The Children First Learning Partnership

AI Policy

(Version 2)

The AI Policy in respect of the Children First Learning Partnership has been discussed and adopted by the Directors Board	
Chair of Board:	*Mrs N Chell*
Responsible Officer:	*CEO – Mrs A Rourke*
Agreed and ratified by the Directors Board on:	*21.05.2026*
To be reviewed: *May 2027*	

Contents

1. Introduction

Artificial Intelligence (AI) is rapidly reshaping the digital world our pupils inhabit. It appears both as standalone tools—such as chatbots and generative content platforms—and as built-in features within commonly used software. AI brings exciting opportunities to enhance learning, reduce teacher workload, support differentiation and expand access to rich learning resources. However, it also brings new safeguarding, ethical, data-protection and online-safety responsibilities.

The Children First Learning Partnership (CFLP) recognises that pupils in EYFS, Key Stage 1 and Key Stage 2 are particularly vulnerable to misleading information, inappropriate outputs, impersonation risks and emotionally persuasive digital content. As such, AI can only be used within the CFLP schools in ways that are age-appropriate, safe, transparent and guided by skilled adults.

This policy outlines the CFLP's commitment to ensuring that AI is used responsibly, ethically and in alignment with statutory duties. It explains how AI will be managed across the Trust, safeguarding expectations, curriculum opportunities, and the responsibilities of staff and leaders.

2. Vision & Strategic Intent

The CFLP's vision is to harness the benefits of AI without compromising safety, equity or human judgement. We aim to:

- ✓ Enhance teaching and learning through thoughtfully selected AI tools
- ✓ Support staff with workload-reducing applications
- ✓ Strengthen inclusion by offering personalised, multisensory learning support
- ✓ Equip pupils with essential digital literacy and critical-thinking skills
- ✓ Ensure staff and pupils understand AI's limitations, risks and potential biases
- ✓ Build digital resilience to help pupils navigate an increasingly AI-shaped world
- ✓ At all times, AI must act as a support, not a substitution for qualified professionals. The CFLP explicitly rejects the idea that AI can replace assessment, teacher expertise, individual relationships or professional judgement.

3. Purpose of the Policy

This policy provides a Trust-wide framework ensuring that:

- ✓ AI is used safely, ethically and transparently

- ✓ AI supports teaching and learning without undermining safeguarding
- ✓ All use complies with government and statutory guidance
- ✓ No AI tool is used without appropriate risk assessment
- ✓ Staff and pupils clearly understand expectations for safe behaviour
- ✓ Leaders and DSLs maintain appropriate oversight of AI systems

4. Scope

This policy applies to:

- ✓ All CFLP employees, contractors, governance members, volunteers
- ✓ All AI tools used across the Trust (local or cloud-based)
- ✓ All pupil-facing AI use
- ✓ Any AI integrated into existing school platforms
- ✓ Staff use of AI for planning, drafting or administrative tasks

5. Statutory Framework

This policy aligns with key statutory and regulatory requirements, including:

- **Keeping Children Safe in Education (KCSIE) 2025**
- Covers AI-related online safety risks including deepfakes, impersonation, extremist content, inappropriate outputs, and monitoring/filtering expectations.
- **DfE Generative AI in Education (2025)**
- Sets expectations for safe, purposeful, ethical adoption of AI with human oversight.
- **DfE Filtering & Monitoring Standards (2025)**
- Requires filtering and monitoring systems to assess dynamic, AI-generated content.
- **DfE AI Product Safety Expectations**
- Requires AI systems to have moderation, transparency, and safety controls.
- **Data Protection Act 2018 & UK GDPR**
- Regulates lawful and secure handling of pupil data.

6. Roles & Responsibilities

Role	Responsibilities
Board of Directors	• Oversees AI safety and compliance across the Trust • Approves policy and ensures resources are in place
Chief Executive Officer (CEO)	• Ensures consistent Trust-wide implementation • Oversees staff training and risk management
Designated Safeguarding Leads (DSLs)	• Assess AI-related safeguarding risks • Ensure monitoring and filtering systems capture AI content • Respond to and record incidents involving AI-generated harm

Data Protection Officer (DPO)	• Conducts DPIAs • Ensures GDPR compliance • Evaluates vendor privacy assurances
School Leaders	• Apply this policy within their school • Ensure staff training and safe practice
All Staff	• Use AI responsibly • Supervise pupils • Follow approval processes • Never input personal data
Pupils	• Follow AI safety expectations • Never enter personal details • Engage in supervised, age-appropriate AI experiences

7. AI Tool Approval Process

Before any AI tool is made available to pupils or staff, it must undergo a thorough review to determine whether it is safe, purposeful and compliant.

