

# Aston Clinton School



## Artificial Intelligence (AI) Policy 2025–2026

*"AI supports learning best when it encourages pupils to think deeply, ask questions, and take pride in their own work."*

Approved by (Governing Board):	Full Committee
Date approved:	Spring 2026
Last reviewed on:	Spring 2026
Next review due by:	Spring 2027 (annual review)

## 1. Introduction:

Artificial Intelligence (AI) is increasingly used in education and, when applied responsibly, can raise aspirations and support high-quality teaching, learning, and school operations. To ensure children are cared for and protected, the use of AI must be safe, ethical, and lawful, with careful attention to safeguarding, data protection, bias, integrity, and over-reliance.

This policy is informed by the Department for Education's *Safe and Effective Use of AI in Education* guidance and leadership toolkit and supports all pupils to succeed. All staff, volunteers, and contractors must follow this policy alongside the school's safeguarding, data protection, and wider school policies.

## 2. Aims and Scope

Our school will use AI to enhance teaching and learning, reduce workload appropriately, and improve accessibility, while ensuring ethical, safe and lawful practice. This policy applies to all staff, governors, pupils, volunteers and contractors using school systems.

## 3. Legislation and Standards

This policy has due regard to the following:

- UK GDPR and Data Protection Act 2018 (including DPIAs for relevant tools).
- Keeping Children Safe in Education (KCSIE).
- DfE Generative AI in education guidance and DfE Product Safety Expectations.
- ICO guidance on use of images and personal data in schools.

## 4. Guiding Principles for AI Use

The school uses Artificial Intelligence (AI) to support high-quality education and effective school operations, while always prioritising the safety, wellbeing, and rights of pupils and staff. In line with the Department for Education's *Safe and Effective Use of AI in Education* guidance, AI is used ethically, transparently, and sustainably, with clear human oversight and accountability to help all pupils succeed.

- **Safety, security, and sustainability**  
AI tools must be safe, secure, and resilient, with appropriate safeguards to protect personal data and prevent misuse. Use of AI should be proportionate and mindful of environmental impact, including energy use and long-term sustainability.
- **Transparency and explainability**  
Staff must understand how AI tools work in practice, including their intended purpose, limitations, and potential risks. AI-generated content must be clearly identified and attributed where appropriate.
- **Fairness and inclusion**  
AI must be used in ways that avoid bias and discrimination and support equality of opportunity. Steps should be taken to identify and mitigate potential bias so that no individual or group, including those with protected characteristics, is disadvantaged.
- **Human oversight, accountability, and governance**  
AI supports, but does not replace, professional judgement. Decisions affecting pupils, staff, or families remain the responsibility of people. All AI use must follow school approval processes and governance arrangements.
- **Contestability and redress**  
AI-generated outputs must be open to review and challenge. Errors, concerns, or unintended consequences should be identified, corrected, and escalated through established school procedures.

## 5. Roles and Responsibilities

### Governing Board

- Provides strategic oversight of the school's use of Artificial Intelligence (AI) in line with the Department for Education's *Safe and Effective Use of AI in Education* guidance.

- Ensures appropriate policies are in place covering safeguarding, data protection, online safety, and acceptable use of AI.
- Holds the Headteacher to account for the safe, ethical, and lawful implementation of AI, including compliance with *Keeping Children Safe in Education* (KCSIE) and UK GDPR.
- Reviews AI-related risks as part of the school's risk management and safeguarding arrangements.

### **Headteacher**

- Has overall responsibility for the safe and effective use of AI within the school.
- Leads the school's AI approach and ensures alignment with educational priorities, safeguarding, and statutory requirements.
- Approves any proposed AI tools before a Data Protection Impact Assessment (DPIA) is undertaken and before use in school.
- Ensures staff receive appropriate training and that an AI action plan is developed, implemented, and reviewed.
- Integrates AI into the school's digital strategy and signs off local procedures.

### **Computing Lead**

- Acts as the first point of contact for staff queries about AI use.
- Supports staff in understanding appropriate and safe use of AI tools.
- Ensures only school-approved AI tools are used and escalates concerns to the Headteacher as required.

### **AI Lead**

- Provides day-to-day oversight of AI use within the school.
- Coordinates staff training and guidance.
- Maintains records of approved AI tools and their intended use.
- Monitors practice to ensure adherence to this policy and identifies safe and appropriate opportunities to enhance teaching, learning, and curriculum provision.

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

- Advises on lawful bases for processing personal data when AI tools are proposed.
- Supports and reviews Data Protection Impact Assessments (DPIAs).
- Confirms data flows, security arrangements, and data retention in line with UK GDPR.

### **Designated Safeguarding Lead (DSL)**

- Ensures safeguarding training includes AI-related risks, including deepfakes, online impersonation, sexual extortion, and misinformation.
- Leads on responding to safeguarding concerns or incidents involving AI use, in line with KCSIE and school safeguarding procedures.

