



AI (Artificial Intelligence) Policy

2026 to 2027

Love Learn and Shine together with Jesus

Policy information	Details
School	St Matthew's Catholic Primary School
Policy owner	Mrs Claire Sime, Headteacher
Data Protection Officer	Mrs Louisa Chamberlain
Approved by	Governing Body
Approval date	September 2026
Review date	September 2027 or sooner if law, guidance, technology or risk changes

This policy enables safe, purposeful and accountable use of artificial intelligence. AI may support teaching, learning and school operations, but it does not replace professional judgement, trusted relationships, safeguarding practice or human responsibility.

1 Purpose

St Matthew's Catholic Primary School recognises that artificial intelligence can help staff develop ideas, prepare resources, improve accessibility and reduce appropriate administrative workload. It can also generate inaccurate, biased, unsafe or misleading content and may create significant privacy, safeguarding, copyright and cyber-security risks.

This policy establishes which tools may be used, what information may be entered, how outputs must be checked, how pupils may encounter AI, and how concerns must be reported. The central rule is that a named person remains responsible for every decision, communication, resource and action supported by AI.

2 Scope

This policy applies whenever AI is used for school business, learning, teaching, assessment, communication or content creation, whether on school or personal equipment and whether the product is free or paid. It covers generative AI, chatbots, large language models, image, audio and video generators, transcription, translation, recommendation and automated decision tools, and AI features embedded in other software.

It applies alongside the Child Protection and Safeguarding, Online Safety, Data Protection, Acceptable Use, Staff Code of Conduct, Safe Use of Children's Images and Recordings, SEND, Assessment, Behaviour, Complaints and Copyright procedures.

3 Definitions

Term	Meaning
Artificial intelligence	Technology that performs tasks associated with human intelligence, such as recognising patterns, generating content, making predictions or recommending actions.
Generative AI	AI that creates new text, images, audio, video, code, presentations or other material in response to instructions or prompts.
Prompt	The instruction, information, file, image or other input supplied to an AI system.
Output	Material produced or altered by an AI system. An output may sound confident while being incorrect or fabricated.
Deepfake or synthetic media	An AI-generated or manipulated image, audio or video that realistically depicts a person saying or doing something that did not happen, or creates a convincing false person or event.
Personal data	Information relating to an identified or identifiable person. Special-category data includes information about health, ethnicity, religion, biometric data and other particularly sensitive matters.

4 Legal and guidance framework

The school will have regard to current law and guidance, including:

- Keeping Children Safe in Education 2026 and Working Together to Safeguard Children;
- the UK General Data Protection Regulation, Data Protection Act 2018 and Data Use and Access Act 2025;
- the Equality Act 2010, Children and Families Act 2014 and SEND Code of Practice;

- the Education Act 2002 duty to safeguard and promote pupils' welfare;
- the Copyright, Designs and Patents Act 1988 and applicable licensing terms;
- the Online Safety Act 2023 and relevant criminal law concerning indecent or pseudo-photographs of children, intimate images, harassment, malicious communications, fraud and impersonation;
- Department for Education guidance on generative AI in education, data protection in schools, AI product safety and filtering and monitoring; and
- Information Commissioner's Office guidance on AI, children's information and automated decision-making.

The law and providers' terms change. The school will review this policy and the Approved AI Tools Register when material changes occur rather than waiting for the annual review.

5 Principles

- Educational purpose. AI will be used only where it supports a clear educational or operational purpose.
- Human responsibility. AI may assist; it must not make the final decision or replace professional judgement.
- Privacy by design. Users enter the minimum information necessary and do not input identifiable or sensitive information unless the school has expressly approved that processing.
- Safeguarding first. AI-related concerns are reported promptly and managed under safeguarding procedures.
- Accuracy and fairness. Outputs are checked for factual errors, fabricated references, bias, stereotyping, discrimination and unsuitable content.
- Transparency. Material AI use is disclosed where a reader could otherwise be misled or where the school requires it.
- Security and approved tools. School work is carried out only through approved platforms, accounts and settings.
- Age-appropriate use. Pupil access reflects age restrictions, provider terms, curriculum purpose, supervision and risk assessment.
- Inclusion. AI should improve access and participation without lowering expectations, labelling pupils or creating unfair treatment.

