# Chiltern Learning Trust

# Artificial Intelligence Policy 2026–27

*Approved by the Board of Trustees:*
Review date: July 2027

**Contents**


1. Introduction
2. Responsibilities
3. Ethics and Product Safety
4. Data Protection
5. Intellectual Property
6. Safeguarding, Online Safety and Image Protection
7. Curriculum: Computing, PSHE and AI Literacy
8. SEND, Inclusion and AI Assistive Technology
9. Academic Integrity
10. Sustainability and Environmental Responsibility
11. Annual Review: 360-Degree Safe
12. Monitoring, CPD and Review
13. 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 tangible benefits. 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 Department for Education's Safe and Effective Use of AI in Education training materials. This policy provides our internal framework for the safe, ethical and effective use of AI across all CLT schools.

This updated policy reflects emerging risks including image scraping and AI-generated abuse material. It introduces strengthened requirements around school self-review,

curriculum development, SEND and inclusion, all trust staff CPD, and the environmental responsibilities associated with AI use. AI threats evolve rapidly, and schools are expected to treat this policy as a living framework, adapting their practice regularly in response to new guidance which will be communicated regularly via the Trust EdTech Lead.

## 2. Responsibilities

Using AI safely in education requires shared understanding and clarity of roles. Each school's AI action plan is expected to involve the following post-holders, working in coordination under headteacher oversight:

- Technology for Learning Leader: AI for teaching and learning, using AI critically, supporting CPD, overseeing the AI action plan and leading the school in working towards the AI quality mark. They have a key role in advising and working closely with:
  - Teaching and Learning Leader
  - Designated Safeguarding Lead (DSL)
  - Personal Development Lead
  - SENDCO
  - The Dedicated Safeguarding Lead
  - Computing Lead
  - Sustainability Lead

- School staff and central team: Use only trust-approved AI tools in line with this policy, data laws and only in approved ways following the trust's AI training. All trust staff must always be transparent about their use of AI and, if unsure about a particular use, seek clarification from their Technology for Learning Lead and Data Protection Officer.
- School and trust leaders: Set clear expectations for use and ensure all trust staff receive regular CPD on the safe and effective use of AI through a visit by the Trust EdTech Lead or by using the DfE materials, in particular Module 3 as referenced in Keeping Children Safe in Education. The Trust EdTech Lead will deliver a programme throughout the autumn term to support the development of a school AI action plans by running workshops at the relevant immersion sessions. This will include risk mitigation, a curriculum approach, inclusion and SEND considerations, and the environmental impact of AI.
- The Trust EdTech Lead: Supports schools to develop AI strategies, embed AI literacy across the curriculum, access CPD and implementation support, and conduct annual 360-degree safe reviews of AI practice.

This policy applies to all employees including the central team, contractors and volunteers associated with the trust's schools. All trust staff should be aware of the evolving potential for AI to reduce workload, 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.

# 3. Ethics and Product Safety

In line with the DfE guidance on the ethics of AI, the trust recognises both the transformative potential of AI in education and the significant risks it presents, particularly around ethical considerations. The DfE's guidance on Generative AI in Education underscores the importance of adhering to ethical standards, emphasising the potential biases and inequalities that could emerge through the use of any AI tool.

Risks include:

- AI tools being biased against particular groups, including biases related to SEND, gender, race, ethnicity and socio-economic background, including in outputs designed to support individual learners.
- AI creating factually incorrect materials through hallucinations (unintentional falsehoods generated by AI).
- AI tools being misused to generate harmful content, including deepfakes, manipulated images and synthetic abuse material.

