



Artificial Intelligence (AI) Policy

Last Reviewed Date:	New	Review Date:	19/02/2026
----------------------------	-----	---------------------	------------

Headteacher		Date:	05/03/2026
Chair of Governors		Date:	16/03/2026

Date of Next Review:	November 2026
-----------------------------	---------------

This policy has been writing by adopting and adapting the HfL model policy template (October 2025).

**C O N T E N T S**

1	Introduction
2	Purpose of this policy
3	Related Policies
4	Scope
5	Glossary / Definitions of AI terms
6	Roles and Responsibilities
7	Data Protection
8	Safeguarding
9	Ethical use
10	List of approved tools, with example uses (if applicable).
11	Staff Training
12	Reporting concerns / Incident management
13	Monitoring and review



1. Introduction

Amwell View School recognises that the use of AI can bring many benefits to education, but that there are also challenges, which need to be addressed and risks mitigated.

Benefits include rapidly producing materials, adapting learning content to meet the needs of individual pupils and giving staff more time to focus on teaching and pupil interaction.

Challenges include those surrounding data protection, bias, use of intellectual property and misuse of the technology.

1.1 Definitions

This policy is aimed at staff and students will not have direct AI access:

- **Default:** Generative AI tools are for staff productivity (drafting/admin/planning) and must not be used directly by pupils.
- **Exception route:** Any pupil-facing or therapy/learning use (even via assistive tech) requires Headteacher approval + DPIA + DSL safeguarding risk assessment and must be on the approved tools register.

2. Purpose of this policy

The aims of this policy are to:

- Ensure that AI technologies are used ethically and responsibly by all members of the school community
- Provide clear guidelines for staff on the safe and effective use of AI.
- Promote the safe and ethical use of AI to benefit teaching, learning, leadership, management and administrative processes.
- Address potential challenges related to data privacy, bias, and security that the use of AI may raise.
- Encourage a culture of continuous learning and adaptation to new AI technologies among staff, as this rapidly evolving technology develops.

The school is committed to fostering an environment where staff are encouraged to continuously learn and adapt to new AI technologies. By doing so, we aim to ensure that our staff are able to use AI tools effectively and responsibly, ultimately enhancing the educational experience for our pupils.

3. Related Policies

Related policies include, but are not limited to:

- **Data Protection Policy** – details procedures for consent, conducting Data Protection Impact Assessment (DPIAs), and implementing data security measures.



- **Safeguarding Policy** – outlines monitoring and reporting mechanisms, risk assessments, and staff training on safe use of AI tools in line with the 'Keeping Children Safe in Education' guidance.
- **Online Safety Policy** – to ensure that AI tools are integrated into the school's broader online safety strategy, including filtering and monitoring systems.
- **Codes of conduct** – to ensure that staff use AI responsibly, respect intellectual property rights, and adhere to guidelines for human oversight and transparency.

4. Scope

This policy applies to, but not limited to:

- **Leadership, Teaching and Support Staff:** This includes teachers, teaching assistants, management, technical, site and administrative staff.
- **School Governors:** This policy extends to school governors who play a crucial role in decision-making and oversight.
- **Peripatetic Teachers, Supply Teachers, Student Teachers, Outsourced Coaches, Contractors:** Individuals who work temporarily within the school.
- **Volunteers:** Volunteers who contribute their time and expertise to the school community are expected to follow the principles set forth in this policy.

5. 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 the 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, data of birth, location data, online identifiers, photographs and address.
- **Ethical Use:** Using AI and data in a way that respects individuals' rights, promotes fairness, and prevents discrimination.

6. Roles and Responsibilities

- **Headteacher and Governing Body:** Responsible for the overall implementation, monitoring and review of this policy.
- **AI Lead:** Janet Warrington acts as the lead for AI, monitors compliance, and organises/provides training, annually and or as required.
- **Data Protection Officer (DPO):** Janet Warrington advises on data protection obligations and responds to data protection concerns related to the use of AI.



- **Designated Safeguarding Lead (DSL):** Neil Ward advises on the safe use of AI tools and responds to safeguarding concerns related to the use of AI.
- **Network Manager and technical support staff:** Beebug (ICT Specialists for Primary Schools) is responsible for the technical implementation of the school's AI practices, procedures and cyber security.
- **All Staff:** Expected to read, understand, and adhere to this policy, use AI responsibly, and report any concerns.