Step	Title	Description
1	Identify Need & Purpose	A staff member or school leader identifies a clear educational, accessibility or workload-related justification for the AI tool. Tools without proven value are not progressed.
2	Safeguarding Review (DSL)	The DSL evaluates risks including harmful or misleading content, impersonation, deepfake potential and ensures Trust filtering and monitoring systems can safely manage AI outputs.
3	Data Protection Review (DPO)	The DPO checks GDPR compliance, confirms data minimisation, ensures no personal data is processed, and verifies the vendor does not train models on school data.
4	Cybersecurity Check (IT Team)	The IT team validates the tool against Cyber Essentials requirements, ensuring secure configuration, safe integration, and no vulnerabilities.
5	Educational Suitability (AI Lead)	The AI Lead assesses curriculum alignment, accessibility for SEND/EAL learners, fairness, avoidance of bias, and overall educational value.
6	Controlled Pilot Study	A small supervised pilot is conducted to test real-world safety, accuracy, usability, pupil experience and educational impact.
7	Final Approval & AI Register Entry	If successful, the tool is formally approved, added to the CFLP AI Register and issued with clear usage guidance for staff.

8. Staff Use of AI

AI can support teachers with planning, resource creation, differentiation and administrative efficiency. However, staff must always supervise and check AI outputs carefully.

Permitted Uses	Prohibited Uses
Drafting lesson ideas and visual resources Simplifying texts for SEND/EAL pupils	Inputting personal, identifiable or sensitive information

Creating vocabulary lists or scaffolded materials Drafting letters or templates (non-confidential) Summarising policy documents	Using AI for marking, feedback or assessment Drafting safeguarding, HR or disciplinary documentation Generating profiles or predictions about pupils Using unapproved or unsafe AI platforms

9. Pupil Use of AI

Pupil use of AI within the CFLP is always carefully planned and tightly controlled. All AI interactions must be supervised, structured, purposeful, age-appropriate, and guided by a responsible adult. AI is introduced gradually across year groups so that pupils develop confidence, digital awareness, and critical-thinking skills in a safe and developmentally appropriate way.

9.1 EYFS – Year 2

In the early years, pupils explore AI concepts only at a very basic level and always through teacher-led activities. Learning focuses on helping children distinguish between what is real and what is pretend, developing simple digital-safety habits, and engaging in guided exploration of AI-generated images or audio.

9.2 Year 3 – Year 4

Pupils begin to recognise that AI systems make mistakes and that not all digital information is reliable. Teaching introduces the idea that AI can misunderstand prompts, produce errors or show bias. Pupils engage in safe, limited text-based interactions with AI in structured lessons where adults model responsible questioning and fact-checking.

9.3 Prohibited Pupil Behaviours

To protect pupils and uphold safeguarding expectations, pupils must never:

- Use AI to complete homework or produce assessed work.
- Share personal details, photos, videos or identifiable information with any AI tool.
- Attempt to bypass school filtering or monitoring controls.
- Create or manipulate synthetic media involving real individuals.
- Generate harmful, deceptive or inappropriate content.

10. Prohibited AI Tools

To protect pupils and staff from identifiable safeguarding, data protection, security and ethical risks, the Children First Learning Partnership maintains a clear list of AI tools and technologies that are **strictly prohibited** for use in all CFLP schools.

This section is not exhaustive; rather, it establishes **categories of tools** that pose unacceptable risk under **KCSIE 2025 online safety duties**, **DfE AI guidance**, **DfE AI Safety Standards**, and **GDPR requirements**. The CFLP will update this list in response to emerging technologies and risks.

