ARTIFICIAL INTELLIGENCE (AI) ACCEPTABLE USE POLICY

2026–2027

"Learning, Living, Loving together in Christ."

Approved by	Governing Body
Date approved	22.10.2026
Review date	Autumn 2027

1. Policy Statement and Catholic Mission

At Our Lady and St Rose of Lima Catholic Primary School, we seek to use technology wisely, safely and ethically in support of our mission, 'Learning, Living, Loving together in Christ.' We recognise that artificial intelligence (AI), including generative AI, can support staff workload and the preparation of high-quality educational resources, but it also introduces risks relating to accuracy, privacy, safeguarding, bias and intellectual property.

Human dignity, the welfare of children and professional accountability are central to our approach. AI will support, not replace, teachers' expertise, children's independent learning or decisions made by responsible school staff.

2. Purpose and Scope

This policy applies to staff, pupils, governors, volunteers and contractors acting on behalf of the school, including work carried out off-site or remotely. It covers AI tools that generate, analyse, transform or recommend text, images, audio, video or other content, whether standalone or embedded in other software.

- Enable appropriate staff use of AI for planning, resources and routine administration.
- Protect pupils, families and staff from data protection and safeguarding risks.
- Set clear limits on pupil access and ensure AI literacy is taught safely.
- Require human review, transparency and accountability.

3. Legal and Guidance Framework

The school will have regard to current Department for Education guidance on generative AI in education and data protection in schools, Keeping Children Safe in Education 2026, the UK GDPR and Data Protection Act 2018, the Equality Act 2010 and relevant copyright law. This policy operates alongside the school's Safeguarding and Child Protection, Online Safety, Data Protection, SEND, Behaviour, Staff Code of Conduct and ICT Acceptable Use policies.

This document establishes the school's own acceptable-use requirements; it does not imply that national guidance requires an outright prohibition on pupil AI use.

4. Roles and Responsibilities

The Governing Body oversees this policy and receives assurance about safeguarding, data protection and implementation. The Headteacher authorises school use, ensures staff are informed and reviews any concerns. The Designated Safeguarding Lead (DSL) oversees safeguarding concerns; the SENDCo advises on inclusion and reasonable adjustments; and the Data Protection Officer (DPO) advises on data protection, procurement and assessments. All staff must follow this policy and report concerns promptly.

5. Permitted Staff Use

Staff may use AI tools for lesson and curriculum planning, drafting and adapting generic resources, creating age-appropriate examples, generating non-personalised communications and supporting routine administration, provided the use is professional, lawful and consistent with this policy.

The policy does not endorse or name particular commercial platforms. Before using a tool for school work, staff must ensure that it is permitted under school arrangements and that any necessary privacy, security, safeguarding and procurement checks have been completed.

- Staff must verify accuracy, suitability, bias, accessibility and copyright implications before sharing or using AI-generated material.
- Staff must exercise professional judgement and remain responsible for all final outputs.
- AI-generated material must not be represented as independently verified evidence or as a substitute for professional assessment.

6. Confidentiality, Personal Data and Images

Staff must not enter or upload confidential, sensitive or identifiable information about pupils, parents, carers or staff into general-purpose or unauthorised AI tools. This includes names, dates of birth, attendance or attainment records linked to individual children, SEND and EHCP information, medical details, safeguarding records, behaviour information, family circumstances and combinations of details that could identify an individual. Staff may use AI for planning, resource development and general administration only with information that is genuinely anonymised and cannot reasonably identify an individual.

Photographs, videos, voice recordings or other identifiable recordings of pupils must not be uploaded to general-purpose AI tools, including for editing, enhancement, transcription or image generation. Any proposed use of an approved specialist system involving pupil images or recordings requires a separate safeguarding and data protection assessment and express school authorisation. Staff must not use AI to create simulated images or voices of identifiable pupils without specific school authorisation and appropriate safeguards.