6 Approved school platforms

The school maintains an Approved AI Tools Register recording the owner, purpose, users, account type, age restrictions, privacy review, data-processing arrangements, risks, controls and review date for each product. A tool appearing popular, free or already available online does not make it approved for school use.

6.1 Google Gemini

Google Gemini is the school's approved general generative AI platform. Staff must use it through their school-managed Google Workspace for Education account and only when the relevant service and settings have been enabled by the school. Personal Google accounts and consumer AI accounts must not be used for school work.

- Gemini may support brainstorming, drafting, summarising non-confidential material, resource creation, adaptation, translation drafts and administrative first drafts.
- Staff must not enter pupil or family names, contact details, work that identifies a pupil, photographs, voices, videos, safeguarding records, SEND or EHCP information, medical information, behaviour records, assessment profiles, HR information or other confidential material.
- Anonymising means removing all details that could identify a person directly or indirectly; changing a name alone is not sufficient.

- Files may be uploaded only where they contain no personal, confidential, copyrighted or restricted information and the upload is necessary for the approved purpose.
- Every output must be checked and edited by a competent member of staff before use.

Primary-aged pupils will not use Gemini independently or through personal accounts. Any teacher-led demonstration or carefully supervised pupil activity must be approved within the curriculum plan, use anonymous content, comply with provider age and access requirements, and include explicit teaching about reliability, privacy and safe use. Independent pupil accounts will not be enabled without a documented Headteacher, DPO, safeguarding and technical review and any required parental information or consent.

6.2 Chalkie AI

Teachers have access to Chalkie AI as a teacher-facing tool to assist with curriculum planning and the creation or adaptation of lesson plans, slides, worksheets, questions, activities, rubrics and other teaching resources. Chalkie AI is not a pupil platform and pupils must not be given staff logins or asked to create accounts.

- Teachers must not enter any pupil personal data or upload identifiable pupil work, photographs, audio, video, safeguarding, SEND, medical, behaviour or assessment records.
- Prompts should describe learning needs generically, for example “adapt for a Year 4 pupil who benefits from short instructions”, without using a name or a distinctive combination of details.
- Teachers remain responsible for curriculum sequence, subject accuracy, level of challenge, adaptive teaching, accessibility and suitability for the particular class.
- Generated questions, answers, diagrams, images, citations and suggested videos or links must be checked before pupils see them.
- Resources must be edited so they reflect St Matthew’s curriculum, Catholic ethos, policies and expectations rather than being used unchanged merely because they were generated quickly.

6.3 Other AI tools

No other AI tool, browser extension, app, chatbot, meeting assistant or embedded AI function may be used with school information or for routine school work until it has been approved and added to the register. A member of staff seeking approval must describe the purpose, intended users, information involved and expected benefit. The Headteacher, DPO and technical or safeguarding leads will review the request as relevant.

7 Permitted staff use

Use	Permitted conditions
Planning and resources	Ideas, first drafts and adaptation using approved tools; no personal data; teacher checks accuracy, curriculum fit, challenge, accessibility and copyright.
Administrative drafting	First drafts of generic letters, agendas, policies or summaries; no confidential case details; authorised person verifies and owns the final version.
Translation and accessibility	Draft translation, simplification, formatting, alternative explanations or accessibility support; a competent person checks meaning, tone and accuracy, especially for safety-critical information.
Research and professional learning	Starting points and summaries only; staff verify with authoritative sources and do not rely on fabricated citations or links.
Assessment support	Generation of practice questions, exemplars or generic rubrics; teachers design and validate assessment and make all judgements themselves.

