



Use of artificial intelligence (AI) policy

Kings Academy Trust

Approval body:	Board of trustees	Approval date: To be confirmed
Last reviewed on:	September 2026	
Next review due by:	September 2027	

Contents

Contents	2
1. Aims and scope	2
2. Legislation.....	3
3. Regulatory principles	3
4. Roles and responsibilities	4
5. Use of AI by staff across the trust, trustees and local governors	5
5.2.1 Filtering and monitoring.....	6
6. Educating pupils about AI	8
7. Use of AI by pupils.....	8
8. Formal assessments.....	9
9. Staff training.....	9
10. Breach of this policy.....	10
11. Referral to our child protection and safeguarding policy	10
12. Monitoring and transparency	11
13. Links with other policies.....	11

1. Aims and scope

At Kings Academy Trust, we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole trust community.

This policy covers the use of AI tools by staff across the trust, trustees, local governors and pupils. This includes generative AI tools such as ChatGPT, Microsoft Copilot and Google Gemini (this list is not exhaustive).

This policy aims to:

- Support the use of AI to enhance teaching and learning
- Support staff across the trust to explore AI solutions to improve efficiency and reduce workload
- Prepare staff across the trust, trustees, local governors and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff across the trust, trustees, local governors and pupils
- Protect the privacy and personal data of all staff across the trust, trustees, local governors and pupils in compliance with the UK GDPR

1.1 Definitions

This policy refers to both 'open' and 'closed' generative AI tools. These are defined as follows:

- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- Enterprise or closed generative AI tools may offer additional contractual and technical controls. They are not automatically safe or approved: security depends on the account configuration, access controls, retention, model-training settings, subprocessors and international data-transfer arrangements.

2. Legislation

This policy complies with the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- Equality Act 2010, including the Public Sector Equality Duty
- Copyright, Designs and Patents Act 1988

The Trust will also have regard to the current versions of the following official guidance and regulatory materials:

- Department for Education: Generative artificial intelligence in education
- Department for Education: Data protection in schools, including guidance on generative AI and the Data (Use and Access) Act 2025
- Department for Education: Generative AI product safety standards
- Department for Education: Keeping Children Safe in Education (KCSIE, 2026)
- Department for Education: filtering, monitoring and cyber security standards for schools and colleges
- Information Commissioner's Office guidance on AI, data protection, profiling and automated decision-making
- Joint Council for Qualifications guidance on AI use in assessments and relevant Ofqual resources

3. Regulatory principles

As a trust, we apply the five cross-sector principles in the government's pro-innovation approach to AI regulation alongside all binding legal duties.

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	• Ensure that AI solutions are secure and safe for users and protect users' data • Ensure we can identify and rectify bias or error • Anticipate threats such as hacking
Appropriate transparency and explainability	• Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate

REGULATORY PRINCIPLE	WE WILL ...
Accountability and governance	• Ensure that the board of trustees, Local governing body and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology • Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

4. Roles and responsibilities

4.0 Trust-level AI lead

Our generative AI trust lead is David Donnelly. They are responsible for the strategic oversight of AI use across the trust.

4.1 Board of trustees

The board of trustees will:

- Take overall responsibility for monitoring this policy and holding school leaders to account for its implementation in line with the trust's AI strategy
- Review and update the AI policy as appropriate, and at least annually.
- Ensure school leaders are appropriately supported to make informed decisions regarding effective and ethical use of AI across the trust
- Sign off approved AI tools and uses only after appropriate data protection, safeguarding, equality, security and product-safety checks have been completed, including a data protection impact assessment (DPIA) where required

Trustees will adhere to the guidelines below to protect data when using generative AI tools themselves:

- Use only approved AI tools (see section 5)
- Seek advice from the data protection officer / IT / as appropriate
- Confirm that the exact tool, account type and intended use have been approved by the Trust
- Do not enter personal data into an AI tool unless that specific processing has been approved following advice from the DPO and all required safeguards are in place
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

4.2 School leaders

School leaders will:

- Take responsibility for the day-to-day leadership and management of AI use in their school
- Liaise with the data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation
- Ensure that the guidance set out in this policy is followed by all staff
- Ensure staff are appropriately trained in the effective use and potential risks of AI

- › Make sure pupils are taught about the effective use and potential risks of AI

4.3 Trust data protection officer (DPO)

The trust-level data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

Our DPO is Satswana and is contactable via admin@satswana.com.