## Approved Tools

- All trust staff must use only trust-approved tools as listed in the Approved AI Tool Register. These tools meet the DfE's Product Safety Expectations, including the requirement that the AI model does not train on prompts or uploaded materials.
- Before adopting any new AI tool, the Trust EdTech Lead must be consulted via the Technology for Learning Leader. The Trust EdTech lead will evaluate the tool against the DfE's product safety standards for generative AI and any other potential and emerging threats. A Data Protection Impact Assessment (DPIA) must be completed which will also contain reference to other risks identified that are particular to AI. If approved, the tool is added to the Approved AI Tool Register.
- All trust staff must be transparent about how they are using AI. If unsure about a particular use, check with the Technology for Learning Leader.
- Key decision making must be human-led, especially any decisions impacting child outcomes. Special consideration should be given to AI use for marking and feedback: AI can seem convincing in this area but its effectiveness is not yet proven, and the process of marking provides important opportunities for teachers to understand individual pupil progress.
- AI detectors are ineffective and should not be used in decision making. There is evidence that they are inaccurate and can discriminate against vulnerable groups including Neurodiverse students and those with English as an additional language. In view of this it is recommended that school review their homework policy, considering how homework can be made AI-proof by including personal reflection.

## Student Use of AI

It is ***particularly important*** that any AI tool used directly with students must be approved by the Trust EdTech Lead and the headteacher, and must meet the DfE's product safety expectations, particularly with regard to safeguarding. Student-facing AI tools must not be anthropomorphised or imply emotions, consciousness or personhood, in line with the DfE product safety standards.

# 4. Data Protection

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

- Use of AI tools not on the AI register is a serious breach. Using unapproved tools is a breach of policy and risks data breaches, which must be reported immediately in line with the Data Protection Policy. All data must be handled in line with the data protection policy.
- All trust staff must not input any data related to work into AI systems that are not secure. The freely available version of ChatGPT, for example, must not be used for work purposes.
- Schools must not input personal or sensitive data into generative AI systems without approval from the EdTech Lead, a completed DPIA, and sign-off from the Data Protection Officer (DPO) which will lead to the tool being added to the approved tools register.
- Schools must ensure data retention, deletion and storage policies are adhered to.

### Key Principles

- Personal data includes names, assessment records, and anything identifiable.
- Lawful processing must have a clear basis: public task, legitimate interest, or consent are the most common.
- AI systems must not store or learn from personal data. Only trust-approved tools, as listed on the Approved AI Tools Register, should be used.

# 5. Intellectual Property

Separate from data protection, intellectual property (IP) refers to the ownership of original work, including student work. Under UK copyright law, a pupil or student automatically owns the copyright of their written work, artwork and other creative outputs.

### Requirements

- Teachers must not input student work into an unapproved AI tool, as the work may be the student's intellectual property and could be retained by the AI system.
- All trust staff should avoid sharing widely any work generated by AI.
- Schools must avoid publicly sharing on school websites any content largely created by a generative AI tool, as there is potential for the output to contain copyrighted material.
- Teachers should be transparent about their use of AI, acknowledging it’s use and citing any sources that AI has referenced.

# 6. Safeguarding, Online Safety and Image Protection

The safety of our students remains paramount. AI creates new and evolving online safety risks including deepfakes, impersonation, AI companions, harmful AI-generated content (for example synthetic sexual materials and propaganda) and the criminal use of image scraping to produce synthetic abuse material. The threat landscape changes rapidly and schools must not treat this as a static area: regular review and all trust staff awareness are essential.

All trust staff must follow the trust's safeguarding policies and Keeping Children Safe in Education (KCSIE) guidance. Any concerning behaviour or material generated by or encountered within AI platforms must be reported immediately, following school and trust safeguarding procedures.

## AI Harms: Key Risks for All Trust Staff to Understand

All trust staff should be aware of the following safeguarding risks associated with AI and in particular generative AI, as outlined in the DfE's Safe and Effective Use of AI in Education training materials (Module 3).

Module 3 Video 2 must be viewed by all members of all trust staff and schools must check for understanding - a google form quiz is provided by the EdTech lead for this purpose.

