John Hunt Academy

Artificial Intelligence (AI) Policy

Approved by:	Mrs A Good & Miss L Devlin	Date: 05/03/2026
Last reviewed on:	New Policy Created 05/03/2026	
Next review due by:	31/07/2026	

ARTIFICIAL INTELLIGENCE (AI) POLICY V3 (2026)

INFORMATION

Version: 3.1
Date created: 28/01/2026
Date updated: 05/03/2026
Next review date: 31/07/2026

Applies to: All staff, governors, volunteers, contractors, student teachers, and approved partners using AI tools for school purposes.

This AI Policy complements and is referenced by our Online Safety Policy, Data Protection Policy, Technical Security Policy, Staff Acceptable Use Agreement (AUA), Mobile Technologies Policy, and Social Media Policy.

1. PURPOSE AND PRINCIPLES

We aim to **responsibly harness AI** to reduce workload, improve efficiency, enhance teaching resources, and strengthen school operations—**never replacing professional judgment**. All use of AI:

- **Supports staff** by reducing workload where possible but **remaining under human oversight**.
- **Complies with UK law and DfE guidance** (including data protection, Safeguarding policies, KCSIE and everyone's intellectual property)
- **Prioritises safeguarding** and equitable outcomes; we actively mitigate **inaccuracy ("hallucinations")**, **bias**, and **harmful content**.
- Is integrated within our existing online safety framework and the **SWGfL policy architecture** (from which our Online Safety policy is formed).

2. SCOPE

This policy governs the use of **generative AI** and other AI enabled services used for curriculum, assessment, communication, administration, and operations. It covers:

- **School approved AI tools** (including M365 Copilot, approved LLM powered apps) on school devices/accounts.
- Any **third party AI** accessed for school purposes, whether on school or personal devices (subject to AUA and filtering/monitoring controls).

3. DEFINITIONS

- **Artificial Intelligence (AI):** Systems that infer how to generate outputs (text, images, predictions) that influence digital/real environments.
- **Generative AI:** AI that creates content (e.g., text, images).
- **Large Language Model (LLM):** A type of generative AI trained on large text datasets to produce language outputs.
- **Hallucination:** Plausible but **incorrect** output generated by AI.
- **DPIA:** Data Protection Impact Assessment; assesses high risk processing and mitigations.

4. ROLES AND RESPONSIBILITIES

- **Headteacher & SLT:** Ensure safe culture, resourcing, and training; approve AI tools; oversee filtering/monitoring reviews with the DSL and IT provider.
- **Governing Body (Online Safety Governor):** Receive annual AI/online safety reports; verify filtering and monitoring and cyber-security checks are completed and effective.
- **Designated Safeguarding Lead (DSL):** Lead safeguarding for AI use; review alerts; handle incidents; ensure AI risks are included in online safety education.
- **Online Safety Lead (OSL):** Coordinate AI education, guidance, and training; maintain AI inventory and risk assessments.
- **IT Service Provider/Technicians:** Maintain filtering/monitoring aligned to **DfE standards**; provide logs and system checks; assist with procurement and configuration of AI tools.
- **All staff:** Use only **approved AI** for school work; apply professional judgment; uphold AUA; report incidents promptly.

5. ETHICAL USE PRINCIPLES

We commit to AI that is:

- **Safe & lawful** (safeguarding, GDPR, lawful basis, minimal data).
- **Fair & inclusive** (assess bias; protect vulnerable groups; avoid disproportionate harms).
- **Transparent & explainable** (be open about AI assistance where appropriate).
- **Accountable & contestable** (humans can overrule/correct outputs; complaints handled via normal routes).
- **Human-centred** (AI supports, never replaces teacher judgment).
- **Proportionate & sustainable** (use AI only where it adds value, mindful of environmental costs).

6. APPROVED USES AND STAFF BENEFITS

Permitted uses (examples):

1. **Planning & resource creation**: Drafting lesson plans, worksheets, success criteria, model texts and differentiated materials—**always reviewed and adapted by the teacher**.
2. **Feedback support**: Generating formative comments or next steps (including EAL/SEND scaffolding), with teacher oversight and factual checks (anonymising data before uploading)
3. **Admin efficiency**: Summarising meetings, drafting emails/newsletters, creating policy templates, scheduling ideas, and extracting action lists.
4. **Data free ideation**: Brainstorming display themes, assemblies, clubs, or enrichment activities **without entering personal/sensitive data**.
5. **Operations**: Drafting risk assessment templates, stocktake checklists, and process maps, subject to SLT signoff.
6. **Note-taking:**
    1. DPIA must be in place
    2. All participants should be informed if a meeting is being recorded

Staff Benefits: Reduced administrative load; however, **human accountability for accuracy and appropriateness is always maintained.**

Not permitted:

1. Uploading personal data without DPIA and/or SLA
2. Relying on AI for Safeguarding or legal advice
3. Using AI to make any decisions with legal or similarly significant effects on individuals

7. USE OF AI BY PUPILS

- Pupils do not create personal accounts on external generative AI services for school tasks. Any exposure to using AI for school tasks **must** take place on school-approved platforms, under teacher supervisions, with filtering and monitoring applied.
- Teaching focuses on **critical thinking** (fact checking, identifying misinformation/deepfakes, respectful use, ethical use).
- A culture of responsible AI use will be fostered through an age-appropriate curriculum which will commence in September 2026.
- Pupils will be encouraged to protect their personal data.
- AI literacy skills will be taught where appropriate.

