Revised: 15 November 2026
Next review: June 2027

GENERATIVE ARTIFICIAL INTELLIGENCE POLICY

Table of Contents

1.	Introduction
2.	Definitions
3.	Scope and Responsibilities
4.	Key Responsibilities
5.	Use of AI by Staff
6.	Approved Uses of AI
7.	Copyright
8.	Our Core AI Tools
9.	Use of AI by Pupils
10.	Potential Misuse of AI
11.	Ethical Use of AI
12.	Bias and Discrimination
13.	Accuracy
14.	Human Oversight
15.	Currency
16.	Data Protection Implications of Using AI
17.	Confidentiality
18.	UK GDPR Compliance
19.	Approval of New AI Tools
20.	Cyber Security
21.	Authorised AI Tools
22.	Policy Review

1. Introduction

Artificial Intelligence (AI) technology is developing rapidly and is increasingly being used across many areas of everyday life, including education. Generative AI (Gen AI) refers to technology that can create new content, including text, images, audio, presentations and other resources in response to instructions or prompts.

At Kingdom Christian School, we recognise that AI offers opportunities to support teachers, improve efficiency, reduce workload and enhance the quality of educational resources. When used appropriately, AI can be a valuable professional tool.

The school uses AI to support staff and age-appropriate learning. Classroom use includes teacher-operated demonstrations and specifically approved pupil activities through iLearn2, with Senso controls and staff supervision.

The purpose of this policy is to establish a safe, consistent and responsible approach to AI use within our school. Our aims are to:

- Support appropriate use of AI to enhance teaching and learning.
- Reduce unnecessary staff workload and improve administrative efficiency
- Protect the privacy, rights and personal information of children, families and staff
- Ensure AI is used safely, ethically and responsibly
- Maintain professional accountability and human oversight

We recognise that Gen AI can introduce risks, including inaccurate information, bias, inappropriate content, data protection concerns and potential copyright infringement.

These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, alongside clear procedures for staff.

Safeguarding and the wellbeing of our children and staff remain central to our approach.

We recognise that AI technology will continue to evolve. This policy will therefore be reviewed regularly to reflect changes in technology, legislation and relevant guidance.

2. Definitions

Artificial Intelligence (AI): Technology that enables computer systems to perform tasks that would typically require human intelligence, such as understanding language, recognising patterns, generating content or solving problems.

Generative AI (Gen AI): A form of AI that can create new content, including text, images, audio, video and computer code.

Microsoft Copilot: Microsoft's AI assistant, approved here for authorised staff use and teacher-operated demonstrations. iLearn2: the school's subscribed primary computing resource used for specifically approved, age-appropriate pupil AI activities.

Data Protection Impact Assessment (DPIA): A process used to identify and minimise data protection risks associated with certain types of personal data processing.

UK GDPR: The United Kingdom General Data Protection Regulation, which sets out requirements for the processing and protection of personal data.

Personal Data: Information relating to an identified or identifiable living individual.

Anonymised Data: Information that has been processed so that an individual can no longer be identified, directly or indirectly.

Bias: Where an AI system produces unfair or discriminatory results due to the information or assumptions on which it is based.

Hallucination: When an AI system generates information that appears factual or convincing but is incorrect or made up.

Deepfake: AI-generated or manipulated images, audio or videos that imitate a real person and may be used to mislead or impersonate them.

Human Oversight: The requirement for a person to review AI-generated information and remain responsible for decisions and actions.

3. Scope and Responsibilities

This policy applies to staff, governors, volunteers, contractors and pupils using school AI provision. Only approved tools, accounts, purposes and features may be used. Public availability or a free account does not establish suitability.

Teachers may demonstrate school-approved AI from the front of the classroom and take questions from pupils. The teacher operates the account, enters prompts and checks responses before displaying or using them. Pupils must not operate a staff account. Direct pupil AI use is permitted only for school-approved, age-appropriate activities through the school subscription to iLearn2 (ilearn2.co.uk), with staff supervision and the approved services enabled through Senso.