Prohibited Category	Examples of Prohibited Tools	Reason for Prohibition
19.1 Unfiltered, Public Generative AI Models	ChatGPT (public version), Google Gemini (public version), Claude (public version), OpenAI Playground, HuggingFace public models	Cannot be filtered/monitored safely. KCSIE 2025 identifies harmful AI-generated content and impersonation risks requiring monitoring and filtering compliance.
19.2 Deepfake, Face-Swap, Voice-Cloning Tools	Reface, FaceMagic, DeepFaceLab, ElevenLabs free-tier, Voicemod	KCSIE 2025 recognises deepfakes and impersonation as online safety risks that cannot be safely controlled in school settings.
19.3 AI Tools That Require, Store or Process Personal Data	AI photo apps, consumer transcription tools, apps storing conversation history	Breaches GDPR data minimisation and DfE expectations for lawful processing of children's data.
19.4 Unsupervised or Age-Restricted Pupil-Facing AI Platforms	Public chatbots, tools requiring 13+/16+/18+ accounts, unmonitored AI chatrooms	DfE guidance requires close supervision of pupil use and adherence to legal age restrictions.
19.5 AI Marking, Grading or Prediction Tools	Automated essay graders, attainment prediction systems, behavioural profiling AI	DfE emphasises AI must not replace teacher judgement; risks of bias and inaccuracy.
19.6 Tools Without Transparent Safety or Data Standards	AI with unclear data storage, unknown training data, no safety disclosures	DfE AI Safety Standards require transparent data handling, safety testing, filtering and monitoring.
19.7 Tools Not Approved Through CFLP AI Tool Approval Process	Any AI tool not assessed by DSL, DPO, IT, AI Lead and the Digital & AI Strategy Group	DfE requires risk assessment before adopting AI; KCSIE requires leadership oversight of digital tools.

11. Curriculum & AI Literacy

CFLP is committed to ensuring that all pupils develop the knowledge, skills and critical understanding needed to navigate a world increasingly shaped by artificial intelligence. AI literacy is woven

progressively throughout the Computing, PSHE, English, Science and Citizenship curriculum in age-appropriate ways, enabling pupils to question, evaluate and understand digital content safely and responsibly.

Through a structured and developmental approach, pupils learn to recognise how AI works, identify its limitations, understand where mistakes can occur, and develop the ability to interrogate and challenge information thoughtfully. This supports CFLP's wider commitment to safeguarding, digital resilience and building informed, responsible digital citizens.

11.1 EYFS (Early Years Foundation Stage)

At this early stage, learning focuses on building foundational digital awareness in safe, highly supervised environments. Pupils explore:

• Real vs pretend – beginning to understand the difference between fictional and real content.
• Who to ask for help – recognising that adults provide guidance when technology is confusing or concerning.
• Basic cause and effect – noticing that digital devices respond to simple actions, forming the basis of early algorithmic thinking.

11.2 KS1 (Years 1–2)

Pupils begin to understand that digital information is not always reliable. Teaching includes:

• AI makes mistakes – recognising that computers do not always give correct answers.
• Not everything online is true – developing early media-literacy awareness.
• Simple fact-checking – encouraging pupils to verify information with a trusted adult.

11.3 Lower KS2 (Years 3–4)

As pupils' reasoning develops, they engage with the basic principles behind AI systems. They learn:

• Algorithms and rules – understanding that computers follow instructions, not thoughts.
• Dataset fairness – exploring how information used to train AI can contain bias.
• Identifying altered or misleading content – spotting simple manipulation or exaggeration.

12. Data Protection & DPIAs

A Data Protection Impact Assessment must be completed for any AI system. This assesses:

- Data minimisation
- Inference risks
- Algorithmic fairness
- Vendor transparency
- Storage location
- Security of data flows

- Personal data must never be entered into generative AI platforms.

13. Cybersecurity (Including Cyber Essentials)

CFLP adheres to Cyber Essentials controls to protect systems and data:

- Secure firewalls and filtering
- Strong access control
- Malware protection
- Patching and update regimes
- Safe configuration of devices

AI increases cyber risks such as phishing, impersonation and synthetic identity fraud; staff receive training to recognise and prevent these.

14. Monitoring & Evaluation

CFLP is committed to ensuring that the use of Artificial Intelligence across all schools is safe, impactful and aligned with our educational values. To achieve this, the Trust undertakes regular and systematic monitoring and evaluation of how AI tools are being used in practice. This process ensures that AI continues to support teaching, learning and operational efficiency while maintaining high standards of safeguarding, equity and quality.

Monitoring and evaluation activities are embedded into existing school review and quality-assurance processes. Findings are used to inform future decision-making, refine staff training, update approved-tool lists and adjust curriculum delivery. The purpose is not only to check compliance, but to ensure that AI genuinely adds value to teaching and learning across the Partnership.

