Artificial Intelligence Policy

St Agnes C of E Primary School

Approved by:	Mrs Sue Gittins
Last reviewed on:	September 2026
Next review due by:	September 2027

Artificial Intelligence Policy

Our Vision and Mission Statement

'Learning together in God's Love'

Our Christian Vision
St Agnes is an inclusive Christian family, we want our children to:

- Learn together with respect, patience and kindness
- **Treat each other as they would like to be treated (Matthew 7v12)**
- Flourish in education and friendships
- **Live life in all its fullness (John 10v10)**
- Be proud of themselves and others
- Ensure everyone is treated equally

Through the range of experiences we offer to all our pupils we encourage an understanding of the meaning and importance of faith and promote all the Christian Values. We particularly focus on Responsibility, Creativity, Forgiveness, Perseverance, Hope, Thankfulness and Friendship. These Christian values form the basis of our vision and are embedded throughout our school life and underpin all our teaching.
St Agnes is a small school that supports our community by providing an education of the highest quality within the context of Christian belief and practice. We work closely with our families to ensure they are fully supported and cared for.
We expect everyone at St Agnes C of E Voluntary Aided Primary School to follow 'The Great Expectations' –

Be Safe
Be in the right place at the right time
Do your best
Handle your emotions
Use appropriate language
Cooperate
Respect everyone and everything

1. Purpose

This policy sets out how artificial intelligence (AI) tools may be used safely, lawfully, ethically and effectively at St Agnes C of E Primary School. AI may support teaching, learning, accessibility and workload reduction, but it does not replace professional judgement, the teacher-pupil relationship, safeguarding responsibilities, curriculum responsibility or data protection obligations.

This policy should be read in the context of Keeping Children Safe in Education 2026, the Data Protection Act 2018, UK GDPR as amended by the Data (Use and Access) Act 2025, Department for Education guidance on generative AI in education, the Generative AI: product safety standards, and the Department for Education filtering and monitoring standards.

2. Scope

This policy applies to:

- All employees, including supply and temporary staff.
- Governors.
- Volunteers and contractors.

- Pupils where AI use is permitted.
- Any third party using AI on behalf of the school.

It applies to AI used for school work or pupil activity on school premises, off-site, at home, on school-managed devices and on authorised personal devices.

Nothing in this policy authorises the use of a personal device where that use is prohibited by the Computing/Acceptable Use, Online Safety, Filtering and Monitoring, Staff Code of Conduct or mobile-phone arrangements. The same safeguarding, confidentiality, security and data-protection requirements apply wherever AI is accessed.

3. Definition of Artificial Intelligence

For this policy, AI includes digital systems that generate, transform, classify, summarise, recommend, predict or analyse content or data using automated models. This includes generative chatbots and assistants, image/audio/video generators, transcription and summarisation tools, embedded AI features, adaptive learning systems, assessment and analytics tools, and systems that use profiling or automated decision-making.

4. Core Principles

AI use within the school will follow these principles:

- **Safeguarding first:** Pupil safety, welfare and best interests take priority over convenience or efficiency.
- **Human accountability:** A named human remains responsible for every school decision, communication, resource and record produced with AI support.
- **Educational integrity:** AI must support, not replace, genuine pupil thinking, teaching and assessment.
- **Data protection by design:** Personal data will be minimised, processed only for an identified purpose and lawful basis, and protected throughout its lifecycle.
- **Transparency:** AI use will be acknowledged where it makes a significant contribution, and appropriate privacy information will be provided where personal data is processed using AI.
- **Accuracy:** Outputs will be critically checked for factual accuracy, reliability, context and suitability.
- **Inclusion and fairness:** AI must not discriminate, reinforce bias or create avoidable barriers for pupils with protected characteristics or SEND.
- **Intellectual property:** Copyright and other intellectual property rights must be respected in inputs, outputs and publication.
- **Security:** AI must not be used in a way that weakens school security, safeguarding controls, filtering or monitoring.

5. Roles and Responsibilities

The Governing Body will:

• Approve and review this policy and provide strategic oversight of AI-related safeguarding, data-protection and educational risks.
• Seek assurance that pupil-facing AI is appropriately controlled and that filtering and monitoring arrangements remain suitable.
• Receive assurance on relevant DPIAs, significant incidents, the approved AI use and staff training.

• Identify a governor or committee responsible for receiving assurance on digital safeguarding and AI governance.