7. Data Protection

- The school ensures that all personal data collected from pupils, staff and parents, including data processed by AI tools, is handled in accordance with the UK GDPR principles.
- Our Data Protection Policy can be found on the school website: [Statutory School Policies](#)
- Where required, consent will be sought for the processing of personal data by AI tools, and the school will be transparent about how and why AI is being used for the processing of personal data.
- The school's data security measures include the following:
 - The school uses Microsoft Exchange Online Protection (EOP) as part of Microsoft 365. This filters inbound and outbound emails for spam, phishing, and malware.
 - The school uses SCCM (System Center Configuration Manager) to manage Windows updates and application patches across all managed devices. Sophos Antivirus is installed on all endpoints, providing real-time protection and automatic virus definition updates.
 - Administrative accounts are restricted to IT staff only and are separate from personal user accounts, reducing the risk of compromise through phishing or malware.
 - Access rights are assigned according to the principle of least privilege; ensuring staff have only the access they need for their role.
 - Daily backups to two devices, and a daily offsite cloud backup of key systems and data are performed. Copies are securely stored offsite to support recovery in the event of data loss or ransomware.
- Data Protection Impact Assessments (DPIAs) are carried out on AI tools that process personal data.
- Data Protection and GDPR Awareness Training is provided to all staff as part of their induction training and annual refresher training to ensure staff are fully informed about the latest data protection regulations and practices, including the use of AI. This include how to handle data breaches and the importance of maintaining data accuracy.
- Data Breaches are reported to the Data Protection Officer using the form which can be found on the school shared drive: [Staff:\Admin\Blank Proformas\Data Breach](#)

8. Safeguarding

- 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 any risk to children this includes regular updates and reviews of AI-related practices to align with KCSiE.



- The school will ensure that the appropriate filtering and monitoring systems are in place to protect pupils online, following the DfE's **filtering and monitoring standards**. The school has web filtering and firewall controls in place to prevent access to inappropriate or malicious sites.

9. Ethical Use

- The school addresses bias and ensures fairness by taking proactive steps to identify and mitigate these biases to ensure fairness and non-discrimination,
- The school maintains human oversight to ensure AI-generated content and decisions are accurate. This involves ensuring that all AI-generated content is reviewed by a staff member before use and establishing clear guidelines that the responsibility for AI output lies with the user, not the AI system.
 - Example: All AI-generated content, such as lesson plans, is reviewed by a member of staff before being implemented. This ensures that the content is accurate and appropriate for the classroom setting.
- No identifiable information about pupils, parents, or staff may be entered into any AI tool) including text, images, audio, video), including SEND health, safeguarding, therapy notes, EHCP content, or anything that could identify an individual indirectly. If AI is used to draft documents, staff must use templates and placeholders (e.g. "<PUPIL NAME>") and complete personal details only inside approved school systems (MIS/CPOMS/email).
- Pupil work will never be uploaded to an AI tool.
- The school limits the use of AI tools to strictly necessary activities.
- Embedded AI features must be reviewed before being enabled where they process pupil data.
- The school is committed to transparency in its use of AI technologies. We will clearly communicate the purposes and benefits of AI tools to all stakeholders, including parents and staff. This includes providing detailed information on how AI tools are used to enhance teaching, learning and administrative processes, as well as the measures in place to ensure their ethical responsible use.

10. List of approved tools, with examples uses (if applicable).

Approved Tools	Approved Uses	Not allowed (unless formally approved):
Co-Pilot, Chat GPT	- Drafting lesson ideas / resources at a generic level - Creating visual timetables from generic symbols (not pupil photos) - Drafting letters with placeholders - Simplifying text without referencing a specific pupil - Generating meeting agenda templates, risk assessment templates (non-personal)	- Writing anything that includes pupil identifiers - Uploading notes from EHCP/medical plans/behaviour plans - Using AI to make decisions about provision, risk or safeguarding - uploading any pupil images/audio/video.
Arbor AI	- Producing emails - Writing letters - Generating reports	



11. Staff Training

- Staff receive induction training, and follow-up annual training on the safe use of AI tools, including how to identify and report AI-generated deepfakes. This training is part of the school's broader Data Protection / GDPR and Cyber Security training programme, ensuring that all staff are equipped to handle AI-related risks.
- The school will maintain an approved AI tools register and a DPIA log for any tool or feature that processes personal data.

12. Reporting Concerns / Incident Management

- Any incidents that occur due to the use of AI tools are reported to either Beebug, the DPO or DSL depending on what needs to be investigated. The report should detail the following:
 - What you received (e.g. a video, audio message, email, chat message)
 - Why it seemed suspicious to you (e.g. unusual tone, mismatched voice, odd visuals, unexpected request).
 - Any evidence you can safely capture (e.g. screenshot, timestamp, send details without forwarding the content)
- **Cyber Security** concerns should be report to Beebug ICT Support – avsitssupport@amwell.herts.sch.uk alongside informing the Headteacher and the DPO. Please refer to the [Cyber Security school policy](#).
- **Data Protection** concerns should be report to the DPO – Janet Warrington dpo@amwell.herts.sch.uk. Please refer to the [Data Protection school policy](#).
- **Safeguarding** concerns should be report to the DSL – Neil Ward (Headteacher) or Deputy DSLs – Jane Connolly (Deputy Headteacher) or Ellen-May Shipp (Senior Leader) and recorded on CPOMS. Please refer to the [Child Protection and Safeguarding school policies](#).
- These concerns will be reviewed by the Headteacher and Governing Body.

13. Monitoring and Review

- This AI Policy will be reviewed at least annually, more frequent reviews may happen as AI is rapidly evolving. Other triggers for updates may include new guidance or regulations from the DfE, major changes to the AI technology that will impact education and/or feedback from stakeholders.
- Staff will be emailed to communicate when the policy has been changed. The policy will can be found on the school website: [Additional School Policies](#)