These risks are evolving and schools must update their approach as new threats emerge:

- Deepfakes and synthetic media: AI can generate realistic audio, video and images of people saying or doing things they did not. This includes the manipulation of real images of children to produce synthetic child sexual abuse material (AI CSAM). UK law criminalises the creation, possession and distribution of tools designed to generate such material and synthetic generated material is treated by law with the same seriousness as actual abuse images.
- Image scraping: Automated tools can harvest photographs from public websites and social media at scale. These images can be processed using AI to generate harmful content, including for extortion, grooming and blackmail. This is one of the most significant and rapidly escalating child protection risks from AI. According to the Internet Watch Foundation, there was an >23,000% increase in Synthetic CSAM in 2025.
- AI tools that simulate or displace human relationships, including those integrated into mainstream platforms such as WhatsApp, can foster emotional dependency, undermine social and emotional development, give harmful advice, and engage in explicit or inappropriate conversations even when the user has disclosed they are a child. Schools must ensure students understand that AI tools are not real people.
- Grooming and radicalisation: Realistic AI avatars can be used for many forms of grooming. AI is also being actively used by terrorist and extremist groups to generate targeted recruitment content and radicalisation material, and to radicalise isolated individuals through one-to-one AI chatbot interactions. all trust staff must be aware of their Prevent duty and refer concerns appropriately where appropriate and follow normal safeguarding procedures in all cases.
- Misinformation and disinformation: AI tools can produce highly convincing false content. KCSIE explicitly includes misinformation, disinformation and conspiracy theories as online content risks that can be safeguarding harms to children. Schools must actively address these through curriculum, online safety work and all trust staff training.

- AI-generated child sexual abuse material (AI CSAM): The freely available nature of nudification apps and image generation tools means young people themselves may create, share or be victims of this type of material, sometimes for curiosity purposes and sometimes for blackmail. The trust provides effective filtering and monitoring solutions and schools should familiarise themselves with how they work and can be used to monitor student use. Always follow KCSIE guidance when responding to such incidents.
- Cognitive offloading: Over-reliance on AI can prevent students from developing deep understanding and independent thinking skills. This is a risk to both learning and to students' long-term capacity to engage critically with AI outputs.
- Bias and inequity: AI systems can reflect and reinforce societal biases, particularly in relation to SEND, gender, race and socio-economic background, in the content that they create. It's important to evaluate all outputs when using it to generate any content to be used in an educational context.
- There is evidence that these risks are heightened for students with neurodiverse students who may find it harder to understand the risks.

Schools must review their approach to these risks regularly. The annual 360-degree safe review (Section 11) provides the mechanism for doing so, but headteachers should ensure that the DSL and Technology for Learning Leader are monitoring developments and updating all trust staff as new threats emerge between annual reviews.

## Image Protection and publishing online

The trust has produced detailed guidance on Using Images Safely in CLT Schools, and all schools must follow this alongside the guidance produced by the UK Safer Internet Centre (Protecting Your Setting's Images from AI Manipulation and Abuse).

What schools **must do:**

- Drawing on the UK Safer Internet Centre guidance, Module 3 of the DfE training materials developed by the trust and the trust's own image safety guidance, the trust's position is that schools must avoid sharing images showing pupils' faces on publicly accessible platforms. Given the documented and increasing risk of image scraping and AI CSAM, **schools must:**
- Use only non-identifying photography: over-the-shoulder shots, backs of heads, group shots from a distance, or close-ups of work and activities rather than faces.
- Where pupil faces must be included in any shared platform including those that are password protected for parental access, always blur or add emoji overlays to anonymise individuals where consent is withheld.
- Limit public visibility of student images. Where identifiable images are used, place them behind a secure, password-protected area such as a parents' portal rather than on open social media.
- Apply a names-no-images or images-no-names approach on publicly accessible materials.
- Gain annual, informed consent from parents, carers and pupils (where competent) before sharing any images on any platform.
- Use only school-owned, approved devices to capture images of pupils. Personal devices must not be used.

- Have a system for logging who is using school-issued devices and the purpose for using them and ensure that students images are only shared internally as needed and mandated by the headteacher.
- Store all images securely in password-protected, restricted-access locations on the CLT network or Google Drive, student images should not be placed in drives that are open to the whole all trust staff body.
- Remove all image metadata (EXIF data, including location information) before publishing any image online.
- Ensure images do not appear alongside full names on any publicly accessible platform.
- Conduct termly or biannual audits of images published on school websites and social media, removing any that are out of date or no longer have valid consent.
- Remove and un-publish any images of any pupil who leaves the school community.
- Follow KCSIE and the trust safeguarding policy immediately if any image-based abuse, blackmail threat or incident involving AI-generated imagery is identified.
- Report blackmail threats to the police as a criminal matter. Do not pay or engage with demands.