4.4 Safeguarding leads

Safeguarding leads are responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:

- › Being aware of new and emerging safeguarding threats posed by AI
- › Updating and delivering staff training on AI safeguarding threats
- › Responding to safeguarding incidents in line with the current version of Keeping Children Safe in Education (KCSIE), including KCSIE 2026 from 1 September 2026

4.5 All staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy.

To protect data when using generative AI tools, staff must:

- › Seek advice from the data protection officer / IT lead as appropriate
- › Confirm that the exact tool, account type and intended use have been approved by the Trust
- › Do not enter personal data into an AI tool unless that specific processing has been approved following advice from the DPO and all required safeguards are in place
- › Acknowledge or reference the use of generative AI in their work
- › Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

4.6 Pupils

Pupils must:

- › Follow the guidelines set out in section 7 of this policy ('Use of AI by pupils')

5. Use of AI by staff across the trust, trustees and local governors

5.1 Approved use of AI

At Kings Academy Trust we are committed to helping staff, trustees and local governors reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any member of staff, trustee or local governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff, trustees or local governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the trust has approved its use doesn't mean it will always be appropriate.

The table below sets out the approved AI tools and the approved uses for each tool.

Approved tools	Approved uses
KeyGPT	Letter to parents/carers Job descriptions and adverts Interview questions
Microsoft Copilot (approved Trust account)	Information gathering and policy-writing support
Chalkie AI	Lesson Planning
Arbor AI	Letter to parents/carers
Google NotebookLM (approved Trust account)	Research
Summary AI	Note-taking in non-sensitive meetings only, subject to approval and participant notice
ChatGPT (approved Trust account only)	Research and policy-writing support

5.2 Process for approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. They should contact their senior leader to discuss any ideas they may have with regards to using AI, so they can take the suggestions forward if they deem it to be a satisfactory new method of working.

David Donnelly is responsible for signing off approved AI tools and uses, taking account of advice from the DPO, safeguarding and IT leads and the results of the Trust's documented risk assessment.

Before approval, the Trust must document the intended purpose, users, lawful basis, expected benefit, risks, controls, owner and review date. The assessment must confirm:

- whether a DPIA, equality impact assessment or update to a privacy notice is required
- the provider's age restrictions and alignment with DfE product safety standards
- data retention, model-training use, access controls, subprocessors, security, contractual terms and international transfers
- appropriate safeguarding, filtering, monitoring and cyber security controls

5.2.1 Filtering and monitoring

The Trust will maintain appropriate filtering and monitoring systems for school devices and networks, including where generative AI tools are accessed. Their effectiveness will be reviewed at least once every academic year by the responsible member of the senior leadership team, supported by the designated safeguarding lead and IT support.

The review will include checks that filtering operates appropriately on all internet-connected devices in every relevant location. The Trust will retain a record of the checks, outcomes, actions and responsible owners. Relevant leaders and staff must understand the controls in place, manage them effectively and know how to escalate concerns.

5.3 Data protection and privacy

Personal data, special category data and confidential information must not be entered into an AI tool unless the exact tool and processing activity have been specifically approved following DPO advice and all required legal, contractual and technical safeguards are in place.

Any unauthorised disclosure of personal or sensitive information to an AI service must be reported immediately as a suspected personal data breach. The Trust will assess and manage the incident under its personal data breach procedure and data protection policy.

Please also refer to section 10 of this policy.