8. SAFEGUARDING AND RISK CONTROLS

8.1 DATA PROTECTION AND PRIVACY

- **No personal data** (pupil, family, staff) or special category data may be entered into external AI tools **unless** the tool is **formally vetted**, a **DPIA** is in place, and processing is lawful under UK GDPR.
- Use **school accounts** and **school configured AI services** only; **multifactor authentication** on sensitive systems; encryption at rest/in transit.
- Respect **copyright and IP** (including pupils' work); do not upload proprietary content for model training without explicit consent/contract terms.

8.2 AVOIDING INACCURATE OR BIASED OUTPUTS

- **Human in the loop:** Staff must **factcheck**, **source check**, and **bias check** all AI outputs; teachers make final judgments as with any other material shared with children.
- **Transparency:** Clearly indicate when AI assisted a document/resource so colleagues understand where **human validation** has occurred.
- **Equity:** Review prompts/outputs for stereotypes or unfair treatment; escalate concerns to DSL/OSL for remedial actions and supplier engagement.

8.3 FILTERING, MONITORING, AND CONTENT SAFETY

- Our internet access and devices are protected by **appropriate filtering and monitoring** reviewed **at least annually** by SLT, DSL, governor, and IT provider, per **DfE standards**.
- Filtering includes illegal content blocklists (e.g., IWF/CTIRU), and monitoring provides timely safeguarding alerts—balanced to avoid unreasonable over blocking that could impede teaching and learning.
- Any AI enabled browsing or chat tools are subject to the same filtering/monitoring regime across **school devices**, onsite and offsite.

8.4 Cyber Security

- We meet (and work towards) the **DfE Cyber Security Standards**: secure access controls, patching, backups (including air gapped/cloud copies), endpoint protection, incident logging and response.
- Staff complete annual cyber awareness training; governors consider **NCSC "questions for governing bodies"** to assure cyber resilience.

9. ACCEPTABLE USE RULES (STAFF)

Staff must:

1. Use **only school approved AI tools** for school tasks; never use unapproved consumer AI for processing school information.
2. **Exclude personal/sensitive data** from prompts unless a vetted, private service and lawful basis exist (see DPIA).
3. **Fact check** and **reference** sources; do not rely on AI for accurate statistics, safeguarding advice, or legal interpretation.
4. Label AI assisted outputs where appropriate; retain accountability for accuracy, tone, and suitability for primary pupils/families.
5. Respect copyright/IP (including pupils' work); do not generate or share content that infringes others' rights.
6. Follow reporting routes for **AI incidents** (data exposure, harmful or biased outputs, technical compromise) immediately.

These rules are mirrored in our **Staff AUA (2026)** and reinforced at induction and annual training.

10. EDUCATION, TRAINING, AND SUPPORT

- **Staff training**: Annual modules on understanding AI, safe interaction, and use cases, using DfE **"Using AI in education settings: support materials"** (Chartered College of Teaching) and school guidance.
- **Pupil education**: Build critical thinking (fact-checking, source credibility, respectful use) into Computing/PSHE from Autumn 2026 with a clearly defined curriculum, integrated with Safety and Online Safety curricula.
- **Family engagement**: Share how we are using AI with parents and seek their input into further developing policy and curriculum.

11. INCIDENT REPORTING AND RESPONSE (AI RELATED)

- **Immediate reporting** to DSL/OSL for:
  - Suspected data breach or inappropriate disclosure via prompts/outputs.
  - Harmful, discriminatory, or factually incorrect outputs used or shared.
  - Technical compromise or suspicious AI activity.
- Follow school safeguarding and cyber incident procedures: secure evidence, contain exposure, notify affected parties where required, and report notifiable **data breaches to the ICO within 72 hours**.
- Log incidents and lessons learned; update training, prompts guidance, and procurement checks accordingly.

12. MISUSE, ACADEMIC INTEGRITY AND UNACCEPTABLE USE

- Examples include: plagiarism; impersonation; using AI content as fact without checking; using AI to fabricate evidence; uploading personal data without consent and DPIA; generating harmful/discriminatory content; peer-on-peer abuse; cyber-bullying.
- Consequences align with school behaviour and Online Safety Policy.