Only school-approved AI may be accessed through the Senso whitelist (allow list) on all school computers. Approval records must distinguish staff demonstrations from direct pupil use and identify the exact service, feature, URL, age/year group, purpose, permitted inputs and review date. A whitelist entry does not approve every feature or make a tool suitable for every child. New or externally linked tools within iLearn2 need their own checks before access is enabled.

AI agents that can independently access systems or take actions require separate written approval and assessment. All staff must read and follow this policy before use. School leaders ensure that approval records and practice remain consistent.

4. Key Responsibilities

Mark Ozenbrook - Headteacher, designated safeguarding lead (DSL), responsible senior leader for filtering and monitoring, and Google Admin Console administrator for pupil accounts.

Rebecca Jennings - Deputy Headteacher and deputy DSL.

Shani Ozenbrook - Headteacher and deputy DSL.

Lorraine Pooley - School Business Manager and authorised Senso user; escalates safeguarding concerns to the DSL or a deputy.

Stephanie McCubbin (Steph) - Safeguarding and Online Safety Governor; receives anonymised assurance reports and challenges effectiveness.

James Gill, Switch Voice and Data - School firewall administrator; coordinates firewall and network checks with Mark Ozenbrook.

Nathan Welsh, Bloobo IT Support - Microsoft account administrator; implements school-authorised Microsoft account and service settings.

Senso console access is restricted to Mark Ozenbrook, Shani Ozenbrook, Rebecca Jennings and Lorraine Pooley. All four have received online safety and other appropriate training. They use individual authorised accounts and access only information needed for their role. Governors and external IT contacts are not granted Senso console access by this policy.

The school's data protection adviser/DPO advises on lawful processing, DPIAs and breaches. Approval decisions remain accountable to school leadership. Staff supervise learning, protect information, check outputs and report concerns. This policy is read with the Online Safety, Filtering and Monitoring, Safeguarding, Data Protection and Technical Security policies and the Staff Code of Conduct.

5. Use of AI by Staff

Staff must follow Keeping Children Safe in Education 2026, applicable UK GDPR and Data Protection Act 2018 requirements as amended, and relevant intellectual property law. The school uses the current DfE AI, product safety and filtering and monitoring guidance to inform its arrangements.

Staff must not knowingly use AI technology in a way that places children, families or colleagues at risk.

AI must not replace professional judgement or be used to make significant decisions affecting individuals.

Staff must use AI responsibly, ensuring that it complements their professional knowledge, experience and expertise.

The use of AI should be carefully planned. Staff should consider whether AI is appropriate for the particular task and whether the benefits outweigh any potential risks.

Where staff are unsure, they must seek advice from Mark Ozenbrook or a deputy DSL before proceeding.

Staff remain professionally responsible and accountable for the accuracy, quality and content of any work supported by AI.

All AI-generated information must be checked, reviewed and adapted as necessary before being used, shared or published.

AI recording, transcription and note-taking tools must not be used in meetings without prior approval and an appropriate data protection assessment. All participants must be informed before any recording or transcription takes place. Any concerns raised by participants must be considered.

Online meetings arranged by the school may use approved recording or transcription facilities where appropriate. Participants must be informed, and recordings and transcripts must be stored securely and retained only for as long as necessary in accordance with the school's retention arrangements.

6. Approved Uses of AI

In line with Department for Education guidance, AI may be used by authorised staff to support appropriate professional tasks, including:

- Creating lesson plans and teaching resources
- Developing quizzes, revision activities and worksheets
- Creating differentiated and scaffolded learning materials
- Generating ideas for classroom activities and displays
- Drafting communications for parents and carers
- Supporting timetable planning and general administration
- Preparing presentations and staff training materials
- Developing school policies and procedures
- Supporting curriculum development
- Creating assembly scripts, prayers and collective worship resources
- Generating ideas for school improvement
- Summarising publicly available educational guidance

AI may assist staff in gathering information and creating educational resources, including whole-class lesson plans, extension activities and general strategies to support different learning needs.

Teachers must use their professional expertise to adapt these materials to the needs of their class.

AI may support general feedback strategies. Staff must not upload individual pupil work or assessment records unless a separately approved educational workflow explicitly permits that processing following data protection assessment. Identifiable pupil information and sensitive records remain prohibited in generative AI prompts and uploads.