The above rules also apply to school and digital brochures or anywhere that schools use images of students, print copies of materials can be shared directly with prospective parents.

# 7. Curriculum: Computing, Personal Development and AI Literacy

Understanding AI's role, potential and limitations is crucial for all students. The Government's Curriculum and Assessment Review recognises that the rise of AI “requires heightened media literacy, critical thinking and digital skills” (Curriculum and Assessment Review, 2026). The revised national curriculum, expected to be introduced for teaching in 2028, will embed AI literacy more formally across subjects. CLT schools are expected to be ahead of this curve, not waiting for statutory requirement before acting.

AI education must not sit in computing alone. It requires a whole-school approach, with coordinated contributions from computing, PSHE, personal development, and all subject areas. The Computing Lead and Personal Development Lead must work together, and their work should be reflected in the school AI action plan.

## Computing Curriculum

AI must be a core component of the computing curriculum, not an add-on. Schools must ensure that computing teaching addresses:

- How generative AI systems work, including how they are trained on data, how they generate outputs, and why they can produce biased or inaccurate results.
- The practical and ethical implications of AI, including AI bias, intellectual property, data privacy and the social impacts of automation.
- How to use AI tools critically and responsibly, including evaluating outputs, understanding hallucinations and prompting effectively.
- A progressive KS3 pathway that develops AI literacy across years 7 to 9, as a foundation for GCSE Computer Science and beyond.

### Personal Development, RSE and Health Education

The risks AI poses to young people's wellbeing, relationships and safety must be addressed explicitly in PSHE and personal development. The personal development curriculum at CLT is bespoke to each community and must continue to evolve as AI develops. Schools must ensure PSHE addresses:

- The risks of AI companion apps and chatbots, including emotional dependency, the blurring of human and AI relationships, and how AI tools can be used to manipulate young people. Students must understand that AI tools are not real people and should not replace human connection.
- Online safety in an AI world, including image-based abuse, deepfakes, AI-enabled grooming and the exploitation of images shared online.
- Critical thinking about AI-generated content, including how to identify misinformation and disinformation, and how AI can be used to create and amplify extremist content.
- Academic integrity and cognitive offloading: students must understand what it means to use AI responsibly in their learning, and the risks of over-reliance.
- The ethics of AI, including questions of fairness, bias, accountability and the environmental cost of AI systems.
- Common Sense Media and Childnet produce relevant resources for PSHE and personal development that schools can use and adapt.
- The harms that AI can facilitate, including deepfakes, image scraping, AI-enabled radicalisation, chatbots and friendships, pedagogical risks and the need to reflect on our own thinking processes, appropriate to the age group. All requirements of the statutory RSE and Health curriculum relating to AI.

### Across the Curriculum

- All subject areas should develop opportunities for students to critically evaluate information, particularly AI-generated content, building skills to discern misinformation and inaccuracies.
- In all exams, schools will follow the Joint Council for Qualifications (JCQ) guidance on AI in assessments.
- Schools should regularly review and refresh their curriculum offer in this area, and share effective practice across the trust in the scheduled immersion sessions for technology for learning leaders and personal development leads.

### Pedagogical risks

- We know that the pedagogical risks of AI bypassing thinking are significant and this should be considered when setting assessment tasks. It’s possible to design tasks that require personal reflection and focus on process over product. Equally, we may consider the approach to using AI and what is appropriate or not.

## 8. SEND, Inclusion and AI Assistive Technology

AI and assistive technology offer significant opportunities to support students with special educational needs and disabilities (SEND) and to reduce barriers to learning.

At the same time, schools must be alert to the particular safeguarding vulnerabilities that some students with SEND may face in relation to AI, including difficulty understanding that AI tools are not real people, heightened susceptibility to AI companion tools, and challenges in critically evaluating AI outputs.