The CFLP will evaluate the following key areas:

14.1 Effectiveness of AI Use

The Trust assesses whether AI tools are achieving their intended purpose, such as reducing workload, enhancing lesson resources or supporting accessibility. This includes gathering feedback from staff, reviewing examples of AI-supported practice and identifying any patterns of success or challenge.

14.2 Impact on Learning and Workload

Monitoring focuses on how AI influences pupil learning, engagement and progress, and whether teacher workload is reduced in meaningful ways. Evaluation considers whether AI-supported resources improve clarity, accessibility or differentiation for pupils, and whether staff feel AI is helping them work more efficiently without compromising accuracy or professional judgement.

14.3 Safeguarding Patterns Related to AI

Safeguarding teams monitor any concerns involving AI, including exposure to inappropriate content, impersonation risks, misinformation, or attempts to bypass filters. This oversight ensures AI-related risks are identified early and acted upon promptly. Trends in safeguarding logs are reviewed to inform future training, updates to filtering systems and policy refinement.

14.4 Equity Implications for SEND/EAL Pupils

The CFLP evaluates whether AI tools support or hinder inclusion. Monitoring checks that AI benefits all pupils and does not disproportionately disadvantage particular groups. This includes reviewing how effectively AI supports communication, accessibility, vocabulary development and personalised learning for SEND and EAL learners.

14.5 Accuracy and Reliability of AI Tools

Because AI tools can produce errors or biased outputs, the CFLP reviews the frequency and impact of inaccuracies. Staff are encouraged to report issues, and Trust leaders assess whether tools remain reliable enough for classroom use. Tools that consistently produce unreliable results may be removed from the Approved Tools Register.

14.6 Quality of Pupil AI Literacy

Schools evaluate pupils' understanding of AI concepts, digital literacy skills and critical-thinking development. This includes reviewing curriculum outcomes, observing classroom learning and identifying areas where pupils require additional support—such as recognising manipulated media, questioning AI-generated information or understanding AI's limitations.

14.7 Continuous Improvement

Findings from monitoring and evaluation activities are shared across the Trust to support collective learning. They inform updates to training, changes to the AI Approval Process, adjustments to safeguarding practice and modifications to the curriculum. As AI evolves, the CFLP remains committed to updating its approach to ensure ongoing safety, relevance and educational benefit.

15. Staff Training

The CFLP recognises that the safe and effective use of Artificial Intelligence in education depends on the knowledge, confidence and professional judgement of staff. AI is an evolving technology, and therefore continuous professional development is essential to ensure that every member of staff understands both the opportunities and the risks associated with its use.

To support this, the CFLP provides annual, structured AI training for all staff, alongside enhanced training for designated safeguarding and leadership roles. This training ensures that staff can make informed decisions, model safe behaviours for pupils, and apply the CFLP AI Policy confidently within their daily work.

15.1 Core Training for All Staff

All staff participate in annual training that builds their understanding of AI and equips them to use AI safely and responsibly. This training includes:

• Safe and responsible AI use – understanding when AI is appropriate and how to use it without compromising safety, professionalism or pupil wellbeing.
• Ethical considerations and bias – recognising how AI systems may reproduce bias, stereotypes or inaccurate information, and learning to mitigate these risks.
• Recognising deepfakes and synthetic media – developing confidence in identifying manipulated or fabricated content that could be used to mislead or harm.
• Identifying misinformation and AI hallucinations – learning how AI may generate false or misleading content, and how to verify accuracy before use.
• GDPR and data protection awareness – reinforcing staff responsibilities around data minimisation, lawful processing and the absolute prohibition on entering personal data into AI systems.
• Understanding AI limitations and operational risks – developing awareness of how and why AI tools fail, generate errors or behave unpredictably.
• KCSIE AI-related safeguarding duties – ensuring staff understand how AI fits into the broader safeguarding system, including impersonation, grooming, misinformation and online safety.

15.2 Enhanced Training for DSLs and Leaders

DSLs, senior leaders and digital governance staff receive additional, role-specific training addressing:

• AI-specific safeguarding risks, including deepfakes, online grooming patterns and synthetic identities.
• Filtering and monitoring responsibilities, ensuring AI-generated content is captured and safely managed.

• Cybersecurity awareness, understanding how AI tools can enable phishing, impersonation or data extraction.
• Risk assessment and the CFLP AI Tool Approval Process.
• Oversight and governance of AI-related risks, responsibilities and incident management.

