Hartsfield JMI School

Artificial Intelligence (AI) Policy	
Approval Date: May 2026	Review Date: May 2027
Name:	Written by: School, based on the Interm IT model policy Laura Gregory/ Philippa Smith
To be approved by Governing body Name:	 Bob Hopcraft

Policy for the Safe, Secure, and Ethical Use of Artificial Intelligence (AI) in Schools

(Aligned to the DfE Cyber Security Standards and Cyber Security Hub Guidance; based on the policy written by Interm IT)

1. Introduction

This policy defines how Artificial Intelligence (AI) tools are used safely, securely, and ethically within the school, in line with the Department for Education (DfE) Cyber Security Standards and DfE guidance on generative AI and data protection.

AI tools, including Microsoft Copilot, may be used to enhance teaching and learning, support administrative efficiency, and aid professional development. All AI use must comply with UK GDPR, the Data Protection Act 2018, and the school's safeguarding and cyber security arrangements, and online safety policy.

The school adopts a "secure-by-design" approach, favouring AI tools integrated within secure, managed environments such as Microsoft 365 Copilot, which supports enterprise security, identity management, and compliance controls.

2. Scope

This policy applies to:

- All staff (teaching, support, administration, leadership)
- All pupils
- Governors
- Peripatetic teachers/coaches, supply teachers, student teachers
- Visitors
- Volunteers
- Voluntary, statutory or community organisations using the school's facilities
- Any authorised third-party users accessing AI tools on behalf of the school

It covers all AI tools accessed via:

- School-managed devices
- School-managed user accounts
- School-related activities (on-site or remote)

3. Governance and Accountability

3.1 Leadership Responsibility

The Governing Body and Senior Leadership Team (SLT) retain overall accountability for AI use and cyber security, including implementation, monitoring and reviewing of this policy, as required under the DfE Cyber Security Standards.

3.2 AI Safety and Cyber Security Oversight

The school will appoint an AI Lead (Laura Gregory) who will:

- Oversee compliance with this policy
- Ensure AI use aligns with cyber security, safeguarding, and data protection policies
- Act as a point of escalation for AI-related incidents or concerns
- Work with IT support to ensure technical controls are applied

The AI Lead will work alongside Hartsfield's DPO and DSL who will:

- advise on data protection obligations and concerns
- the safe use of AI
- monitor and respond to safeguarding concerns related to the use of AI

The AI Lead will also work with Hartsfield's Network Manager (Interm IT) who will advise on the technical implementation of the school's AI practices, procedures and cyber security.

All staff are expected to read, understand and adhere to this policy, use AI responsibility, and report any concerns.

4. Cyber Risk Management

- AI tools are included within the school's annual cyber risk assessment, which is reviewed at least termly by Interm IT. The school also uses Risk Protection Agency (RPA), the DfE's cyber security insurance.
- Risks considered include:
    - Data protection breaches
    - Account compromise
    - Inappropriate content generation
    - Inaccurate or biased outputs

- Only AI tools that meet the school's security and data protection requirements may be approved for use.

5. Approved AI Tools and Secure Access

5.1 Preferred AI Platform

The school's preferred AI tools are:

- Microsoft Copilot (Education / Microsoft 365 Copilot)
- TwinklAI

This is due to:

- Integration with school-managed (Microsoft 365/Google accounts)
- Identity and access management controls
- Compliance with UK GDPR and DfE data protection expectations.

5.2 Access Control

- AI tools must only be accessed using school-managed accounts
- Shared, personal, or anonymous accounts must not be used
- Access permissions are granted on a least-privilege basis, in line with DfE standards.

6. Data Protection and Privacy

The school is committed to protecting personal data in compliance with the UK General Data Protection Regulation and the Data Protection Act 2018. Hartsfield will handle personal data, including data processed by AI systems, lawfully, fairly and transparently, safeguarding the privacy and rights of individuals. Further information about the gathering and sharing of information can be found in the school's Data Protection Policy.

In line with DfE guidance on generative AI and data protection:

- Personal data must never be entered into AI tools.
- This includes names, contact details, photos, safeguarding information, behaviour records, and any data that could identify an individual.
- AI prompts must be fully anonymised and generic.