### Opportunities

- AI can support inclusion through tools such as text-to-speech, speech-to-text, dictation technologies that adapt to atypical speech, screen readers, and applications that describe scenes using a phone camera.
- AI can support teachers and TAs in preparing differentiated resources, breaking down complex concepts, drafting all trust staff guides for supporting specific needs, and generating template letters and communications, reducing the significant administrative burden that falls on SEND teams.
- The starting point must always be the individual learner's specific needs and barriers, not their diagnostic label. A range of tools should be explored to understand what is possible, and an appropriately trained professional should always be involved in decisions about individual accessibility tools.
- Schools should explore the trust's EdTech Hub resources for inclusion and accessibility (edtechhub.co.uk/edtech-and-ai-for-inclusion-and-accessibility/) and engage the SENDCO in the school AI action planning process.

### Risks for Students with SEND

- Students who find it harder to understand the concept of bias, misinformation or AI's non-human nature may be particularly vulnerable to the harms associated with AI companion tools, and may struggle to critically evaluate AI outputs. Schools must consider this when making decisions about student-facing AI tools.
- Any AI tool used with students, including accessibility tools, must meet the DfE's product safety expectations and be approved by the Trust EdTech Lead and headteacher the added to the trust's approved AI tools register.
- AI systems must not be used to make automated judgements or predictions about individual pupils, students or all trust staff.

---

## 9. Academic Integrity

AI can be misused in assessments. Schools must maintain a culture in which students understand the difference between AI as a tool to support learning and AI as a means to bypass the learning process itself.

### Requirements

- Schools must follow JCQ guidance on AI use in examined assessments.
- AI detection tools are unreliable and must not be used as the primary method of identifying misuse. They can produce false positives that disproportionately affect certain groups, including students for whom English is an additional language. Professional judgement and knowledge of a student's typical work remain the most effective approach.
- Schools should redesign assessment tasks where possible to require personal reflection, individual reasoning and practical application of knowledge, which are harder for AI to complete convincingly.
- Clear expectations about when and how AI may or may not be used must be communicated to students and embedded from the earliest key stages.
- Any suspected AI misuse should be investigated by the teacher or assessor, with appropriate action taken in line with JCQ guidance and school policy.

# 10. Sustainability and Environmental Responsibility

A significant concern about the use of generative AI is its environmental impact. Training large AI models requires enormous computational power, and ongoing operation consumes substantial energy. Data centres use significant amounts of electricity, often from grids still dependent on fossil fuels, and large quantities of water for cooling. This contributes to carbon emissions and raises equity concerns about resource use in water-stressed regions.

Schools should:

- Ensure all trust staff understand the environmental implications of AI use. As part of CPD, all trust staff should consider whether AI is really the most appropriate tool for a given task, and avoid unnecessary repetition of resource-intensive prompts.
- Favour lighter-weight AI tools for routine tasks rather than large-scale reasoning models where these meet the need adequately.
- Encourage effective prompting to reduce the number of iterations needed to produce a useful output, which in turn reduces energy use.
- Incorporate AI's environmental impact into the curriculum, particularly in computing and geography, as part of climate and sustainability education. Students should understand how AI data centres work and what their environmental cost is.
- Engage the school sustainability lead in AI action planning, ensuring environmental responsibility is considered alongside safeguarding, curriculum and inclusion.

# 11. Annual Review

Given the pace of change in AI, schools must treat their AI practice as a living area of their safeguarding and school improvement work. New threats emerge regularly, guidance is updated, and tools change. Annual review is the minimum expectation. All CLT schools are required to conduct an annual 360-degree safe self-review which will relate to their use of AI using the SWGfL 360-safe tool.

## Requirements

- Each school must complete an annual 360-degree safe review (360safe.org.uk/), facilitated by the Technology for Learning Leader, to ensure that Online Safety and AI practices are kept up to date and reflect current safeguarding guidance.
- In addition the school should review with the following question
  - Is the school using only trust-approved AI tools on the Approved AI Tool Register?
  - Are all trust staff trained on the safe and effective use of AI, including on the safeguarding risks identified in the DfE training materials?
  - Is the school's approach to images and social media in line with current guidance, including this policy and the CLT Using Images Safely document?
  - Are we making full use of AI assistive technology to support equity of access for students with SEND and other additional needs?
  - Have we updated the computing curriculum to embed AI literacy as a core component, including coverage of AI harms?

