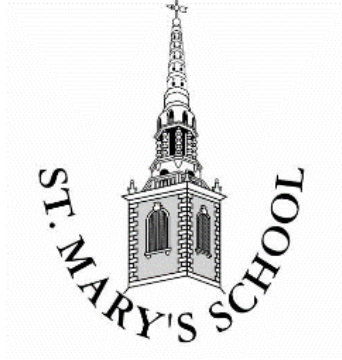




Artificial Intelligence Policy

Policy Agreed: 23rd September 2026

Review date: Autumn 2027

(Interim) Executive Head Teacher: Anthony David

Chair of Governors: Rebecca Shilling

We believe that everyone is precious and loved by God. We aspire to let our light shine in all that we do. We nurture and empower one another to flourish. Together we shine in our world by showing compassion and by serving others. Let God's light shine through us.

1. Opening statement

St Mary's CofE Primary School is committed to the highest standards. As a church school, we believe every child has an inherent spirit and potential, which we see through their natural curiosity and love of learning. This underpins our inclusive, holistic approach, so that every pupil can flourish academically, socially and spiritually. Our core vision — nurture, aspire, compassion and empower — guides our work.

We are also committed to the Convention on the Rights of the Child, as supported by UNICEF, and in particular Article 3: that the best interests of the child must be a primary consideration in all actions concerning them. That article is the test we apply to every decision in this policy.

At no point does AI replace a human. It is a tool we are learning to use to create a better learning environment. A member of staff remains accountable for every decision, every judgement and every piece of work that leaves this school.

Used well, AI can support personalised learning, reduce administrative burden and improve outcomes. This policy sets out how we secure those benefits within a framework of safety, equity and accountability.

2. Purpose and scope

2.1 Purpose

- To provide clear guidance on the safe, ethical and effective use of AI at St Mary's.
- To ensure compliance with UK law and statutory guidance.
- To foster a learning environment in which AI enriches education while protecting pupils' rights, wellbeing and safety.

2.2 Scope

This policy applies to all staff (teaching, administrative and support), governors, volunteers, pupils, and external parties such as AI suppliers and consultants who use AI tools or handle data connected with AI tools in the school context. It covers all AI systems in use — learning analytics platforms, adaptive learning tools, automated marking, generative AI, chatbots, image generation and any other AI-powered application — whether provided by the school or used by staff on their own initiative.

3. Legal and regulatory framework

This policy has due regard to:

- Keeping Children Safe in Education 2026 — which for the first time includes specific paragraphs on generative AI, and updated online risk categories reflecting AI-generated harms
- Generative artificial intelligence (AI) in education (DfE)
- Generative AI: product safety standards (DfE, updated 19 January 2026)
- The DfE's AI in education training modules and leadership toolkit, produced with the Chiltern Learning Trust and the Chartered College of Teaching
- Working Together to Safeguard Children

- UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
- The ICO's Age Appropriate Design Code (the Children's Code)
- The Online Safety Act 2023
- The Crime and Policing Act 2026 — which makes it a criminal offence to make, adapt, supply or offer to supply AI nudification tools
- Filtering and monitoring standards for schools and colleges (DfE)
- Cyber security standards for schools and colleges (DfE)
- The Equality Act 2010 and the Public Sector Equality Duty

4. Guiding principles

4.1 Child-centred

Every use of AI must enhance educational outcomes, maintain pupil agency, and protect pupils' physical and mental wellbeing. Any use of AI must comply with the safeguarding principles in Keeping Children Safe in Education.

4.2 Equity and inclusion

We ensure equitable access to AI tools for all pupils, including those with SEND. We will not allow AI to widen the digital divide, and we provide support to pupils who lack access to technology at home. We check AI tools for bias, including bias that could disadvantage pupils by ethnicity, disability, sex or background.

4.3 Privacy and data protection

We safeguard personal data under the UK GDPR and the Data Protection Act 2018, are transparent about how pupil data is collected, stored and used, minimise the collection of sensitive data, and adopt secure data governance.

4.4 Transparency and accountability

We communicate clearly with pupils, parents and staff about the purpose, benefits and risks of AI. Where AI informs a decision affecting a pupil, that decision is interpretable and open to human review.

4.5 Human in the loop

AI supports professional judgement; it never substitutes for it. Staff remain accountable for anything they produce with AI assistance.

5. Choosing and approving AI tools

No AI tool may be introduced at St Mary's — including a free tool used by an individual member of staff — without approval from the AI Coordinator. Approved tools are held on the school's AI Tools Register.