13. REVIEW, ASSURANCE, AND GOVERNANCE

- **Annual governance report**: DSL/OSL submit an anonymised AI & Online Safety report (incidents, training completion, tool inventory, DPIAs, filtering/monitoring checks, cyber resilience).
- **Standards alignment**: Record compliance and gaps against **DfE Filtering & Monitoring** and **Cyber Security standards**; agree improvement plan.
- **Policy updates**: Revise this policy when DfE guidance changes (e.g., updates to Generative AI guidance and inspection expectations).

14. LOCAL SCHOOL CONSIDERATIONS

AI TOOLS INVENTORY

Tool Name	Purpose	Approved Use Cases	Data Handling Notes	Risk Level	Review date
Microsoft 365 Copilot	Integrated productivity AI	Lesson planning, document drafting, summarising	Uses school M365 tenant; GDPR compliant		31/07/25
Otter	Transcription and meeting notes	Staff meeting summaries, CPD notes	Avoid sensitive data; check storage settings		31/07/25
Canva	Design and creative content	Posters, newsletters, teaching visuals	Avoid uploading sensitive images or pupil data		31/07/25
Arbor	MIS with AI features	Data insights, reporting	Handles pupil data; ensure DPIA and secure login		31/07/25

Approval (for any new AI tool):

- Staff member proposes tool and its use to SLT
- SLT complete screening
- DPIA if necessary
- SLT approval
- Inventory updated
- Training provided for staff
- Review date set

LOCAL CONTEXT

- **Equity & inclusion**: Use AI to scaffold for **EAL**, **SEND**, and pupils affected by **digital poverty**, ensuring outputs are accessible, culturally sensitive, and bias checked.
- **Community trust**: Be transparent with families about AI use; avoid uploading community identifying data; emphasise human oversight and compliance with national standards.
- **Environmental constraints**: Where home connectivity is limited, ensure classroom use of AI is supervised, filtered, and pedagogically justified; do not require pupils to use external AI accounts.

15. LINKED POLICIES AND DOCUMENTS

- Online Safety Policy
- Staff/Volunteer AUA (inc. AI clauses from September 2026)
- Learner AUA (KS1/KS2, age appropriate)
- Data Protection Policy & Privacy Notices
- Technical Security Policy (inc. passwords, patching, backups)
- Mobile Technologies & Social Media Policies
- AI Tools Inventory & DPIA Register
- Filtering & Monitoring Review Log; Cyber Incident Response Plan

STAFF ACCEPTABLE USE AGREEMENT (AUA)

AI ADDENDUM

This addendum applies to all staff using AI tools for school purposes. By signing, staff agree to:

- Use only school-approved AI tools: Microsoft 365 Copilot, Otter, Canva and Arbor.
- Never input personal or sensitive data unless the tool is vetted and a DPIA is in place.
- Fact-check and bias-check all AI outputs; maintain human oversight.
- Label AI-assisted content where appropriate for transparency.
- Respect copyright and intellectual property, including pupils' work.
- Report any AI-related incidents (data breaches, harmful outputs) immediately to the DSL/OSL.
- Follow all safeguarding and data protection policies when using AI tools.

AI RISK ASSESSMENT

Risk	Description of risk	Likelihood	Impact	Actions to take	Person responsible
Data privacy	Exposure of personal information, sensitive data or intellectual property				
Bias	Reinforcing of stereotypes or discrimination				
Inaccurate content	Hallucinations, misinformation or disinformation				
Cyber vulnerability	Security risks to school network and/or systems				
Misuse by staff	Breach of Staff AUA				
Deepfakes	Impersonation, reputational damage				

STAFF CHECKLIST

DO	Do NOT
Use Co-Pilot only inside M365 school accounts	Paste pupil information into public or non-approved AI tools
Use anonymised or non-personal data only	Upload licenced worksheets without checking copyright
Review and edit all AI outputs	Allow AI to make final judgements on pupils or data
Store files in M365 OneDrive or SharePoint	Save any school information into personal cloud storage

Questions to ask before running a task through AI:

- Does this task involve personal data?
- Is the data anonymised?
- Am I using a secure school-managed device?
- Will I check output for accuracy and bias?
- Am I saving the document in OneDrive/SharePoint?

REFERENCES

- **SWGfL Online Safety Policy Template (Jan 2025)** — structure & clauses for AI, filtering/monitoring, cyber security, AUAs. Link
- **DfE: Generative Artificial Intelligence (AI) in Education** — policy paper (updated Aug 12, 2025). [gov.uk]
- **DfE: Filtering and Monitoring Standards** — digital standards for schools (updated Nov 17, 2025). [gov.uk]
- **DfE: Cyber Security Standards for Schools and Colleges** — core standard guidance. [gov.uk]
- **DfE Collection: Using AI in education settings — support materials** (CLT/CCT modules). [gov.uk]
- **UKCIS: Education for a Connected World** — curriculum framework strands. [gov.uk]