students to navigate and contribute to an increasingly digital world.

8. Academic Integrity

AI can be misused in assessments.

Teachers should:

- Follow **JCQ guidance** on AI use in examined assessments
- Understand that AI detection tools are usually ineffective and only approved tools should be used for this purpose, other approaches should be considered such as redesigning independent work to make it less easy to complete with AI, or including an element of verbal assessment or personal reflection.

9. Monitoring, Training and Review

The pace of AI development demands a flexible and well-informed response. Schools must stay up to date.

Requirements:

- You can expect to receive regular updates on AI by the EdTech lead.
- Further training and guidance is available on the DfE website, co-developed by Chiltern Learning Trust: <https://www.gov.uk/government/collections/using-ai-in-education-settings-support-materials>
- We should all work together to maintain a culture of **human oversight, transparency, and critical reflection.**

10. Associated Documents and Roles

Document	Description	Owner
Data Protection Policy	GDPR compliance and DPIA process	Trust DPO
Safeguarding Policy and KCSIE policy	Online safety and child protection	Trust Director of Safeguarding
Business Continuity Plan	Outlines the measures in place to maintain service and access to systems/data in the event of potential incidents	Trust Operations Director

The 'Trust Approved AI Tools' register can be found in the trust's GDPR shared folder.