The Headteacher will:

• Ensure the policy is implemented and understood.
• Ensure there is a clear AI approval process and that significant risks are escalated appropriately.
• Ensure adequate training is available and approve exceptional or higher-risk AI uses where appropriate.

The Designated Safeguarding Lead will:

• Lead on the safeguarding implications of AI and be involved in decisions about pupil-facing AI.
• Ensure AI-related safeguarding concerns are recorded and acted upon and incorporated into whole-school online-safety arrangements.

The Data Protection Officer will:

• Advise on lawful bases, special-category data, controller/processor relationships, contracts, international transfers, transparency, retention, individual rights and personal-data breaches.
• Advise on and review DPIAs.

The SLT Digital Lead / IT support will:

• Support the approval and review of AI tools used by the school.
• Assess security, permissions, authentication, filtering, monitoring and logging.
• Identify material supplier/model changes and ensure access to AI services is technically appropriate.

The Computing Lead will:

• Support age-appropriate AI literacy within the curriculum and help pupils understand that AI outputs can be wrong, biased or misleading.
• Support staff in appropriate educational use of AI.

The SENCO will:

• Be consulted where AI is proposed for SEND assessment, accessibility or personalised support which could materially affect a pupil.

All staff will:

• Follow this policy and use only approved tools for the approved purpose.
• Protect personal and confidential data, maintain professional judgement and report safeguarding, security and data-protection concerns promptly.

Pupils will:

• Follow staff instructions and Acceptable Use/Online Safety rules.
• Use AI only when and how instructed, not attempt to bypass safety controls, and tell a trusted adult if AI produces upsetting, unsafe or inappropriate content.

6. Approval, Risk Assessment and Procurement

Only AI tools or AI-enabled features approved for the relevant school use may be used for school business. The school will keep an appropriate record of AI tools approved for school

use. Approval is use-case specific: approval for staff lesson planning does not automatically permit pupil-facing use, assessment analytics or the processing of personal data.

Before approving a new AI tool, or a materially different use of an existing tool, the school will consider proportionately:

- The educational or operational purpose and whether the expected benefit outweighs the risks.
- Intended users and supplier age restrictions.
- Safeguarding risks and the suitability of filtering, moderation, monitoring and staff supervision.
- What personal or special-category data would be processed and whether it is necessary.
- The relevant lawful basis and any additional special-category condition.
- Whether the supplier acts as processor, controller or joint controller and whether suitable contractual terms are in place.
- Whether prompts, uploaded files or outputs are used to train or improve the provider's model, and whether model-training/history functions can be disabled.
- Storage location, international transfers, retention, deletion, backups and exit arrangements.
- Privacy information and support for data-subject rights.
- Security, authentication, permissions, logging, patching and cyber-security controls.
- Accuracy, bias, accessibility, equality, SEND and copyright implications.
- How supplier or model updates will be identified and reviewed.

The DSL and DPO must be consulted before procuring or deploying a pupil-facing AI tool or an AI tool that will process pupil personal data. IT support/SLT Digital Lead must assess security, filtering, monitoring and technical controls.

A Data Protection Impact Assessment (DPIA) must be completed before processing that is likely to result in a high risk to individuals. A DPIA will be completed where children's personal data is used for profiling or automated decision-making and will be reviewed following a material change to the supplier, model, purpose or data flow.

7. Staff Use of AI

Staff may use approved AI tools for appropriate purposes including:

- Lesson and curriculum planning and resource creation.
- Drafting administrative documents and routine communications.
- Generating model texts, examples, questions and ideas.
- Professional research and reflection.
- Supporting assessment processes, such as designing tasks or drafting feedback, where a teacher makes the final judgement.
- Accessibility support where the tool and use have been approved.

Staff must:

- Use only the AI tool and account approved for the intended task.
- Fact-check and sense-check outputs and verify significant factual claims using reliable sources.
- Adapt outputs to the school context, curriculum, age group and individual needs.

- Review outputs for bias, stereotyping, unsafe content, copyright risk and inaccuracies.
- Take final professional responsibility for anything used, taught, shared, recorded or sent.
- Never enter passwords, authentication codes, confidential network information or security details into an AI system.

Staff must not use AI to fabricate evidence, records, quotations, pupil work, signatures or events, or to create misleading communications purporting to come from another person. AI-generated drafts of reports, records or parent communications must be checked and edited by the responsible member of staff before use.

