



**The Kite  
Academy  
Trust**  
Flying high  
together

## **KITE ACADEMY TRUST**

### **ARTIFICIAL INTELLIGENCE ACCEPTABLE USE POLICY (STAFF)**

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
<b>2</b>	<b>Aims of the Policy .....</b>	<b>2</b>
<b>3</b>	<b>Scope .....</b>	<b>2</b>
<b>4</b>	<b>Definitions .....</b>	<b>2</b>
<b>5</b>	<b>Principles for AI Use.....</b>	<b>3</b>
<b>6</b>	<b>Roles &amp; Responsibilities.....</b>	<b>3</b>
<b>7</b>	<b>Approval &amp; Risk-Benefit Assessment.....</b>	<b>4</b>
<b>8</b>	<b>Acceptable Uses .....</b>	<b>4</b>
<b>9</b>	<b>Prohibited or Restricted Uses.....</b>	<b>5</b>
<b>10</b>	<b>Data Protection &amp; Confidentiality.....</b>	<b>5</b>
<b>11</b>	<b>Safeguarding &amp; Pupil Use .....</b>	<b>6</b>
<b>12</b>	<b>Output Verification &amp; Quality Assurance.....</b>	<b>6</b>
<b>13</b>	<b>Intellectual Property &amp; Licensing .....</b>	<b>6</b>
<b>14</b>	<b>Training &amp; Awareness.....</b>	<b>6</b>
<b>15</b>	<b>Vendor Due Diligence &amp; Procurement.....</b>	<b>7</b>
<b>16</b>	<b>Monitoring, Auditing &amp; Reporting .....</b>	<b>7</b>
<b>17</b>	<b>Non-Compliance &amp; Disciplinary Action .....</b>	<b>7</b>
<b>18</b>	<b>Review &amp; Updates.....</b>	<b>7</b>
<b>19</b>	<b>Acknowledgement .....</b>	<b>7</b>
	<b>Document Management.....</b>	<b>7</b>
	<b>Appendix 1 - Form to request approval for new AI tool .....</b>	<b>8</b>

## 1 Introduction

The Kite Academy Trust recognises that Artificial Intelligence (AI) and machine learning can enhance teaching, learning and administration.

However, AI tools also present significant risks to data protection, safeguarding, intellectual property and the Trust's reputation.

This policy sets out the conditions under which Trust employees, Trustees, Governors, volunteers and contractors (collectively referred to as staff) may use AI systems.

It applies alongside the Trust's ICT Policy and Acceptable Use Agreement, Confidentiality Policy & Statement, Code of Conduct for Governors & Staff, Cyber Response Plan, Data Protection Policy, Disciplinary Procedure, Safeguarding & Child Protection Policy and Staff Laptop Policy.

This policy reflects requirements in UK GDPR, the Data Protection Act 2018, the Department for Education's (DfE) Generative AI in Education guidance (June 2025) and Keeping Children Safe in Education (KCSiE) 2025. Where this policy conflicts with law or regulation, the latter prevails.

## 2 Aims of the Policy

This policy aims to:

- To support safe and appropriate use of AI in teaching and administration.
- To protect personal and confidential information and ensure compliance with data-protection law.
- To safeguard pupils, staff and stakeholders from harm or discrimination arising from AI use.
- To ensure that AI does not undermine professional judgement or educational integrity.
- Embed accountability and transparency in AI across the Trust

## 3 Scope

This policy applies to all staff when using any AI system (including, but not limited to, large language models, image or audio generation tools and automated decision-making systems) for Trust purposes or on Trust equipment/networks.

It covers both licensed and publicly available tools, whether accessed on-site or remotely, and personal devices used for Trust business.

It does not cover personal use of AI unrelated to Trust business, provided no Trust data is processed, and use does not breach the Trust policies detailed in Section 1.

## 4 Definitions

### **Artificial Intelligence (AI)**

Software systems that can, for a given set of human defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.

### **Generative AI**

Models such as ChatGPT, Microsoft Co-Pilot, Google Gemini, Claude and DALL E, that create text, images or other content using data on which they were trained.

### **Personal data**

Information relating to an identified or identifiable individual (pupils, parents/carers, staff or stakeholders), including special category data (e.g. but not limited to, health, ethnicity, SEND, safeguarding information).

### **Automated Decision-Making (ADM)**

Decisions about individuals made solely by automated means without meaningful human involvement (restricted under UK GDPR Article 22).

## 5 Principles for AI Use

All AI use within the Trust will uphold the UK government's AI principles of safety and robustness, transparency, fairness, accountability, and contestability/redress, and will be:

### **Human-centred**

AI is used to augment staff; humans retain responsibility.

### **Fair and inclusive**

The use of AI will avoid bias and discriminatory outcomes.