5.3.1 Use of AI in sensitive meetings

Regardless of whether an AI tool is otherwise approved, AI tools must not be used in meetings or discussions involving identifiable safeguarding or child protection information, special category personal data, or other confidential pupil or staff information. This prohibition includes AI meeting assistants, bots, transcription, recording, summarisation and automated note-taking tools.

Participants must not enable an AI assistant for such a meeting or upload any audio, transcript, minutes, notes or other meeting content to an AI service. Where a meeting record is required, staff must use the Trust's authorised non-AI arrangements and follow the data protection, records management and safeguarding policies.

5.3.2 Automated decision-making and profiling

AI must not make the final or solely automated significant decision about a pupil, parent/carer, applicant or member of staff. This includes decisions concerning admissions, exclusions, assessment outcomes, safeguarding, SEND provision, recruitment, disciplinary action or staff performance.

Any proposed exception must be approved in advance by the Trust AI lead and DPO. It must have a documented lawful basis, meaningful human involvement, appropriate safeguards for special category data, clear information for affected individuals and rights to make representations, obtain human intervention and contest the decision. A DPIA must be completed where required.

5.4 Intellectual property

AI services may retain or use submitted content to operate, evaluate or improve their models, depending on the provider, account type and settings. These arrangements must be checked as part of approval and kept under review.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions.

Kings Academy Trust will not allow or cause intellectual property, including pupils' work, to be used to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

5.5 Bias

We are aware that AI tools can perpetuate or amplify bias, including bias affecting protected characteristics under the Equality Act 2010. Critical review, equality impact consideration and fact- and sense-checking must be applied before relying on AI output.

Kings Academy Trust will ensure we can identify and rectify bias or error by training staff in this area.

We will also regularly review our use of AI to identify and correct any biases that may arise.

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

<https://www.kingsacademytrust.org/documents/policies/complaints-handling-policy.pdf>

AI-related data protection complaints will be handled under the Trust's data protection complaints procedure. They will be acknowledged within 30 days and answered without undue delay, in accordance with the Data (Use and Access) Act 2025.

5.6 Raising concerns

We encourage staff to speak to their school leader in the first instance if they have any concerns about the potential use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

5.7 Ethical and responsible use

Kings Academy Trust will always:

- Use generative AI tools ethically and responsibly
- Remember the principles set out in our trust's equality policy when using generative AI tools
<https://www.kingsacademytrust.org/documents/policies/equality-policy.pdf>
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff members, trustees and local governors must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt

6. Educating pupils about AI

Here at Kings Academy Trust we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make best use of generative AI.

- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content

Pupils will also be taught to recognise and respond to the four categories of online risk identified in KCSIE:

- Content – exposure to illegal, inappropriate or harmful material, including misinformation, disinformation, pornography and AI-generated harmful content.
- Contact – harmful interaction with other users or generative AI applications that simulate people, including grooming, exploitation and manipulation.
- Conduct – online behaviour that causes or increases the likelihood of harm, including making, sending or receiving explicit images generated or altered using AI, impersonation and online bullying.
- Commerce – risks including scams, phishing, inappropriate advertising and financial exploitation.

7. Use of AI by pupils

Kings Academy Trust recognises that AI has many uses to help pupils learn.

- As a research tool to help them find out about new topics and ideas

- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

- Pupils may use only Trust-approved tools, through approved accounts, in accordance with provider age restrictions and with appropriate supervision, safety settings, filtering and monitoring.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools:

- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

We consider any unattributed use of AI-generated text or imagery to be plagiarism and will follow our plagiarism procedures as set out in schools exams policies.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt
- Pupils should be provided with training on the use of AI through the curriculum and online safety.

8. Formal assessments

Kings Academy Trust will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments. See our trust exams / assessment policy for more details.

We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on [AI use in assessments](#).

The Trust will also take account of current Ofqual resources on AI and coursework integrity and will ensure that centre procedures, staff guidance and pupil messaging remain consistent with the latest JCQ requirements.