All assessment decisions and feedback relating to individual children remain the responsibility of the teacher.

AI may generate general resources and ideas. Pupils may participate in teacher-operated demonstrations and directly use approved iLearn2 activities only within the controls in section 9.

AI may assist staff with the drafting of general school communications and reports. Staff must ensure that no confidential or identifiable pupil information is entered into AI systems.

AI may help staff research general educational approaches and identify ideas for school improvement. Decisions about school development, pupil progress and educational provision must remain with the appropriate members of staff.

Where AI has materially supported the production of a document, presentation or communication, staff should be transparent about its use where appropriate.

AI must not be used for personal financial gain or for purposes that contravene school policy or applicable legislation.

7. Copyright

Staff must ensure that copyrighted materials, including commercial textbooks, purchased digital resources, licensed teaching materials and third-party content, are not uploaded into AI systems unless the school has the appropriate rights or permission.

Staff must respect copyright and intellectual property when creating, adapting or publishing AI-generated materials.

AI-generated content should be checked carefully before being shared externally. Staff should be aware that AI-generated content may not automatically qualify for copyright protection under UK law.

8. Our Core AI Tools

Microsoft Copilot is approved for authorised staff use and teacher-operated demonstrations, subject to the recorded account and service settings. Pupils aged 3-11 must not use Copilot directly: Microsoft excludes under-13s from Copilot Chat. Staff use school-managed Microsoft accounts; Nathan Welsh at Bloobo IT Support manages those accounts on the school's instructions.

The school subscription to iLearn2 is the approved route for direct pupil AI activities. Teachers select the appropriate programme and confirm its recorded approval and Senso access before the lesson. Approval is specific to the activity and any underlying or externally linked tool.

Staff must use school-approved accounts, protect credentials and check privacy and data-control settings. Children must never use staff accounts. Mark manages pupil accounts through Google Admin Console; Nathan Welsh manages Microsoft accounts. Account creation or a subscription does not override age restrictions or approve all AI features.

9. Use of AI by Pupils

Teachers may demonstrate school-approved AI from the front of the classroom and take questions from pupils. The teacher operates the account, enters prompts and checks responses before displaying or using them. Pupils must not operate a staff account. Direct pupil AI use is permitted only for school-approved, age-appropriate activities through the school subscription to iLearn2 (ilearn2.co.uk), with staff supervision and the approved services enabled through Senso.

During a demonstration the teacher controls the screen, accepts questions and checks responses before displaying them. Pupils can discuss accuracy, bias and limitations. The teacher stops the activity if unsuitable content or a concern arises.

Direct pupil use is limited to the approved iLearn2 programme, age/year group and educational purpose, with staff supervision. Check provider terms,

developmental suitability, SEND needs, linked services and data handling. No general approval is given to public chatbots or a whole provider catalogue.

Only school-approved AI may be accessed through the Senso whitelist (allow list) on all school computers. Approval records must distinguish staff demonstrations from direct pupil use and identify the exact service, feature, URL, age/year group, purpose, permitted inputs and review date. A whitelist entry does not approve every feature or make a tool suitable for every child. New or externally linked tools within iLearn2 need their own checks before access is enabled.

Microsoft Copilot is not available for direct pupil use in the school's 3-11 age range. A pupil cannot bypass that restriction through a teacher account, a different sign-in or a whitelist entry.

Do not enter identifiable pupil information, photographs, videos, SEND, medical, safeguarding or behaviour records into generative AI prompts or uploads. Initials and codes do not make identifiable information anonymous. Approved iLearn2 activities may use task responses and non-identifying prompts within the recorded limits; there is no blanket permission to upload pupil work. A proposed educational workflow involving non-identifying pupil work, voice or account data requires specific approval and data protection assessment before use. Approval or whitelisting does not override the prohibited inputs above; any proposed exception requires a prior policy review. Pupil material must not be used to train AI models.

Explain safe use and how to report concerns in language pupils understand, and inform parents of the school's approach. Do not set AI homework requiring unapproved services or accounts. Any change to the approved use requires review before access is enabled.

