Naima JPS

Artificial Intelligence (AI) Policy

Last review:	September 2026
Next review:	September 2027
Signed off by (governing body):	Julian Levy
Signed off by (Senior Management Team):	Bill Pratt

NAIMA
Jewish Preparatory School

ARTIFICIAL INTELLIGENCE (AI) POLICY

This Policy is intended for the entire school including EYFS

Policy Statement

Naima JPS recognises that Artificial Intelligence (AI), including Generative AI, presents significant educational opportunities to enhance learning and reduce administrative workloads. However, in strict compliance with the statutory requirements of Keeping Children Safe in Education (KCSIE) 2026, the school maintains that AI usage must be rigidly managed under a "Safeguarding-First" lens to eliminate risks relating to child welfare, data protection, and academic integrity. This policy establishes the explicit operational regulations required to maintain a secure, compliant, and focused digital environment.

Purpose of this Policy

The purpose of this policy is to:

- Ensure all pupil, staff, and parent interaction with AI tools strictly adheres to KCSIE 2026 safeguarding standards, DfE guidelines, and statutory data protection laws.
- Clearly define the explicit boundaries between authorised educational AI applications and prohibited platform uses.
- Protect the Naima JPS community from AI-specific online safety hazards, including the making or sharing of nude or semi-nude images, AI-assisted grooming, and algorithmic bias.
- Establish clear technical controls, data privacy rules, and monitoring protocols for AI systems utilised across the school network.

Scope of this Policy

This policy applies to all members of the school community who interact with, deploy, or manage Artificial Intelligence technologies associated with Naima JPS.

- It applies to anyone who uses or interacts with the school's technology and digital ecosystem, including the Senior Management Team, teaching staff, learning assistants, supply teachers, governors, parents, pupils (across EYFS, Key Stage 1, and Key Stage 2), external contractors, temporary personnel, and visitors.
- It covers the professional, educational, and administrative use of all artificial intelligence systems, tools, and platforms, including mandated enterprise systems (Microsoft Copilot and Google Gemini) and all unapproved, open-consumer variants (such as ChatGPT or Claude).
- It covers embedded AI software, automated text editors, AI-driven data analytics, translation software, algorithmic design features, and predictive plugins embedded within existing school applications.
- It applies to any interaction with AI systems via school-loaned devices (such as iPads or laptops) or via personal devices connected directly to the monitored school network.

- It operates across all environments, governing both on-site school usage during operational hours and remote or home-based usage when executing school business, completing homework, or processing school-related documentation.

Safeguarding and Online Safety

In accordance with statutory guidance, Naima JPS treats AI-related risks under the core "4Cs" online safety framework:

- **Content Risks:** Generative AI tools can bypass traditional web filters to fabricate harmful, misogynistic, radicalising, biased, or age-inappropriate material on demand.
- **Contact Risks:** This encompasses the risk of harmful online interactions directly with AI systems. Pupils must not utilise or interact with unauthorised AI chatbots or "companion" applications that simulate peer relationships or foster unhealthy algorithmic dependency.
- **Conduct Risks (AI-Generated Material):** Under UK law, the mandatory legal definition of the making or sharing of nudes and semi-nudes explicitly covers images digitally altered or wholly generated using artificial intelligence (including deepfakes or "nudifying" applications). Any individual found creating, downloading, or sharing such material will be immediately referred to the Designated Safeguarding Lead (DSL) and reported to the police.
- **Commerce Risks:** All stakeholders must remain vigilant against hyper-realistic AI-generated phishing scams, voice/video cloning impersonations, and fraudulent platforms.

Network Restrictions and Data Privacy

Free, open-consumer AI tools (especially when accessed via personal accounts) actively harvest and store whatever text, prompts, or documents are typed into them to train public models. Under data protection regulations and KCSIE online safety standards, entering any school or pupil data into these consumer platforms creates an immediate safeguarding risk and a severe data breach.