### **Transparent**

Staff will be open about when and how AI is used and will clearly label AI-assisted outputs.

### **Accountable**

Staff will ensure AI is used with the appropriate approvals, records, audits and Data Protection Impact Assessments (DPIA).

### **Secure**

When using AI, staff will ensure that data, systems and intellectual property are protected.

## 6 Roles & Responsibilities

### **Trust Board**

The Trust Board will:

- approve this policy and oversee its implementation;
- ensure AI use aligns with the Trust's strategic objectives and legal obligations.

### **CEO/ Executive Team/ Academy Head Teachers/ Business Services Managers**

The CEO/ Executive Team/ Academy Head Teachers/ Business Services Managers are accountable for compliance with this policy and for monitoring AI use and conducting risk assessments.

### **IT Manager**

The IT Manager will:

- maintain an inventory of approved AI tools;
- perform risk benefit assessments;
- monitor usage;
- report incidents to the Executive Team/ Academy Head Teachers/ Business Services Managers and Data Protection Officer (DPO).

### **Data Protection Officer (DPO)**

The DPO will:

- advise on data protection compliance;
- conduct data protection impact assessments (DPIAs);
- respond to data subject requests;
- work with IT Manager to investigate potential breaches.

### **Line Managers**

Line Managers will:

- ensure staff are aware of and comply with this policy;
- report misuse or concerns.

## All Staff

All staff will:

- read and comply with this policy, the staff ICT Acceptable Use Agreement, Data Protection Policy and safeguarding procedures.

## 7 Approval & Risk-Benefit Assessment

### Approval required

Staff may only use AI tools that have been approved by the Executive Team and IT Manager, subject to a risk benefit assessment. Requests for new AI tools must be made in writing to the IT Manager using the form at Appendix 1, outlining the intended educational/administrative benefits, risks and risk mitigation.

### Risk benefit assessment

The Executive Team and IT Manager will consider:

- the educational or operational benefit relative to potential harms (source: [gov.uk](https://www.gov.uk));
- age appropriateness and safeguarding measures (for pupil facing tools);
- data protection implications, including whether personal data will be processed (source: [gov.uk](https://www.gov.uk));
- compliance with intellectual property laws and licensing;
- cyber security risks and compatibility with Trust systems.

### Review

Approved tools will be reviewed annually or sooner if significant changes occur.

## 8 Acceptable Uses

Approved AI tools may be used for the following, subject to the restrictions in Section 8:

### Administrative tasks

- drafting letters or reports;
- summarising non-confidential information;
- generating generic content to aid communication;
- translation to support EAL families;
- accessibility formatting (e.g. converting text to simpler language or audio).

### Teaching and learning

- lesson planning;
- curriculum resource generation;
- knowledge retrieval from public sources;
- creative inspiration.

AI outputs must be checked for accuracy, bias and suitability before use in lessons.

### Research

- obtaining general background information or alternative perspectives from non-confidential sources.

### Professional development

- exploring AI concepts or features for self-education;
- asking hypothetical questions to understand how AI might support a staff member to undertake their role more effectively.

AI must not be presented as human work without acknowledging the use of AI assistance (see 12 Intellectual Property & Licensing).

## 9 Prohibited or Restricted Uses

Staff must **not** use AI tools for any of the following unless explicitly authorised by the IT Manager and DPO:

### **Processing personal or special category data**

Staff must not input names, contact details, named assessment data, named behavioural records, named medical or named safeguarding information or any information that could identify an individual (source: [gov.uk](#)).

### **Decision making affecting individuals**

AI must not be used to make or recommend decisions relating to pupil grading, admissions, recruitment, performance management or disciplinary actions (source: [gov.uk](#)).

Human professionals must always make the final judgement.

### **Legal, HR or safeguarding advice**

AI must not be used as a source of legal counsel, HR advice or safeguarding decisions. Consult the relevant professional or DfE guidance.

### **Confidential or proprietary information**

Staff must not upload internally confidential information or any content protected by copyright or commercial sensitivity. AI providers may use such inputs to train their models, causing a breach of confidentiality and copyright (source: [gov.uk](#)).

### **Plagiarism or academic dishonesty**

Staff must not:

- use AI to generate work and present it as entirely their own without acknowledging AI assistance;
- use AI to complete assignments or assessments on behalf of pupils;
- encourage pupils to use AI to cheat.

These practices undermine academic integrity and may constitute malpractice.

### **Bias, discrimination or harmful content**

Staff must not use AI to produce or propagate material that is discriminatory, harassing, inappropriate, unsafe or damaging to any individual or group.

### **Malicious or unethical activities**

Staff must not use AI to generate deceptive communications (e.g. deepfake emails or messages), malware or code intended to exploit systems. This includes any attempt to circumvent the Trust's security controls.