10. Potential Misuse of AI

The school recognises that AI can be misused to create misleading, inappropriate or harmful material.

Staff should be aware of the potential for AI-generated misinformation, impersonation, deepfakes and fraudulent communications.

Staff must not use AI to create, distribute or share inappropriate, discriminatory, misleading or harmful content.

Staff must not use AI to impersonate colleagues, parents, children or other individuals, or to create misleading communications.

Report online safety or AI safeguarding concerns immediately to Mark Ozenbrook, Headteacher and DSL. If he is unavailable, contact Rebecca Jennings, Deputy Headteacher and deputy DSL, or Shani Ozenbrook, Headteacher and deputy DSL. Do not wait for the weekly review. Concerns about a Headteacher follow the separate allegations/whistleblowing route to the chair of governors or proprietor, with LADO advice as appropriate. Immediate danger requires emergency services. Data breaches also follow the Data Protection Policy and its DPO/adviser reporting route.

11. Ethical Use of AI

The school expects all staff to use AI carefully and with an awareness of its limitations.

12. Bias and Discrimination

AI-generated information may reflect bias within the data on which the system has been trained. This may result in unfair, discriminatory or inappropriate content.

Staff must review AI-generated materials to ensure that they are fair, inclusive and consistent with the school's values.

13. Accuracy

AI may generate information that appears convincing but is factually incorrect. This is sometimes referred to as a hallucination.

Staff must verify information before relying on it, particularly where it relates to safeguarding, legislation, educational guidance or statutory requirements.

14. Human Oversight

AI does not have human understanding, compassion or professional judgement. Staff must ensure that AI-generated information is reviewed and that responsibility for decisions remains with people.

AI-generated information is not always accurate or reliable. AI tools may produce misleading information, outdated guidance, incorrect facts or inappropriate suggestions.

Staff must:

- Check the accuracy of all AI-generated information.
- Ensure that resources are appropriate for the age and development of the children.
- Check that educational content is consistent with the school's curriculum, its ethos and the applicable Independent School Standards.
- Verify legal, safeguarding and statutory guidance against authoritative sources.
- Review all resources before using them in the classroom or sharing them externally.
- Ensure that content reflects the school's ethos, values and expectations.

AI must never be treated as a substitute for professional expertise or judgement.

The member of staff using AI remains responsible for the final content and any decisions made using it.

15. Currency

AI systems may not always have access to the most recent information. Staff must check current and authoritative sources where up-to-date guidance is required.

16. Data Protection Implications of Using AI

Do not enter identifiable pupil information, photographs, videos, SEND, medical, safeguarding or behaviour records into generative AI prompts or uploads. Initials and codes do not make identifiable information anonymous. Approved iLearn2 activities may use task responses and non-identifying prompts within the recorded limits; there is no blanket permission to upload pupil work. A proposed educational workflow involving non-identifying pupil work, voice or account data requires specific approval and data protection assessment before use. Approval or whitelisting does not override the prohibited inputs above; any proposed exception requires a prior policy review. Pupil material must not be used to train AI models.

General hypothetical examples and genuinely anonymous information may be used within approval limits. The restriction covers children's and families' personal details, individual incidents, written work that identifies someone, support plans and sensitive correspondence. Information is not anonymous if the school or a third party could reasonably identify the individual.

A separately proposed educational workflow involving pupil work, voice or account information must identify exactly what data is processed, by whom, where, for how long and for what purpose. Consider technical and account data as well as prompts. Complete the required data protection assessment and privacy information before use; a teacher's permission or a parental signature alone is not sufficient.

17. Confidentiality

Staff must not enter confidential school documents, internal plans, financial information, personnel records, contracts or sensitive correspondence into third-party AI unless the specific tool and purpose have been explicitly approved following appropriate checks. This is not an exception to the pupil-information restrictions in section 16.

18. UK GDPR Compliance

The school assesses approved AI against applicable UK data protection law, provider terms and its own policies. The DPO/data protection adviser must be involved where personal data is proposed. Identify a lawful basis, any additional condition for special-category data, necessary contracts, retention and deletion arrangements, security and any international transfers. Complete a DPIA before processing likely to result in high risk; record the assessment and decision.