Use	Permitted conditions
Creative content	Synthetic text, images, audio or video only where lawful, appropriate, clearly contextualised and not based on identifiable members of the school community without specific approval.

8 Prohibited and restricted uses

AI must not be used to:

- make or determine safeguarding, child-protection, SEND, medical, admissions, attendance, behaviour, exclusion, complaint, recruitment, capability, appraisal or disciplinary decisions;
- generate a risk assessment, referral, chronology, professional judgement or statutory document from identifiable case information;
- predict whether a pupil or adult is likely to offend, misbehave, have a diagnosis, be abused, succeed academically or pose a risk;
- monitor emotion, infer protected characteristics or profile a person without an expressly approved lawful process;
- fabricate evidence, minutes, quotations, references, observations, pupil voice, parental views, assessment outcomes or professional involvement;
- produce work that a pupil or employee presents dishonestly as entirely their own;
- create discriminatory, sexual, violent, humiliating, extremist, fraudulent or otherwise harmful content;
- create or manipulate a real person's image, voice or identity without authority;
- circumvent filtering, monitoring, access controls, licensing, payment controls or security restrictions; or
- enter passwords, security configurations, confidential contracts, financial details or information that could assist a cyberattack.

AI may help organise genuinely anonymised information, suggest questions or produce a blank template, but the accountable professional must supply and verify the substance and make the decision.

9 Personal data confidentiality and security

Information typed, spoken, pasted or uploaded into an AI product is a disclosure to that product. Deleting a chat later does not remove the need to use an approved lawful process from the outset.

- Use school-managed accounts, multi-factor authentication where available and authorised devices and networks.
- Apply data minimisation. Use fictional or fully anonymised examples whenever AI support is appropriate.
- Do not use initials, class, year group, rare condition, family event or other combined details that could allow a person to be recognised.
- Do not enter special-category data, criminal-offence data, safeguarding information or confidential employment information into generative AI.
- Report accidental disclosure, unexpected data retention, misdirected output, account compromise or other suspected breach immediately to Mrs Louisa Chamberlain, DPO, and follow the Data Breach Procedure.
- Do not copy an AI response into a pupil, personnel, safeguarding or medical record unless it has been independently verified, is necessary and is clearly identified as appropriate professional content rather than an AI conclusion.

Before approving a new tool or significant new use, the school will consider a Data Protection Impact Assessment, lawful basis, processor terms, international transfers, retention and deletion, sub-

processors, model training, access controls, age restrictions, security testing, data-subject rights and the ability to export or delete school data.

10 Safeguarding online safety and filtering

KCSIE requires schools to recognise that generative AI can create and amplify safeguarding risks and that filtering and monitoring arrangements must take account of AI use. The DSL, DPO, curriculum and technical leads will consider access routes, prompts, outputs, uploads, image generation, bypass methods and emerging patterns of harm.

- All staff apply the “it could happen here” approach and report concerns to the DSL without delay.
- Pupils are taught in an age-appropriate way that AI can be wrong, biased or manipulative; that people and images online may not be real; and that personal information, images and passwords must not be entered.
- AI does not replace supervised internet use, safe-search settings, filtering, monitoring, staff vigilance or professional curiosity.
- A blocked prompt, harmful output or concerning search may itself indicate a safeguarding need and must not be dismissed as a technical issue.
- Staff must not ask an AI system to interpret whether a disclosure is true, assess risk in place of the DSL or generate a response to a child in immediate danger.

11 Deepfakes synthetic media and impersonation

Deepfakes and other synthetic media can be used for bullying, sexual harassment, humiliation, coercion, grooming, fraud, misinformation and impersonation. A convincing image, recording or message is not proof that an event occurred; equally, the possibility of AI manipulation must never be used to dismiss a child's report.

No pupil, staff member or other user may use AI to create, alter or share content that impersonates, sexualises, threatens, humiliates or misrepresents another person. This includes face swapping, nudification, cloned voices, fabricated messages and images or recordings that appear to show a person saying or doing something they did not do.

Staff must not upload a real pupil's image, video, voice, name, work or identifying information to a generative AI system for image generation, editing, animation, background removal, avatars, voice cloning, training or experimentation. Any exceptional proposal requires prior written approval from the Headteacher and DPO, a documented safeguarding and data-protection assessment, and use of an approved service. Consumer AI tools will not be approved for this purpose.

11.1 Responding to suspected harmful AI content

1. Protect the child and establish whether there is an immediate safety risk.
2. Do not download, print, forward, copy or ask the child to send sexual, intimate or harmful material.
3. Record only the minimum necessary information, such as how the concern came to attention, platform, account, URL, date and time, without reproducing the content.
4. Report immediately to the DSL. Notify the DPO if personal data or a school system may be involved.
5. Do not investigate independently or search a device beyond the school's authority and current guidance.
6. The DSL will follow KCSIE, the Child Protection and Safeguarding Policy and current guidance on sharing nudes and semi-nudes, including AI-generated imagery, and will consider parents where safe, Children's Social Care, police, platform reporting and removal support.
7. Preserve appropriate evidence only on the advice of the DSL, police or specialist agency and record decisions and support securely.

12 Accuracy bias and quality assurance

Generative AI predicts plausible content; it does not know whether its answer is true. It may invent facts, citations, cases, quotations, links, images or explanations. It may reproduce social, cultural, racial, religious, sex, disability or other bias.

Before using or sharing output, the responsible member of staff must:

- check claims against reliable and, where appropriate, primary or official sources;
- open and verify every cited link, quotation, statistic and reference;
- check spelling, tone, reading level, safeguarding, cultural and religious appropriateness;
- check for bias, stereotypes, omissions and unequal impact;
- confirm curriculum accuracy, sequencing, terminology and level of challenge;
- check that adaptations do not narrow the curriculum or lower expectations for pupils with SEND or EAL; and
- edit the output so it represents the staff member's own professional judgement.

13 Copyright intellectual property and licensing

AI output is not automatically free to use. Inputs and outputs may reproduce or closely resemble copyrighted, trademarked or licensed material, and the legal status of some AI-generated work may be uncertain. Staff must use lawfully obtained material, comply with licences and provider terms, credit sources where required and avoid prompts intended to imitate a living artist, author or distinctive protected work for publication.

Staff must not upload textbooks, paid resources, test papers, subscription materials, unpublished school documents or substantial third-party content unless the licence and the approved platform expressly permit it. AI-generated citations are not evidence of permission. Questions should be referred to the Headteacher or DPO before publication or commercial use.

14 Transparency and marking AI use

The school will be proportionate and honest about material AI assistance. Disclosure is required where AI has made a substantial contribution to published or externally shared content; where synthetic images, audio or video could be mistaken for real material; where a pupil has been permitted to use AI in assessed work; or where a recipient reasonably needs to understand how content was produced.

Routine spelling, grammar, formatting, brainstorming or early drafting support does not need a label where a member of staff has fully checked, rewritten and accepted responsibility for the final material. AI must never be described as the author, decision-maker, witness or professional responsible for a document.

15 Teaching pupils about AI

AI literacy will be taught through computing, online safety, relationships and health education, English and other appropriate curriculum opportunities. Teaching will be age-appropriate and will include:

- what generative AI is and that it produces predictions rather than guaranteed truth;
- checking information, sources and images rather than trusting confident presentation;
- privacy, safe prompting and why personal details and images must not be entered;
- bias, stereotypes, manipulated media, deepfakes and impersonation;
- copyright, ownership, attribution and honest authorship;
- how AI can support creativity and access without replacing thinking, practice or human relationships; and
- how and where to report worrying content or requests.

16 Pupil use and academic integrity

At primary level, pupil use of generative AI will be limited, purposeful, teacher-directed and supervised. The teacher will state whether AI is allowed, what it may be used for and how any assistance should be acknowledged. Pupils must not use AI to avoid learning, complete work they are expected to produce themselves, or misrepresent AI output as their own.

Where unauthorised AI use is suspected, staff will speak with the pupil, consider age, understanding, SEND and context, review the learning process and apply the Behaviour and Assessment policies proportionately. Detection software will not be treated as conclusive proof because it can be inaccurate. The response will focus on honesty, learning and restoration as well as any necessary consequence.

17 Communication and records

AI may assist with a generic first draft, but it must not be given confidential case details or used to generate a purported record of a meeting, telephone call, observation or disclosure that it did not witness. Official records must be factual, timely and made by the responsible person. Safeguarding information is recorded on CPOMS and relevant operational information on Arbor in accordance with school procedures, not in an AI chat history.

No automated meeting transcription or note-taking tool may be used without prior approval, a lawful basis, clear notification to participants, appropriate consent where required, security controls, retention arrangements and a process for human verification.

18 Roles and responsibilities

Role	Responsibilities
Governing Body	Approve and monitor the policy; seek assurance about safeguarding, data protection, equality, procurement, training and risk; ensure appropriate challenge and resources.
Headteacher Mrs Claire Sime	Own the policy; approve school use and significant changes; ensure human accountability, training and consistent practice; decide on tool approval with relevant advisers.
Data Protection Officer Mrs Louisa Chamberlain	Advise on lawful processing, DPIAs, contracts, privacy notices, breaches, data-subject rights and the Approved AI Tools Register.
Designated Safeguarding Lead	Lead responses to AI-related safeguarding concerns; ensure KCSIE procedures, referrals, support and recording; inform filtering and monitoring review.
IT provider and system administrators	Apply approved settings, accounts, access, security, filtering, monitoring, updates and incident support; do not enable AI features without authorisation.
Curriculum and subject leaders	Evaluate educational purpose, accuracy, progression, workload impact, accessibility and staff guidance for subject use.
All staff	Use only approved tools and accounts; protect information; check outputs; disclose material use; report incidents; remain personally accountable.
Pupils	Follow teacher instructions and the Acceptable Use Agreement; protect personal information; produce honest work; report harmful or suspicious content.

19 Approval of new tools and uses

8. Request. The staff member submits the purpose, intended users, data involved, expected benefit, provider and proposed trial.
9. Educational review. A relevant leader considers curriculum value, accessibility, workload and alternatives.
10. Safeguarding and privacy review. The DSL and DPO consider age, content, data flows, terms, training, risk and whether a DPIA or contract is required.
11. Technical review. The school or IT provider considers identity, access, security, filtering, monitoring, integration, deletion and support.
12. Decision. The Headteacher approves, restricts, pilots or refuses the tool or use. No use begins before written approval.
13. Register and review. Approved conditions, users, owner and review date are added to the register. Material provider changes trigger reassessment.

20 Incidents breaches and concerns

Any harmful output, personal-data disclosure, unauthorised tool, account compromise, discriminatory decision, suspected deepfake, malicious prompt, cyber-security issue or breach of this policy must be reported promptly to the appropriate lead. The school will contain the issue, protect affected people, preserve appropriate evidence, assess risk, seek removal where relevant and consider notification to parents, the local authority, police, Children's Social Care, the Information Commissioner's Office, a platform or another body.

A good-faith report will be treated as an opportunity to protect people and improve systems. Deliberate, reckless or repeated misuse may be managed under the relevant staff or pupil conduct, behaviour, disciplinary or safeguarding procedures.

21 Training and monitoring

Staff will receive proportionate training on approved platforms, safe prompting, personal data, copyright, fact-checking, bias, deepfakes, safeguarding, disclosure and incident reporting. Pupils receive age-appropriate AI literacy and online-safety teaching. Governors receive sufficient information to exercise oversight.

Leaders will review the Approved AI Tools Register, provider changes, account settings, incidents, staff feedback, pupil use, filtering and monitoring, educational impact and equality implications. Monitoring will be proportionate and lawful and will not rely solely on automated detection.

22 Review approval and complaints

This policy will be reviewed at least annually and sooner where law, statutory guidance, provider terms, school systems, technology or risk changes. Concerns about school AI use may be raised with the Headteacher or DPO and, where unresolved, through the school Complaints Policy. Safeguarding concerns must be reported immediately and are not held pending a complaint.

Approval	Details
Approved by	Governing Body
Date approved	September 2026
Headteacher signature	

Approval	Details
Chair of Governors signature	
Next review	September 2027

Appendix 1 Approved AI Tools Register at adoption

Tool	Approved users and purpose	Conditions
Google Gemini within the school-managed Google Workspace for Education environment	Staff: general generative AI support for planning, drafting, ideas, adaptation and non-confidential administrative work. Teacher-led pupil demonstration only unless separately approved.	School account and approved settings only. No personal, special-category, safeguarding, confidential or identifiable pupil data. Human verification required. Review Google terms, controls and age access when they change.
Chalkie AI	Teachers: lesson and resource planning, slides, worksheets, questions, activities, rubrics and adaptation.	Teacher-facing only. No pupil accounts or logins. No pupil personal data or identifiable work. Teacher checks curriculum accuracy, challenge, links, media, accessibility and suitability.

The operational register may contain further technical and contractual detail and will be maintained separately so it can be updated promptly. A platform is approved only for the purposes and conditions recorded, not for every function it offers.

Appendix 2 Staff check before using AI output

- Am I using an approved tool through the correct school account?
- Have I removed all personal, confidential, safeguarding, SEND, medical, HR and identifying information?
- Is AI genuinely helpful for this task, and is a human still making the decision?
- Have I checked every fact, answer, quotation, source, link, image and calculation?
- Have I checked curriculum fit, challenge, bias, inclusion, safeguarding and the school's Catholic ethos?
- Do I have permission or a lawful licence for anything uploaded or reproduced?
- Could a reader be misled about whether content or media is real or human-created, and should I disclose AI assistance?
- Am I willing to put my name to the final version and accept full responsibility for it?

Appendix 3 AI incident response

Concern	Action
Personal or confidential information entered or exposed	Stop use; do not make further copies; preserve necessary facts; tell the DPO immediately; follow the Data Breach Procedure.
Harmful sexualised manipulated or deepfake content involving a child	Protect the child; do not download or forward; report immediately to the DSL; follow KCSIE and image-sharing procedures; notify the DPO if personal data is involved.

Concern	Action
Inaccurate biased or unsafe material shared	Withdraw or correct it promptly; tell the relevant leader; assess who received it and any harm; record and learn from the incident.
Unauthorised tool account or extension	Stop using it; tell the Headteacher or delegated AI lead and IT provider; assess data exposure; remove access when safe to do so.
Account compromise phishing or malicious prompt	Disconnect or secure the account as advised; contact IT immediately; do not enter further credentials; tell the DPO or DSL where data or safeguarding may be affected.

Appendix 4 Key references

- Department for Education: Generative artificial intelligence in education; Generative AI and data protection in schools; safe-use support materials; and generative AI product safety standards.
- Department for Education: Keeping Children Safe in Education 2026 and digital and technology standards for schools and colleges.
- Information Commissioner's Office: guidance on AI and data protection, children and the UK GDPR, automated decision-making and edtech.
- Google for Education: Google Workspace for Education terms, privacy information, administrative controls and Gemini for Education information.
- Chalkie AI: schools information, privacy notice, terms, data-processing information and provider DPIA materials.