5.1 The approval process

- The AI Coordinator evaluates the tool against the DfE's Generative AI product safety standards (see 5.2) and the criteria below.

- The Data Protection Officer confirms whether a Data Protection Impact Assessment is required. A DPIA is required before any AI tool that processes pupils' personal data is adopted — not afterwards.
- The DSL confirms the safeguarding position.
- The Headteacher approves, and the tool is added to the AI Tools Register.

Evaluation criteria: educational benefit and evidence of impact; data security and privacy compliance; potential for bias or discriminatory impact; accessibility and inclusivity; age-appropriateness; and alignment with safeguarding requirements.

5.2 The DfE product safety standards — what to ask a supplier

The DfE updated its standards on 19 January 2026. They are written for suppliers, but they are the sharpest procurement checklist a school has. Four areas were added in the January update, and they are the ones most likely to catch out a tool that looks fine on the surface:

Area	What to ask
Filtering	Is harmful content prevented by design, or is a filter bolted on after the model responds? The DfE now requires embedded filtering. “We moderate afterwards” is not an acceptable answer. Does the protection hold across a whole conversation, and at home?
Mental health	Does the product detect signs of distress — negative emotional cues, escalating help-seeking, references to depression, anxiety, psychosis, suicide or self-harm — and route the child to human support, including raising a safeguarding flag to the DSL?
Cognitive development	Does it prevent “cognitive offloading” — the child getting the answer without doing the thinking? Does it report to teachers on how often pupils ask it to do the work for them?
Emotional and social development	Does it guard against dependence, and against substituting for real human relationships? This matters most with conversational tools.
Manipulation	Does it exploit the user for commercial gain — upselling, engagement-maximising design, dark patterns?
Data	Where is data stored? Is pupil data used to train the model? Can we get it deleted? Does the product meet the Children's Code?

6. Staff use of AI

Staff may use approved AI tools to support their work — planning, resource creation, drafting, administration. The following rules are absolute.

NEVER enter a child's name, personal data, sensitive data, or any safeguarding information into a public or unapproved AI tool. Once it is in, you cannot get it back, and you have made a data breach.

- Never use AI to make or record a safeguarding decision, or to write a safeguarding record. Safeguarding records are written by humans, in the child's own words where they are quoting a child.
- Never use AI to write a report, reference or assessment about a named child using their personal data in an unapproved tool.

- Always check AI output for accuracy, bias, tone and appropriateness before using it. AI tools fabricate confidently. You remain professionally accountable for anything you produce.
- Be transparent. Where AI has materially shaped a document that goes to parents or governors, say so.
- Do not use AI to generate images of children, or images that could be mistaken for real children.
- Staff use of AI is subject to the Staff Code of Conduct and the Data Protection Policy.

7. Pupil use of AI

We are a primary school. Our approach is cautious by design.

- Pupils use AI only on approved tools, only for a defined educational purpose, and only under adult supervision.
- Pupils do not have unsupervised access to open, general-purpose chatbots or image generators on school devices or the school network.
- School filtering and monitoring systems cover AI tools, and their effectiveness is reviewed at least annually, as KCSIE 2026 requires.
- Pupils are taught, in an age-appropriate way, that AI can be wrong, that it can be biased, that it is not a person and does not care about them, that anything they type into it may be stored, and that images and voices can be faked.
- Pupils are taught to tell a trusted adult if an AI tool says or shows them something that worries them.

AI and digital literacy are taught through our computing, RSHE and online safety curriculum.

8. AI and safeguarding

KCSIE 2026 recognises AI as a safeguarding risk in its own right. Staff must understand and report the following. Every concern goes to the DSL immediately.

8.1 Deepfakes, nudification and AI-generated indecent images

Freely available tools can create sexualised images of real people, including children, from ordinary photographs. AI-generated indecent images of children are illegal, exactly as photographs are. The Crime and Policing Act 2026 has made it a criminal offence to make, adapt, supply or offer to supply nudification tools — though at the time of writing the offences are not yet in force, and browser-based services are not caught by the legislation. The risk to our children is live now.

If you suspect a device contains a nude, semi-nude or indecent image of a child — including an AI-generated one — do NOT view, copy, share, forward or delete it. Secure the device. Tell the DSL immediately. The national guidance on incidents involving nudes and semi-nudes applies to AI-generated images in exactly the same way.

8.2 Image scraping

Automated tools harvest photographs from public websites and social media — including school websites — and those images can be used to create deepfake abuse material or for extortion. This is no longer hypothetical. We therefore review carefully what images of

children we publish, where, and at what resolution, in line with the Mobile Devices Policy and our consent arrangements.