### **Staff**

- Use only school-approved AI tools for professional purposes.
- Do not enter personal, confidential, or sensitive data into open or unapproved AI systems.
- Critically evaluate and verify AI-generated content before use.
- Acknowledge and attribute AI use where required.
- Report any concerns or misuse in line with safeguarding and whistleblowing procedures.

### **Pupils**

- Use AI only when permitted and under appropriate supervision.
- Do not present AI-generated work as their own.
- Follow the school's online safety and acceptable use rules.
- Acknowledge AI use when directed by staff.

## 6. Data Protection and Privacy

AI tools may process or store data, including on external or cloud-based servers. Any use of AI that involves personal data must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The school will only approve AI tools where a clear lawful basis has been identified and appropriate safeguards are in place, and staff will use only AI tools that have been approved by the school.

All staff are required to take part in regular training to ensure the safe, lawful, and effective use of AI platforms and to maintain an up-to-date understanding of data protection, safeguarding, and ethical responsibilities.

Personal data must never be entered into open AI systems. Where an approved AI tool processes personal data, a Data Protection Impact Assessment (DPIA) must be completed in advance. This assessment must confirm whether the tool is open or closed, demonstrate that closed systems with appropriate organisational controls are used, and set out clear arrangements for data security, retention, and deletion. The DPIA must also confirm that personal data is not used to train AI models or reviewed by human operators unless this is explicitly permitted, justified, and robustly risk managed.

Special category (sensitive) personal data must never be entered into any AI system. This includes, but is not limited to, identifiable pupil or staff names, assessment and attainment records, addresses, medical or health information, Special Educational Needs and Disabilities (SEND) data, ethnicity, safeguarding or child protection records, and photographs or videos that identify a child.

Any suspected misuse, loss, or unauthorised access to personal data must be treated as a potential data breach and reported immediately in line with the school's Data Protection and Incident Reporting policies.

## 7. Intellectual Property (IP) and Copyright

Intellectual property refers to original work created by a person, such as: written work, artwork, images, videos, or other creative outputs. In school, this includes pupils' work and ideas, which belong to the pupil and must be respected and protected.

- Pupil work is the intellectual property of the pupil and must not be uploaded to open or unapproved AI tools.
- Staff must not upload copyrighted third-party materials into AI systems unless the school holds the appropriate rights or permissions.
- Care must be taken when sharing AI-generated content publicly (including on school websites or social media) to avoid publishing material that may resemble or reproduce copyrighted works.
- School policies, official documents, or published materials must not be issued where they have been largely generated by AI without appropriate professional review and legal verification.

## 8. Use of AI by Staff

Permitted uses include: lesson ideas, differentiation, drafting resources, summarising notes, generating admin drafts—subject to verification and attribution.

Prohibited: entering any personal/sensitive data into open tools, feeding identifiable pupil work into tools that train on inputs, relying on AI for decisions/assessment without human oversight.

## 9. Use of AI by Pupils

- Supervised use only for research/creative exploration and curriculum-linked tasks.
- Not permitted for assessments or to generate work to pass off as own.
- No creation of inappropriate/offensive content (including deepfakes).
- All use must be transparent, referenced where directed and age-appropriate.

## 10. Safeguarding and Online Safety

In line with *Keeping Children Safe in Education (KCSIE) 2025*, the school recognises that emerging technologies, including Artificial Intelligence (AI), can introduce new safeguarding risks and forms of harm.

- Staff must remain vigilant to AI-enabled safeguarding risks, including deepfakes, online impersonation, sexual extortion, bias, misinformation, and grooming. These risks are treated in the same way as other forms of online harm and child-on-child abuse referenced within KCSIE.
- Any concerning behaviour, content, or misuse of AI that may place a child at risk must be reported immediately through the school's safeguarding procedures.
- Senior leaders will ensure safeguarding arrangements remain effective by engaging in appropriate AI-related safeguarding training.

## 11. Curriculum and Assessment Integrity

The school delivers a curriculum that develops pupils' age-appropriate understanding of Artificial Intelligence (AI), including how to question sources, evaluate information critically, and use technology safely and responsibly. Through Computing and PSHE, pupils build digital literacy, critical thinking, and online safety skills as part of their wider personal development. Learning and assessment tasks are designed to promote authentic pupil work through in-class activities, discussion, practical application, and reflection.

## 12. Monitoring and Review

- This policy is reviewed at least annually or sooner if risks, tools or guidance change.
- The AI Lead and Headteacher monitor usage and report to governors

## 13. Linked Documents

- Safeguarding and Child Protection Policy
- Online Safety and Acceptable Use Policies
- Data Protection Policy and DPIA templates
- Staff Code of Conduct
- Behaviour Policy
- Equality Policy
- PSHE Policy