9. Staff training

Staff will be kept up to date with developments in AI, with continued CPD and updates in the availability of AI and new AI programmes available across the Trust. They will be able to develop and improve their practice on a regular basis with access to

- continuing professional development (CPD) opportunities on AI through the National College.
- training on new AI programmes
- changes in policy and updates on new developments will be shared with staff across the trust.
- All staff, including those who do not work directly with children, must read KCSIE 2026 Part One in full and follow the applicable school child protection and safeguarding procedures.

- Safeguarding and online-safety training will cover AI-generated and manipulated imagery, deepfakes and deep nudes, AI-enabled grooming, impersonation, coercion and sexual extortion.
- Staff will be trained to receive and record disclosures appropriately, report concerns immediately to the DSL, avoid viewing or forwarding illegal images, and understand their responsibilities for filtering and monitoring.
- Safeguarding and child protection training, including online safety, will be provided at induction, regularly updated and supported by updates at least annually.

10. Breach of this policy

10.1 By staff

Breach of this policy by staff will be dealt with in line with the trust's staff code of conduct.

Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members must cooperate with any investigation into a suspected breach of this policy. Access will be obtained only through authorised IT, HR, data protection or safeguarding procedures and must be lawful and proportionate.

- Relevant prompts, outputs, files, account records and audit logs may be examined where necessary
- Staff must not disclose passwords, passkeys or authentication codes

You must report any breach of this policy, either by you or by another member of staff, to your senior leader immediately.

10.2 By trustees or local governors

Trustees or local governors found in breach of this policy will be handled by the CET team following the appropriate steps and procedures.

10.3 By pupils

Any breach of this policy by a pupil will be dealt with in line with the trust's behaviour policy <https://www.kingsacademytrust.org/documents/policies/behaviour-and-anti-bullying-policy.pdf>

11. Referral to our child protection and safeguarding policy

The school is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse material, including AI-generated or manipulated imagery
- Harmful content
- Harmful advertisements and promotions

- Bullying
- The making or sharing of nudes and semi-nudes involving a person under 18, whether taken by the child, created by another person, digitally altered or wholly generated using artificial intelligence, including deepfakes and deep nudes
- AI-enabled grooming, coercion, extortion or manipulation

Every incident involving the making or sharing of nudes or semi-nudes must receive an appropriate safeguarding response, whether the image is consensual or non-consensual, self-generated, created by another person, manipulated or generated using AI.

Staff must not intentionally view, copy, print, download, forward or otherwise share a nude or semi-nude image of a child. If an image is viewed inadvertently, this must be reported immediately to the DSL. Where viewing is unavoidable, or a device may need to be secured to preserve evidence, staff must follow the Trust's child protection procedures, current UKCIS guidance and any police advice.

The DSL or a deputy will lead the response, consider the needs and safety of every child involved, make referrals to the police or local authority children's social care where appropriate, and ensure that decisions, actions and reasons are recorded. A child reporting an incident must be taken seriously, supported and never made to feel ashamed or responsible for creating a problem.

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately.

Any such incident will be dealt with according to the procedures set out in the school's child protection and safeguarding policy and child protection referral process.

12. Monitoring and transparency

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the CET Team whenever there is a significant change to either AI use by the trust or the associated risks of AI usage.

This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.

The policy will be shared with the board of trustees at least annually.

All staff, including those who do not work directly with children, are expected to read and follow this policy. Executive Headteachers, Headteachers and Heads of School are responsible for ensuring that the policy is implemented.

David Donnelly will monitor the effectiveness of AI usage across the trust.

We will ensure we keep members of the trust community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use across the schools in our trust

13. Links with other policies

This AI policy is linked to our:

- Data protection policy

- Child protection policy
- Assessment policy
- Exams policy
- Homework policy
- Behaviour policy
- Staff code of conduct
- Marking and feedback policy
- ICT acceptable use policy
- Online safety policy
- Equality policy
- Records management and retention policy
- Information security and cyber security policies
- Recruitment and selection policy