16. Transparency & Communication

The CFLP is committed to ensuring that the use of Artificial Intelligence across all schools within the Partnership is open, transparent and clearly understood by staff, pupils, parents, governors and the wider community. Transparency is a core safeguarding principle and an essential component of maintaining trust in the responsible adoption of new technologies.

AI has the potential to influence teaching, learning, operational processes and pupil experience. For this reason, the CFLP believes that all stakeholders should have access to clear information about where, how and why AI is being used within the Trust. Transparent communication also helps ensure that expectations are consistent, that concerns can be raised early, and that AI is implemented safely and appropriately.

17. Maintaining an AI Register

The Trust maintains a summary of the CFLP AI Approved Tools Register, which lists all AI tools that have been formally reviewed and approved. This promotes openness and provides reassurance that every tool used in school has undergone appropriate safeguarding, data protection and cybersecurity assessment.

17.1 Informing Parents and Carers About AI Use

Parents and carers are kept informed about AI use through school websites, letters, curriculum updates and digital-safety events. This helps families understand the role AI plays in learning and supports them in reinforcing safe digital habits at home.

17.2 Digital-Safety Information Sessions

The CFLP delivers regular digital-safety workshops and information sessions for parents and pupils. These sessions include guidance on recognising misinformation, understanding AI-generated content, and supporting safe online behaviour. They strengthen the home–school partnership and promote shared responsibility for AI safety.

17.3 Labelling AI-Assisted Content

Where appropriate, staff label AI-assisted resources or documents. This models transparent practice for pupils and helps them understand how AI contributes to digital content creation.

17.4 Responding to Questions and Concerns

Schools maintain open channels for staff, pupils, parents and governors to raise questions or concerns about AI use. Feedback is welcomed, and responses are provided promptly to ensure confidence and clarity around the implementation of AI across the Trust.

18. Policy Review

The rapid evolution of artificial intelligence means that this policy cannot remain static. The CFLP recognises that new AI capabilities, emerging risks, and changes to national expectations may significantly affect how AI should be used within education. For this reason, the AI Policy is treated as a **living document**, subject to regular scrutiny and adaptation to ensure continued safety, compliance and relevance.

The CFLP is committed to ensuring that its approach to AI remains aligned with the latest Department for Education (DfE) guidance, Keeping Children Safe in Education (KCSIE) requirements, data-protection obligations and sector best practice. The Trust will therefore keep this policy under active review and will update it whenever necessary to maintain high standards of safeguarding, data security and educational quality.

The policy will be formally reviewed:

- **Annually**

An annual review allows the Trust to reflect on developments in AI, update processes in line with national guidance, evaluate outcomes from school practice, and ensure all content remains up to date and legally compliant.

- **After any significant incident involving AI**

If an AI-related safeguarding, data-protection or cybersecurity concern arises, the policy will be reviewed immediately. This ensures lessons are learned, risks are addressed, and controls are strengthened without delay.

- **Following updates to DfE guidance, KCSIE or statutory standards**

Changes to national guidance—particularly those relating to online safety, AI use in education, data protection or filtering and monitoring—will trigger a policy update to ensure the CFLP remains fully compliant with statutory expectations.

- **When new AI risks, tools or technologies emerge**

AI technologies develop at pace, and new tools may introduce unanticipated safeguarding, security or ethical risks. If emerging technologies significantly alter the AI landscape, the policy will be reviewed to ensure appropriate safeguards and governance arrangements are in place.

GLOSSARY OF TERMS

AI (Artificial Intelligence)
Systems capable of performing tasks that usually require human intelligence.

Generative AI
AI models that create new content, such as text, images or audio.

Deepfake
Fabricated or manipulated media designed to imitate real individuals.

Algorithm
A set of rules or steps followed by computers to solve a problem.

Filtering
Blocking access to harmful content online.

Monitoring
Reviewing digital activity to identify safeguarding risks.

Misinformation
False or misleading information spread unintentionally or deliberately.

DPIA (Data Protection Impact Assessment)
A GDPR tool for assessing risks to data privacy.

Cyber Essentials
The UK Government's baseline cybersecurity standard.

Synthetic Media
Digitally generated content (images, voices, videos) that appears real.

Version Control:

Version	Date	Amendment	By
2	27/03/2027	Policy rewritten	CEO