### **Unapproved personal use**

Staff must not use AI on Trust systems for purely personal benefit (e.g. running a side business or generating controversial content) unless it aligns with the limited personal use permitted in the Staff Acceptable Use Agreement and does not interfere with duties.

## 10 Data Protection & Confidentiality

All staff must be mindful of, and comply with, the following:

### **Minimisation**

Staff should only use anonymised or fictional data when testing or demonstrating AI tools. If personal

data must be processed, consult the DPO and complete a DPIA.

#### No sensitive inputs

Staff must not enter sensitive information about individuals including, but not limited to, information relating to mental/physical health, ethnicity, SEND status or safeguarding concerns.

#### Transparency and consent

If AI processing could identify a data subject or impact their rights, staff must obtain explicit consent and clearly explain the purpose and outcome. This is particularly relevant for automated marking or personalised feedback.

#### Retention and deletion

AI outputs and associated data should be stored only as long as necessary and in line with the Trust's Records Retention Policy. Do not rely on AI providers to store or secure your data; download and save outputs to approved Trust storage if required.

### 11 Safeguarding & Pupil Use

Staff must not use AI tools directly in front of pupils, nor should these tools be presented as unbiased or authoritative sources of information.

The Trust will maintain effective filtering and monitoring systems which will be reviewed annually to ensure compliance with DfE guidance and standards.

Staff must report any concerns regarding pupil misuse of AI, or exposure to harmful content, via the Trust's safeguarding procedures.

### 12 Output Verification & Quality Assurance

All staff must always review and fact-check any content generated by AI to ensure it is accurate, appropriate and aligned with the curriculum and our Kite values. AI outputs should be used to support—not replace—professional judgement.

All staff must:

- Check factual accuracy and cross reference information with reliable sources. AI often ‘hallucinates’ and it may invent details or references.
- Review for bias, discrimination or inappropriate language. Do not use AI content that could be offensive or misleading.
- Edit and contextualise the output; AI generated text/images should be seen as a starting point, not the finished product.
- Acknowledge the use of AI where appropriate. When AI significantly contributes to a document or resource, include a note such as *“This resource was prepared with assistance from [AI tool].”*

### 13 Intellectual Property & Licensing

All staff must:

- Respect copyright laws and not input or output copyrighted material without permission. AI may reproduce parts of copyrighted texts, which could be unlawful if republished (source: [gov.uk](https://www.gov.uk)).
- Not use pupils' work to train AI models. The Trust will not share data with third party AI vendors without a suitable Data Protection Impact Assessment (DPIA).
- Review the terms of service of any AI tool to understand how data may be used.

### 14 Training & Awareness

Staff will receive regular training on AI use covering this policy, data protection obligations and practical examples.

Staff must complete refresher training when significant changes to AI tools or regulations occur.

Failure to participate in required training may lead to suspension of access to AI tools.

## 15 Vendor Due Diligence & Procurement

Before approving any AI tool, the Trust will be mindful of its obligations under the UK GDPR and Data Protection Act 2018 and Keeping Children Safe in Education, and will ensure that any tool that is procured aligns with DfE product safety expectations for generative AI.

## 16 Monitoring, Auditing & Reporting

Use of Trust approved AI tools may be monitored and logged for security, safeguarding and compliance reasons. By using these tools, staff consent to such monitoring (see ICT Acceptable Use Agreement).

The IT Manager will audit AI use periodically to ensure compliance and to identify emerging risks or benefits.

## 17 Non-Compliance & Disciplinary Action

Breaches of this policy may result in disciplinary action under The Kite Academy Trust Disciplinary Procedure, up to and including dismissal. Serious breaches involving personal data may also result in regulatory fines or criminal sanctions.

Misuse of AI that endangers pupils will be treated as a safeguarding matter and reported accordingly.

## 18 Review & Updates

This policy will be reviewed annually, or sooner if legislation, guidance or technological developments require changes.

Significant updates must be approved by the Trust Board after consultation with staff representatives.

## 19 Acknowledgement

All staff must acknowledge in writing that they have read and understood this policy before being granted access to AI tools.

## Document Management

<b>Document ID:</b>	P1170		
<b>Last Review:</b>	December 2025	<b>Review Period:</b>	1 year
<b>Responsibility of:</b>	Deputy CEO	<b>Ratified by:</b>	Trustees (18.12.25)

## Appendix 1 - Form to request approval for new AI tool



The Kite Academy Trust

### REQUEST FOR AI TOOL

Name:	
Academy/ Team:	
Role:	
Name of requested AI tool:	
<b>Education/ administrative benefits of requested AI tool for the Trust:</b>	
<b>Risks of requested AI tool to the Trust and how these can be mitigated:</b>	
Cost of requested AI tool per user (if applicable):	
Signed:	Date: