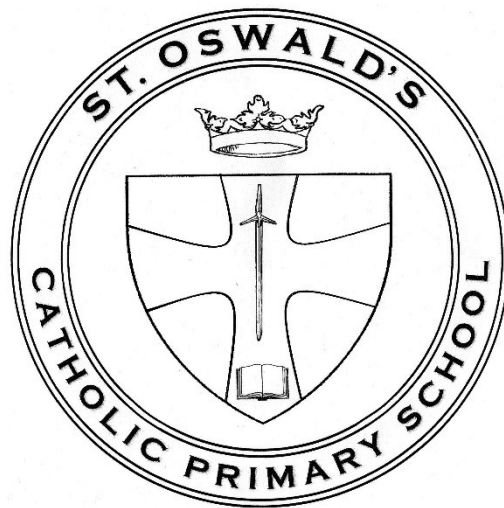


# St Oswald's Catholic Primary School



## 'Safe Use of AI' policy 2025-28

Approved by:	Approval date	Renewal date
Full Governors	4 <sup>th</sup> December 2025	Autumn 2028

This Safe Use of AI Policy is set within the context of the whole school aims and mission statement:



*Together with Jesus,  
We will Learn and Grow in Faith*

## **Policy Statement**

St. Oswald's Catholic Primary School recognises that Artificial Intelligence (AI), including generative AI tools, can provide valuable opportunities to enhance teaching, learning, inclusion, accessibility and administration. However, AI also presents risks related to online safety, safeguarding children, data protection, academic integrity, reputational risk and digital well-being.

This policy sets out the safe, ethical and responsible use of AI within the school in line with:

**Keeping Children Safe in Education (KCSIE) 2025** — particularly updated sections on misinformation, disinformation and conspiracy theories.

**Department for Education (DfE) Guidance: Generative AI – Product Safety Expectations (2024).**

**Working Together to Safeguard Children (2025).**

**The UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018.**

**Teachers' Standards and inspection expectations.**

Our school's values and commitment to safe, inclusive, ethical learning.

## **What is AI?**

AI (Artificial intelligence) means computer systems that can make suggestions, answer questions, create pictures or write text - for example, chatbots, image generators or spelling and grammar checkers.

Examples include: ChatGPT, Copilot, Google Gemini, Canva Magic Write, or AI image creators.

## **Scope**

This policy applies to all staff, pupils, governors, volunteers and contractors (including external providers) who use or may be exposed to AI tools in the school context.

It covers:

Generative AI tools

AI integrated into educational platforms (e.g. learning management systems, safeguarding software, adaptive learning tools)

Administrative, communication and marketing uses of AI

Any personal use of AI where the school is directly or indirectly identifiable (e.g. via school email, school device)

## **Statutory and Regulatory Context**

**KCSIE 2025:** Schools must recognise that online content risks can include misinformation, disinformation, conspiracy theories and must put in place appropriate online safety and safeguarding measures.

**DfE Generative AI Guidance:** Schools must ensure filtering, monitoring and safety when AI is accessed in educational contexts.

**UK GDPR & Data Protection Act 2018:** Personal and sensitive data must only be processed lawfully; schools must be clear about any AI tools used and how data is shared/stored.

**Other policy frameworks:** Intellectual Property, cyber security, safeguarding, equality, inclusion and children's rights.

## **Principles of Safe AI Use**

In line with our school's ethos and statutory requirements, AI will be used in ways that are:

**Safe** – AI tools must not expose pupils or staff to harmful, misleading, inappropriate or biased content.

**Ethical** – AI use must respect human dignity, fairness, diversity and inclusion.

**Transparent** – Pupils, staff and where appropriate parents/carers must understand when and how AI is being used.

**Responsible** – AI must not replace professional judgement in teaching, safeguarding or decision-making. Staff remain accountable for any outputs used.

**Compliant** – AI use must align with data protection law, safeguarding duties, online safety expectations, and DfE product safety expectations.

## **Roles and Responsibilities**

**Governing Body** - Oversee compliance with AI safety, safeguarding and data protection responsibilities. Ensure the policy is monitored, reviewed and updated.

**Headteacher / Senior Leadership Team (SLT) / DSL (Designated Safeguarding Lead)** - Approve AI tools before use in teaching, learning or administration. Ensure appropriate filtering, monitoring and safeguarding measures apply to AI platforms in line with DfE expectations. Leads risk assessment of new AI tools or uses. Ensure staff training, pupil education and parental guidance are in place.

**Designated Safeguarding Lead (DSL)** - Monitor risks related to AI use including exposure to harmful content, grooming risks, misinformation/disinformation. Manage safeguarding incidents linked to AI misuse, in line with the Online Safety and Safeguarding Policies.

**Data Protection Officer (DPO) (or equivalent)** - Advise on Data Protection Impact Assessments (DPIAs) for AI tools. Ensure compliance with UK GDPR, data processing agreements with AI providers. Review data retention, storage and usage of AI systems.

**Computing team including Hi-Impact** - Maintain an inventory of approved AI tools. Ensure technical and cyber-security measures (e.g. access control,

patching, monitoring logs) are in place. Work with staff and external providers to assess AI tools for suitability.

**Staff** - Use AI responsibly and only in line with this policy. Must not upload sensitive, personal or identifiable pupil/staff data into AI tools unless approved and compliant. Educate pupils on safe, critical and ethical use of AI. Monitor pupil use of AI tools; evaluate outputs for accuracy, bias or inappropriate content.

**Pupils** - Use AI tools only for authorised learning purposes and in the manner directed by staff. Must not attempt to bypass school monitoring/filtering or use AI to generate harmful, misleading, or inappropriate content. Will be taught to critically evaluate AI outputs, to recognise limitations (e.g. bias, inaccuracy) and not solely rely on AI.

**Parents/Carers** - Encouraged to understand the benefits and risks of AI, support safe use at home. Will be provided with guidance on AI safety, digital citizenship and how to support children's critical use of AI. Should be informed if the school plans to allow pupils to use AI tools at home or outside school.

### **Safeguarding, Misinformation & Disinformation**

St. Oswald's recognises that AI can generate or amplify:

**Misinformation** - False or misleading content shared without intent to mislead.

**Disinformation** - Deliberately false or misleading content, such as deep-fakes.

**Conspiracy theories** - Content undermining safe institutions or promoting harmful ideology.

To address this:

Pupils will be taught critical thinking and media literacy skills through the curriculum (e.g. Computing, PSHE/RSHE, Digital Citizenship).

Staff will receive training on identifying, evaluating and addressing risks of misinformation/disinformation via AI tools.

Any AI-related safeguarding incident (e.g. student creating/receiving inappropriate AI-generated content) will be reported to the DSL and managed as per the Safeguarding & Online Safety Policies.

The school will maintain monitoring and alerting mechanisms where possible for AI usage that could expose pupils to harmful content.

### **Data Protection, Privacy and Intellectual Property**

AI tools often store, reuse or adapt user inputs and outputs. Therefore:

No personal, sensitive, or safeguarding-related data (e.g. pupil names, contact details, pupil images, special educational needs, safeguarding incidents) may be entered into AI tools unless a formal risk assessment and data protection safeguards are in place.

Staff and pupils must ensure all material used in an AI system is anonymised or de-identified unless specific consent and safeguards exist.

Any AI tool used must be vetted for compliance with UK GDPR, data protection law and relevant UK / EU guidance.

Schools must consider intellectual property rights: inputs and outputs of AI tools may have copyright implications, and pupils' original work should not be used to train AI models without appropriate consent.

### **Curriculum, Teaching & Learning**

AI will be integrated into teaching and learning in a way that supports and enriches the school curriculum, but not as a replacement for teacher expertise.

Pupils will be educated about:

The benefits and limitations of AI (e.g. accuracy, bias, transparency).

How to recognise false or misleading content, including deep-fakes, AI-generated images/videos, incorrect outputs.

Ethical issues around AI: plagiarism, bias, intellectual property, fairness, equitable access.

Staff will use AI where appropriate (for example for planning, accessibility adaptations, differentiated resources) but will always apply professional judgment and oversee pupil work that uses AI tools.

The school will ensure that any use of AI is age-appropriate: special caution is applied in EYFS and Key Stage 1 where children are developing foundational skills; AI should not undermine this process.

Assessment and homework policies will be reviewed to reflect potential AI use (or misuse) and ensure pupil work remains authentic and attributable to pupils.

### **Use of AI in Marketing, Administration & External Providers**

Any external provider (e.g. communications/marketing agency) must have SLT approval before using AI to create or edit school content (text, images, video).

Any AI-generated content (images, text, video) must be reviewed for accuracy, appropriateness, bias, inclusivity and safeguarding implications before publication.

AI tools must not be used for decision-making about staff or pupils (e.g. recruitment, performance review, behaviour modelling, safeguarding decisions) without human oversight.

School-wide administrative AI (e.g. for scheduling, data entry) must be logged, and processing of personal data must comply with data protection and school record policies.

### **Misuse / Breaches of this Policy**

**Staff:** Misuse of AI (for example entering personal pupil data into an unapproved tool, using AI to make safeguarding decisions, distributing AI-generated content unchecked) may result in disciplinary action under the Staff Code of Conduct.

**Pupils:** Misuse of AI (such as attempting to bypass filters, using AI to generate harmful or misleading content, submitting AI-generated work as their own) will

be treated as a behaviour and safeguarding issue, and may be subject to sanctions under the school's Behaviour Policy.

**Parents/Carers:** Breaches (for example misrepresentation of the school via AI tools, sharing vulnerabilities about the school online via AI) may result in restricted access to school events, or referral to external agencies if appropriate.

**Third Parties / Suppliers:** Breaches of contract or data misuse may lead to contract termination and/or legal action.

### **Training, Awareness & Communication**

**Staff:** Initial in depth training and annual refresher training (at minimum) on AI safety, misinformation/disinformation, ethical/professional use of AI in a primary setting, and how to support pupils using AI. Additional training when new AI tools are introduced.

**Pupils:** Age-appropriate education on safe and responsible AI use through curriculum time (Computing, PSHE/RSHE) and assemblies. Pupils will be supported to build digital resilience, critical thinking and digital citizenship skills.

**Parents/Carers:** The school will provide guidance and awareness materials on AI use at home, explaining what AI is, what the school is doing, how parents can support safe use, and what to watch out for (privacy, bias, misinformation).

Clear communication channels will be established so that staff, pupils or parents can raise concerns about AI use, outputs or incidents.

### **Review & Monitoring**

This policy will be reviewed annually, or sooner if significant changes in legislation, guidance, technology or school practice occur.

The school will maintain a register of approved AI tools, their risk assessments and usage logs.

The governing body will receive regular reports on AI tool usage, incidents, training outcomes, parental engagement and any safeguarding issues related to AI.

The school will monitor the effectiveness of AI tools and adjust practice accordingly (e.g. filtering, monitoring, supervision, curriculum support).

Any significant AI-related incident (data breach, safeguarding concern, reputational risk) will trigger an immediate review of practice and potential revision of the policy.