8. Assessment and Educational Integrity

AI may support staff in planning assessment tasks, identifying possible questions, drafting feedback or exploring patterns in learning. AI must not replace teacher professional judgement or be the sole basis for a decision about a pupil's attainment, progress, behaviour, SEND, safeguarding needs or access to support.

Pupils must not:

- Submit AI-generated work as if it were their own independent learning.
- Use AI to rewrite or artificially improve work in a way that misrepresents what they can independently understand or produce.
- Use AI in a task where the teacher has stated that AI assistance is not permitted.

Teachers will make the permitted level of AI support clear and use professional judgement to determine whether submitted work genuinely represents the pupil's learning.

9. Pupil Use of AI

Because St Agnes is a primary school, pupil-facing AI will be introduced cautiously. Pupils may use AI only through a school-approved learner-facing tool, for a defined educational purpose, within the supplier's age restrictions and with appropriate staff supervision and safeguards. Teacher-led modelling may use a teacher-facing AI tool without giving pupils their own account or direct unsupervised access.

Permitted pupil use may include:

- Learning how AI works and how to evaluate its outputs.
- Teacher-directed research or comparison activities.
- Supported accessibility where approved.
- Structured activities in which pupils critique, improve or verify AI-generated material.

Pupils must not:

- Create or use an AI account that has not been approved by the school.
- Enter their own or another person's personal, private, medical, emotional, family or safeguarding information.
- Ask AI to create harmful, sexual, discriminatory, violent, extremist or otherwise inappropriate content.
- Attempt to bypass an AI tool's safety controls or the school's filtering and monitoring.
- Submit AI-generated work as their own.

- Treat an AI system as a counsellor, friend, confidant or substitute for a trusted adult.

AI activities should preserve pupil thinking. Staff should, where appropriate, require pupils to attempt, explain, question, compare or verify before using AI-generated suggestions or answers.

10. Safeguarding and Online Safety

AI forms part of the school's whole-school online-safety and safeguarding arrangements. AI-related concerns may include harmful or sexual content, AI-generated nudes or semi-nudes, deepfakes or voice clones, impersonation, harassment or bullying, grooming or exploitation, self-harm or suicide content, extremist or radicalising material, discriminatory material, scams or malicious links, and a pupil making a personal or safeguarding disclosure to an AI service.

Any AI-related safeguarding concern must be reported immediately to the Designated Safeguarding Lead (DSL) or a deputy and recorded through the school's agreed safeguarding system, CPOMS, in accordance with the Child Protection Policy.

Staff must not ask an AI system to determine whether a safeguarding concern meets a referral threshold, assess whether a child is telling the truth, decide whether a disclosure is credible, determine whether a referral should be made or decide what safeguarding action should be taken.

AI-generated or digitally altered sexual imagery involving children, including deepfakes or "deep nudes", must be treated as a safeguarding concern and managed in accordance with Keeping Children Safe in Education, the school's Child Protection and Online Safety procedures and relevant UKCIS guidance.

11. Data Protection, Confidentiality and Lawful Basis

All AI processing of personal data must comply with the Data Protection Act 2018, UK GDPR as amended by the Data (Use and Access) Act 2025, the school's Data Protection Policy, relevant privacy notices and the school's retention and records-management arrangements.

Staff must not enter personal, confidential, medical, SEND, behaviour, safeguarding or staff HR information into open/public or otherwise unapproved AI tools.

Where an approved use genuinely requires personal data, the use must have been specifically authorised. Before processing begins, the school must identify and record an appropriate lawful basis. Where special-category data is involved, an appropriate Article 9 condition and, where required, Data Protection Act 2018 Schedule 1 condition must also be identified. The DPO will advise; consent must not be assumed to be the default lawful basis.

For approved processing involving personal data, the school will ensure that only the minimum necessary data is used; appropriate privacy information is provided; controller and processor responsibilities are established; suitable contractual and security arrangements are in place; unnecessary model-training, history or data-reuse functions are disabled where possible; and school personal data is not used for the supplier's own model training, product development or commercial purposes unless that processing has been separately assessed and found lawful.

12. Anonymisation and Sensitive Information

Where an AI task can be completed without personal data, staff must use fictional, composite or genuinely anonymous information. Removing a name does not, by itself, anonymise information. Pseudonymised information remains personal data if the individual can be re-identified using information reasonably available to the school, provider or another likely recipient.