- **Network Blocks:** To protect our community, the school network actively blocks all unauthorised, free consumer AI platforms. Personal AI accounts must never be used for any schoolwork.
- **Future Provision:** The school is currently reviewing its long-term infrastructure to determine if we can safely provide enterprise versions of additional AI tools that possess appropriate, managed privacy, security, and safeguarding protections.

Approved Staff AI Tools and Operational Boundaries

To support workload management safely, Naima JPS provides and recommends two managed enterprise AI tools integrated within our secure ecosystem:

- Microsoft Copilot (utilising enterprise-protected OpenAI models) via school Microsoft 365 profiles.
- Google Gemini via official school Google Workspace profiles.

NAIMA Jewish Preparatory School

- Anthropic Claude via SSO (single sign on) official school Microsoft 365 or Google Workspace profiles and data sharing setting disabled.
- OpenAI ChatGPT via SSO (single sign on) official school Microsoft 365 or Google Workspace profiles and data sharing setting disabled.

Mandatory Requirement: Staff are strictly required to verify that they are actively signed into their official Naima JPS work accounts before interacting with these tools to ensure enterprise privacy shields remain active. If using Anthropic Claude or ChatGPT, users must ensure that within the privacy settings of their account, all data sharing options are disabled.

To remain fully compliant with data protection laws, including the *Data (Use and Access) Act 2025*, staff must strictly segment their tasks in accordance with the table below:

Zone	Meaning	Examples	Rule
GREEN	Low-risk, generic work with strictly no personal, sensitive, or identifying pupil/staff data.	**Lesson & Resource Ideas:** Generating lesson presentations, vocabulary lists, lesson ideas, or model texts. **Generic Reading Adjustments:** 'Adapt this fictional text for Year 3 reading age' (never name a specific pupil). **Non-Identifying Work Examples:** 'Here is a Year 4 written piece of work about Rome written at expected standard' (remove pupil name & identifying details). **Admin Tasks:** Generic email structures, mind mapping, or summarising statutory guidance.	**Permitted in approved tools** (Microsoft Copilot, Google Gemini, Anthropic Claude*, OpenAI ChatGPT*). **Staff check before use.** Verify all outputs for accuracy and bias.
AMBER	Potentially useful but requires extra professional judgement, source checking, copyright checks, or leadership guidance.	**Parent Communication Templates:** Drafting letters using placeholders ONLY (e.g. '[Pupil Name]', '[Date]'). **Pupil Work & Copyright:** Inputting original pupil creative work (e.g. artwork) requires explicit parental consent unless using enterprise zero-data-retention tools. **Curriculum & Assessment:** Curriculum sequencing suggestions, feedback rubrics, or translating generic school notices. **Strategic Research:** Research informing policy, image generation for school publications.	**Use anonymised/generic inputs.** Verify against authoritative sources. **Seek leadership advice** where outputs materially influence school practice or involve pupil creative IP.

NAIMA Jewish Preparatory School

RED	Personal, sensitive, confidential, high-stakes, or automated decision-making processes.	**Identifiable Pupil Data:** Pupil names, DOBs, contact details, or identifiable work samples. **Specialist Support:** SEND records, EHCP documents, medical data, or pastoral notes. **Safeguarding & Behaviour:** Safeguarding concerns, MyConcern records, or behaviour tracking logs. **HR & Leadership:** Confidential HR matters, staff performance management, or uploading internal policy drafts.	**Strictly prohibited. Do not enter into any AI tool.** **Use established school systems** (e.g. MyConcern, official database) and standard professional processes.