8.3 AI chatbots, dependence and mental health

Conversational AI can foster dependence and can substitute for human relationships. There have been high-profile cases linking unregulated conversational AI to self-harm. Staff should be alert to a child who talks about an AI as though it were a friend, or who appears to be seeking emotional support from one. This is a wellbeing concern and should be shared with the DSL.

8.4 Radicalisation

Extremist groups use generative AI to produce propaganda at scale and to run chatbots for targeted recruitment — a vulnerable child can now be drawn towards extremism through private one-to-one exchanges with an AI, with no human moderator involved. Concerns are reported to the DSL under the Prevent duty.

8.5 Child-on-child abuse

AI-generated images, deepfakes and voice cloning used against another child are child-on-child abuse and are dealt with under the Behaviour Policy and the Child Protection and Safeguarding Policy. They are never dismissed as a prank.

9. Data protection

- A Data Protection Impact Assessment is completed before any AI tool that processes personal data is adopted.
- We collect the minimum personal data necessary, and are clear about our lawful basis for processing it.
- We do not permit pupil personal data to be used to train a supplier's model unless this has been assessed, is lawful, and is disclosed to parents.
- Robust security measures — encryption, role-based access — protect data integrity and confidentiality.
- Personal data processed through AI is retained only as long as necessary and then securely disposed of.
- Parents are told how AI is used in the school and what protections are in place. Where consent is the lawful basis, informed consent is obtained and can be withdrawn.
- Any suspected breach involving an AI tool is reported to the DPO immediately and handled under the Data Protection Policy.

10. Fairness, oversight and appeals

- AI tools are monitored for algorithmic bias and discriminatory outcomes. Where bias is found, we mitigate it or discontinue the tool until it is resolved.
- AI-driven insights complement human judgement; they do not replace it.
- Where an AI system contributes to a decision affecting a pupil, there is a clear route to request review by a qualified member of staff.
- No decision with a significant effect on a child is taken by an AI tool alone.

11. Roles and responsibilities

Who	Responsibility
Governing Body	Oversees implementation of this policy; receives an annual report on AI use, incidents and the AI Tools Register; ensures leaders remain compliant with data protection, safeguarding and education regulation.
London Borough of Islington	As our local authority, provides guidance, training and support, and is a source of advice on data protection and safeguarding in relation to AI. We work with Islington's education and information governance teams when adopting new tools with significant data implications.
Headteacher and SLT	Approve AI-related budget and resource allocation; appoint the AI Coordinator; communicate changes in this policy to staff, pupils and parents.
AI Coordinator — Anthony David	Evaluates and recommends AI tools; maintains the AI Tools Register; organises staff training on AI, data protection and safeguarding; monitors tool performance and compliance; leads the annual audit.
Data Protection Officer	Advises on DPIAs, lawful basis and data sharing; investigates any breach involving an AI tool.
Designated Safeguarding Lead	Owns the safeguarding response to AI-related concerns — deepfakes, AI-generated images, chatbots and distress, radicalisation.
Teaching staff	Use approved tools appropriately; maintain oversight of AI-assisted work; report concerns about performance, bias, data handling or safeguarding.
IT support	Ensures the infrastructure is secure and compatible; applies filtering and monitoring to AI tools; carries out system checks and updates.
Pupils	Use AI tools responsibly and follow the rules they are taught; tell an adult about anything that worries them.
Parents and carers	Engage with the school on AI; raise any concerns about their child's data or safety; talk to their child about AI at home.

12. Training

- All staff complete the DfE's AI in education training modules, developed with the Chiltern Learning Trust and the Chartered College of Teaching. The safeguarding content in these was significantly expanded in 2026 and staff engagement with them is a training priority.
- Leaders use the accompanying leadership toolkit.
- Training covers effective and ethical use, data protection, and the AI-specific safeguarding risks in section 8.
- Parents are offered written guidance or an information session on how AI is used at St Mary's.

13. Monitoring, incidents and review

- The AI Coordinator conducts an annual audit of AI tools and practice, reporting to the Governing Body.

- Any data breach, misuse of an AI tool, safeguarding concern, or evidence of bias is reported and investigated — safeguarding concerns to the DSL immediately, data concerns to the DPO.
- Findings from audits, incidents and feedback are used to refine our practice and this policy.
- This policy is reviewed annually, and sooner whenever technology, the law or statutory guidance moves — which in this field is often.

|