Examples of acceptable language:

- "A Year 5 pupil"
- "A member of staff"
- "A primary school setting"

Avoid:

- Unique scenarios
- Specific incidents
- Small contextual details that could indirectly identify individuals or the school

7. Filtering, Monitoring, and Safeguarding

Hartsfield is committed to the safeguarding of all pupils and will ensure that AI tools are used in a way that protects children from harm. This includes monitoring and reporting concerns, and adherence to the 'Keeping Children Safe in Education' (KCSIE) guidance. The school will follow the latest KCSIE guidance to ensure that all AI tools used within the school environment are safe and do not pose risk to children.

To implement this, the school will ensure that:

- AI access is subject to the school's filtering and monitoring systems, in line with DfE requirements, through the use of SENSO and Netsweeper.

The school will:

- Assign named roles responsible for filtering and monitoring (IntermIT, governor for Cyber Security and Computing and the head teacher)
- Review AI-related filtering and monitoring at least annually (IntermIT and the AI Lead)
- Ensure harmful or inappropriate content is blocked without unnecessarily limiting learning

Pupil AI use must always be age-appropriate, supervised, and controlled.

8. Guidelines for Staff

8.1 Safe Use Expectations

Staff must:

- Use AI tools only for legitimate educational or operational purposes
- Avoid entering confidential or sensitive information
- Review all AI generated content before implementing it, to ensure that it is accurate, safe and free from bias
- Apply professional judgement at all times

AI outputs:

- Do not replace teacher expertise
- Must be checked for accuracy, bias, safeguarding, and appropriateness
- Must be reviewed for UK spelling, terminology, and curriculum alignment

8.2 Training and Awareness

Staff will receive training on:

- Safe AI use
- Cyber security awareness
- Data protection and safeguarding responsibilities

Staff must report any AI-related concerns, errors, or risks immediately to the AI Lead and, if appropriate, the DPO or DSL.

9. Guidelines for Pupils

9.1 Supervised Use

Pupils may only use AI tools:

- With staff permission
- Under appropriate supervision
- For clearly defined learning activities

Pupils must not enter:

- Names
- Home addresses
- Personal experiences
- Information about others

9.2 Digital Literacy

The school will teach pupils to:

- Understand what AI is and how it works
- Recognise its limitations and potential inaccuracies, including developing an understanding of how AI systems can inadvertently perpetuate bias and false information
- Identify age restrictions for AI tools to protect younger users
- Report inappropriate or concerning outputs immediately

This supports the DfE's emphasis on developing safe digital behaviours.

10. Incident Management

- AI-related incidents (e.g. data exposure, inappropriate content, account compromise) are treated as cyber security incidents.
- Incidents will be managed in line with the school's Cyber Incident Response Plan, Safeguarding and Data Protection policies, including:
    - Immediate containment
    - Reporting to relevant leads
    - Notification to the DPO where required
    - Recording and documenting of incidents
- Serious incidents will be escalated in line with DfE and ICO guidance. [gov.uk]

11. Monitoring and Review

- This policy is reviewed annually, or sooner if:
    - DfE guidance changes
    - New AI tools are introduced
    - A significant incident occurs
- Staff, pupil, and parent feedback is considered as part of continuous improvement.

12. Conclusion

This policy ensures AI is used in a way that is secure, lawful, and educationally beneficial, fully aligned with the DfE Cyber Security Hub standards and safeguarding expectations. By prioritising secure platforms such as Microsoft Copilot, the school supports innovation while maintaining robust cyber resilience and protecting its community.

Appendix 1: Glossary / Definitions of AI terms

- **Artificial Intelligence (AI)** : refers to the use of computer systems and algorithms to perform tasks that typically require human intelligence.
- **Generative AI** : AI tools that generate new outputs based on the data they have been trained on, such as text, images, or code.
- **Machine Learning (ML)** : ML algorithms allow systems to learn from data and improve their performance over time. For example, ML may be used in personalised learning platforms that adapt content based on pupil progress, or systems where personalised recommendations are made, based on a user's prior activity on that platform.
- **Personal Data** : Information collected that relates to an identified or identifiable living person. This may include but is not limited to name, date of birth, location data, online identifiers, photographs and address
- **Ethical Use** : Using AI and data in a way that respects individual s' rights, promotes fairness, prevents discrimination and considers environmental impact.