**Note 1 (Vendor Privacy): For Anthropic Claude and OpenAI ChatGPT, staff must ensure that data-sharing and model-training settings are manually disabled prior to use.*
***Note 2 (DfE Intellectual Property & Consent): In accordance with DfE guidance, children retain copyright over original creative work. Staff must never input pupils' original written or digital work into public/unmanaged AI tools without parental consent, as vendor terms may use inputs to train public models.*

Accuracy and Professional Accountability

- **Always check before you use:** Staff must never give AI-generated worksheets, texts, or resources directly to pupils without checking them first. You must read through and fact-check everything to catch "hallucinations" (made-up facts) or biased information.
- **No hands-off decisions:** Staff must never use AI to make decisions or help with sensitive issues regarding child protection, student welfare, safeguarding, or behaviour tracking.
- **You are responsible:** Teachers are completely and solely responsible for the accuracy, safety, and suitability of any material brought into their classrooms.
- **Keep your devices secure:** Pupils are strictly prohibited from using or handling staff laptops, iPads, or devices. This prevents children from accidentally accessing your school AI profiles, search histories, or confidential school data.

Rules for Pupil Use of AI

Supervised Use Only:

- Pupils may only interact with or utilise AI tools when under the direct supervision of a teacher for explicit, pre-approved educational purposes.
- Pupils are strictly prohibited from using AI tools that are age-restricted and these are filtered on the school network.
- Pupils are strictly prohibited from creating personal accounts or accessing consumer-facing AI systems on school premises.

- Pupils are permitted to use AI tools within the Canva app under the direct supervision of a teacher and we are currently reviewing managed age-appropriate AI tools for future use.

Homework, Assessments, and Academic Integrity:

- The use of AI tools by pupils to complete independent homework or assessments is strictly prohibited. Pupils must complete their work independently to encourage cognitive retention. Presenting AI-generated text, art, or code as original work constitutes academic dishonesty and plagiarism.
- The use of AI tools to aid classwork is at the absolute discretion of the school and the class/subject teacher.
- When authorised to use AI, pupils will be explicitly taught to proofread and fact-check AI outputs, understanding that AI is a secondary support tool, not a replacement for original thought or research.

Technical Controls, Incident Reporting and Troubleshooting

- **Technical Monitoring:** The school network utilizes Smoothwall to monitor and filter online content, track keyword detection, enforce application control, and log access attempt behaviours. In line with KCSIE 2026 mandates, this technical filtering system undergoes an annual effectiveness audit.
- **Incident Reporting:** Any technical filtering breach, accidental exposure to inappropriate AI content, or safeguarding concern must be reported instantly on MyConcern to the Designated Safeguarding Lead, Gemma Babani, or in her absence to the Deputy Designated Safeguarding Leads, Dani Karr and Corinne Nejad. Parents must report filtering errors directly to the Senior Management Team without delay.
- **Technical Troubleshooting:** If an approved AI tool or device encounters a functional issue or login failure, staff must reboot the device completely before escalating a ticket to the IT Technician via email, copying Tom Bright, Head of Computing and Digital Learning, into all digital correspondence.

Staff Training and Stakeholder Engagement

- **CPD Requirements:** All staff will receive regular Continuing Professional Development (CPD) regarding the deployment of AI to support learning safely. Training will explicitly cover data leak mitigation, spotting AI-generated online safety hazards, and recognising algorithmic biases.
- **Community Engagement:** Naima JPS commits to engaging regularly with governors, staff, pupils, and parents to listen to community views regarding emerging technologies and to communicate policy updates transparently.

Breach of Policy

Any breach of this policy will be treated with the utmost seriousness:

- Pupils: Breaches will be dealt with under the *Discipline and Promoting Positive Behaviour Policy* or, where explicit or illegal material is involved, the *Safeguarding and Child Protection Policy*.
- Staff: Violations of data privacy, utilising personal AI accounts for schoolwork, entering confidential details into AI platforms, or failing to verify resources may lead to formal disciplinary proceedings under the *Staff Code of Conduct*.

Acknowledgment

By accessing or utilising AI tools within Naima JPS, all staff and pupils agree to abide by the terms of this policy. This document must be read in conjunction with the school's Data Protection Policy, Safeguarding and Child Protection Policy, Acceptable Use Agreement and Online Safety Policy. Staff remain responsible for ensuring all AI activities strictly comply with statutory data protection regulations and online safety frameworks.