    - Have we updated the RSE and Health curriculum and approach to Personal Development to address AI-related risks, including companion AI, emotional dependency, deepfakes and image-based abuse?
    - Are we actively addressing AI-enabled misinformation, disinformation and radicalisation risks in line with our Prevent duty?
    - Are we reviewing our online filtering and monitoring systems to ensure they are effective in identifying AI-generated harmful content and non-approved tool use content and feeding back to our managed service provider?
    - Are we considering the environmental impact of our AI use and embedding sustainability awareness around AI in the training and curriculum?
- The outcomes of the review must inform the school's AI action plan and be reported to the headteacher and relevant governor.
- The Trust EdTech Lead will support the review process and provide updated guidance where national or trust-level practice has changed.
- Between annual reviews, headteachers must ensure the DSL and Technology for Learning Leader are monitoring developments informed by the Trust EdTech Lead and Trust Safeguarding Director and updating all trust staff as significant new threats or guidance emerge.

# 12. Monitoring, CPD and Review

The pace of AI development demands a flexible, well-informed and proactive response. all trust staff CPD is central to keeping schools safe. Knowing about the risks and harms from AI is not a one-off exercise: as tools evolve and new threats emerge, CPD must be updated accordingly.

## CPD Requirements

- All trust staff must complete the DfE's Safe and Effective Use of AI in Education training Module 3 Video 2 and the associated knowledge-check circulated by the EdTech Lead to Technology for Learning Leaders, co-developed by Chiltern Learning Trust. This covers safeguarding risks, data protection, academic integrity, inclusion, AI in leadership and the curriculum. Links to the training are available via the Trust EdTech Lead.
- CPD should address all of the key risks identified in this policy, including image scraping and AI CSAM, AI companion risks, deepfakes, grooming and radicalisation, misinformation, cognitive offloading and environmental impact.
- School leaders must ensure that CPD is not a one-time event. As AI develops and new guidance is issued, all trust staff must be updated. The DSL and Technology for Learning Leader are responsible for monitoring developments and bringing updates to all trust staff attention.
- The Trust EdTech Lead will deliver a programme in the autumn term each year to support the development and updating of school AI action plans.
- CPD should include subject-specific guidance on how AI affects assessment, lesson planning and resource creation in different disciplines, and how AI assistive tools can support SEND learners.
- Schools should foster a culture in which all trust staff discuss AI openly, share what is working and raise concerns without hesitation.

### Training and Guidance Resources

- DfE Safe and Effective Use of AI in Education training materials: https://www.gov.uk/government/collections/using-ai-in-education-settings-support-materials
- UK Safer Internet Centre guidance on image protection: saferinternet.org.uk/education-images
- Common Sense Media AI literacy resources for PSHE and personal development.
- Childnet AI misuse and nudification lesson resources (years 13 to 17).

### Monitoring and Review

- Online safety policies must be regularly reviewed in line with KCSIE requirements to ensure they remain up to date with safeguarding issues as they emerge.
- Schools should maintain a culture of human oversight, transparency and critical reflection, ensuring AI is always used as an assistant rather than a replacement for professional judgement.
- This policy will be reviewed annually by the Trust EdTech Lead and presented to the Board of Trustees for approval.

## 13. Associated Documents and Roles

| Document | Description | Owner |
|---|---|---|
| Data Protection Policy | GDPR compliance and DPIA process | Trust DPO |
| Safeguarding Policy | Online safety and child protection | Trust Director of Safeguarding |
| CLT Using Images Safely in Schools | Guidance on photography, consent, image scraping and AI risks | Director of Safeguarding, EdTech Lead, Marketing Lead. |
| UK Safer Internet Centre: Protecting Your Setting's Images from AI Manipulation and Abuse | External guidance on image security for education settings | saferinternet.org.uk |
| DfE Safe and Effective Use of AI in Education Training | National training co-developed by CLT | Trust EdTech Lead / DfE |
| Business Continuity Plan | Measures to maintain service and access to systems/data in potential incidents | Operations / Contracts Manager. |
| Approved AI Tools Register | List of tools approved for use across CLT schools | Trust EdTech Lead working with the Trust DPO |

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