Staff, pupils and parents receive appropriate information about the actual processing and monitoring. No statement that content is not used for model training should be taken to mean it is not stored. Microsoft school-account protections must be checked for the exact service and configuration.

19. Approval of New AI Tools

Mark Ozenbrook approves the educational and safeguarding use after consultation with the deputies and the school's data protection adviser/DPO where needed. An authorised Senso user implements the recorded whitelist change. Mark coordinates any firewall change with James Gill and Microsoft

settings with Nathan Welsh. The relevant staff and pupil profiles must be tested on all school computers before use, including new or replacement computers. Staff-only approval must not open a service to pupil accounts.

The request must identify the tool/feature and underlying provider, educational purpose, intended users and ages, account route, inputs/uploads, data collection, provider age terms, privacy/retention/model-training arrangements, content safeguards, accessibility and likely benefits and risks.

For iLearn2, record the specific programme and any external website, app, chatbot or plugin it uses. The subscription itself does not replace these checks. Approval requires suitable provider age terms and an acceptable risk assessment; complete any required DPIA first.

Record the approver, date, exact whitelist entries, staff/pupil profiles, technical tests, restrictions and next review. Check browser, app, extension and alternative sign-in routes. Do not enable a broad exception that defeats illegal-content protections or exposes staff-only AI to pupils. Disable or restrict access if the required controls cannot be verified.

20. Cyber Security

Use secure authorised accounts, appropriate permissions, authentication, supported software and updates. Senso filtering and monitoring and the school firewall support this policy. Mark manages Google pupil accounts; Nathan Welsh manages Microsoft accounts; James Gill manages the firewall. Technical roles do not confer Senso console access.

Senso console access is restricted to Mark Ozenbrook, Shani Ozenbrook, Rebecca Jennings and Lorraine Pooley. All four have received online safety and other appropriate training. They use individual authorised accounts and access only information needed for their role. Governors and external IT contacts are not granted Senso console access by this policy.

Senso logs and filtering checks are reviewed weekly on Monday. Shani Ozenbrook and Lorraine Pooley carry out the established weekly log review, with Mark Ozenbrook accountable and Rebecca Jennings providing deputy cover. High-risk email alerts are reviewed and escalated immediately when received, rather than held for Monday. Mark ensures named cover during school use. Actions, owners, outcomes and trends are recorded in the

safeguarding and technical logs as appropriate; summary assurance goes to SLT and each governing body meeting.

Staff remain alert to phishing, scams, impersonation and deepfakes. Report incidents through the DSL/deputy route in section 10 and the school's cyber-security and data-breach procedures. Monitoring records are restricted, retained and reviewed under the school's data protection arrangements.

21. Authorised AI Tools

The authorised-use record distinguishes these current routes. It must also record the exact service/account, activity-specific checks, access configuration, approval and review date.

Microsoft Copilot - authorised staff professional support and teacher-operated classroom demonstrations only. School-managed Microsoft accounts; no direct pupil access for ages 3-11.

iLearn2 school subscription (ilearn2.co.uk) - teacher-selected, school-approved, age-appropriate AI activities for pupils under supervision. Only approved programmes and checked linked services are enabled through the Senso whitelist on all school computers.

Other AI or new features - not authorised until Mark Ozenbrook has approved the specific use and the recorded technical and data protection checks are complete. Whitelist entries must reflect the authorised-use record. A platform approval does not authorise unrelated uploads or confidential information.

Use the AI risk assessment template in Appendix D of the Online Safety Policy and the 2026 online safety audit/action plan to retain supporting evidence. Outstanding configuration or training actions remain open until completion evidence is recorded.

22. Policy Review

Mark Ozenbrook and the governing body review this policy at least annually, with the deputies, relevant technical contacts and data protection adviser/DPO. Review sooner after new AI features, changed age terms, incidents, changes in processing, revised guidance or a site move. Keep the Online Safety and Filtering and Monitoring policies and audit actions aligned.

This revision was prepared on 15 November 2026. Formal governing body approval is to be recorded. Next scheduled review: June 2027.