Any AI-enabled system proposed to process personal information must be formally approved by the Headteacher following consultation with the Data Protection Officer (DPO). Appropriate security and data protection checks, risk assessments and, where required, a Data Protection Impact Assessment must be completed before use. Staff must not independently authorise the entry of personal information. Removing a name alone does not necessarily anonymise information. If in doubt, staff must not upload it and must seek advice. Suspected unauthorised disclosures must be reported immediately in accordance with the school's Data Protection and Safeguarding Policies.

7. Pupil Access to AI

Pupil access to AI is permitted only in exceptional, carefully planned, age-appropriate and directly supervised educational circumstances with prior school authorisation and a clear learning purpose. Teacher demonstration will normally be preferred to direct pupil interaction.

Before an activity, the teacher and school must confirm that the tool's terms and minimum-age requirements permit the proposed use, that safeguarding and privacy controls are suitable, and that any required risk assessment and school approval are in place.

- Pupils must not independently access AI tools during the school day or create personal AI accounts for school activities.
- Any direct interaction must use a school-approved arrangement under continuous teacher supervision.
- Pupils must not enter personal or confidential information or upload images, videos or recordings of children.
- Pupil AI use must not replace independent thinking, original work, creativity or core knowledge and skills.
- The school may refuse or withdraw permission where safeguarding, data protection or educational concerns arise.

8. Teaching About AI and Digital Citizenship

Pupils will learn about AI, its potential benefits and limitations, misleading or fabricated content, manipulated images, fairness, privacy and safe digital behaviour through the Computing, Online Safety and RSHE curriculum. This teaching does not require children to use AI tools themselves. Activities will be age-appropriate and aligned with the school's Catholic values of truth, dignity and responsibility.

9. Safeguarding and Online Safety

AI-related concerns, including harmful outputs, grooming risks, deepfakes, impersonation, bullying, sexualised or abusive imagery and inappropriate interactions, must be reported promptly to the DSL in accordance with the Safeguarding and Child Protection Policy. Staff must not investigate suspected illegal imagery by downloading, forwarding or unnecessarily viewing it. The school will follow established safeguarding and reporting procedures and involve external agencies where appropriate.

10. Assessment and Professional Decisions

AI must not independently determine pupil attainment, grades, SEND provision, behaviour sanctions, safeguarding risk, referrals or eligibility for support. These decisions must be made by authorised staff using appropriate evidence and professional judgement. Staff may use AI to generate generic assessment materials, but must check their validity and appropriateness. Pupil work must reflect the child's own understanding and effort, with any permitted AI-supported activity clearly explained.

11. Equality, Inclusion and Accessibility

The school will consider whether AI tools or outputs may disadvantage pupils or groups through bias, inaccessible design or inaccurate assumptions. AI may support the creation of adaptable generic teaching materials, but identifiable SEND information must not be entered into general-purpose or unauthorised AI tools. Any proposed processing of personal data in an approved specialist system must follow Section 6 and must not replace individualised professional planning or statutory provision.

12. Transparency, Copyright and Communications

Staff must check that AI-generated content is suitable for its intended audience, does not infringe copyright or licensing requirements and does not misrepresent facts or sources. AI-generated images and other synthetic content should not be presented as authentic photographs or real events. Communications issued in the school's name must be reviewed and authorised through normal school processes. Parents will be informed where AI is used directly with pupils as part of an authorised educational activity.

13. Staff Training, Approval and Reporting

Staff will receive guidance on permitted uses, privacy, safeguarding, reliability and the limitations of AI. Any proposed pupil-facing use, or a new AI service intended for school-wide use, must be referred to the Headteacher for consideration with the DSL, DPO and IT support as appropriate. A data protection impact assessment will be completed where required. Concerns about misuse, unsafe outputs or accidental disclosure must be reported promptly.

14. Breaches of Policy

Suspected breaches will be considered proportionately in line with the school's safeguarding, data protection, behaviour and staff conduct procedures. The school will take account of the circumstances, seriousness,

intent and any relevant SEND or equality considerations. Serious concerns may be referred to external agencies or regulators where required.

15. Monitoring and Review

The Headteacher will monitor implementation and review this policy annually, or earlier in response to changes in technology, guidance, legislation or identified risks. The Governing Body will approve substantive revisions.