Scenarios must not contain a combination of details that would allow a pupil, staff member or family to be identified from context. Where there is reasonable doubt, the information must be treated as personal data.

13. Profiling and Automated Decision-Making

The school will not use AI to make a final safeguarding, behaviour, SEND, admissions, employment, disciplinary or other significant decision solely by automated means. Meaningful human review must be active, informed, carried out by a person with appropriate authority and competence, and capable of changing the outcome.

The school will avoid profiling children wherever possible. Any proposed use of children's personal data for profiling or automated decision-making must be referred to the DPO and DSL before use and must be covered by a DPIA. Any exceptional proposal for a solely automated significant decision must not proceed without written approval from the Headteacher and governing body and DPO confirmation that all applicable legal safeguards are in place.

14. AI-Enabled Audio, Image and Video Recording

This policy does not authorise CCTV, facial recognition, biometric recognition, covert surveillance, continuous audio monitoring or general monitoring of staff or pupils. Those activities require separate consideration under the relevant school policy, data-protection arrangements and DPIA process.

AI-enabled recording or transcription of lessons, meetings, conversations, pupils or staff must not take place unless specifically approved in advance by the Headteacher or delegated senior leader, with DPO advice and DSL involvement where pupils are affected. Approval must identify the purpose, lawful basis, people affected, privacy information, access controls, retention period, storage arrangements, supplier data use and whether a DPIA is required.

AI must not be used to create a realistic face-swap, voice clone or other synthetic impersonation of a pupil, parent or member of staff without an exceptional, documented and lawful educational purpose and prior SLT/DSL/DPO approval. Sexualised synthetic imagery of children is prohibited and must be treated as a safeguarding concern.

15. Personal Devices, BYOD and Circumvention of Controls

Use of AI on personal devices for school purposes is subject to the school's Computing/Acceptable Use and BYOD arrangements. Personal-device use does not remove any safeguarding, confidentiality, security or data-protection obligation.

Pupils must not use mobile phones or other prohibited smart technology to access AI during the school day, except where a documented exception or reasonable adjustment applies under the school's mobile-phone arrangements. Where the school authorises BYOD laptops

or tablets for learning, they must be used under the BYOD and Acceptable Use arrangements and on the designated school network.

No user may use mobile data, a personal hotspot, tethering, a VPN, proxy service or any other technique to bypass or defeat school filtering, monitoring, access controls, age restrictions or AI safety controls. Staff must not store, upload or process school personal or confidential data through AI on a personal device unless both the device use and the specific AI processing have been formally authorised and appropriate security controls are in place.

16. Intellectual Property and Transparency

Staff and pupils must respect copyright, licensing and intellectual property when providing material to an AI system, using AI outputs or publishing AI-assisted work. Original pupil work, staff-created material or third-party copyright material must not be uploaded to a service that uses inputs for model training, product development or other commercial purposes unless the school has confirmed that there is appropriate permission, licensing or another lawful basis or applicable exception.

Staff must consider whether AI-generated output may reproduce or derive from protected material before using it in published resources, the school website or other public material. AI use should be acknowledged where it makes a significant contribution to a school document, resource or piece of work, in a manner proportionate to the context.

17. Bias, Accuracy, Equality and Accessibility

AI outputs may be inaccurate, outdated, misleading or biased. Staff must critically evaluate outputs before use. AI must not be used as the sole basis for identifying ability, SEND, behaviour risk, safeguarding risk or intervention.

Where AI is used for accessibility or personalised learning, staff must consider the individual pupil's needs, reasonable adjustments, accessibility, the Public Sector Equality Duty and whether the tool may disadvantage a pupil because of a protected characteristic.

18. Security and Cyber Safety

Users must:

- Use school-approved accounts and authentication arrangements.
- Keep passwords and multi-factor authentication codes private.
- Not attempt to jailbreak, reconfigure or bypass an AI product's safety features.
- Not follow AI-generated instructions that require installation of unauthorised software, running unknown code or weakening security settings.
- Treat unexpected AI-generated links, files, messages or requests for credentials as potentially unsafe.

Any suspected compromise, data loss, malicious use or AI-related cyber incident must be reported promptly under the school's cyber-security and personal-data-breach procedures.

19. Retention, Individual Rights and Records

AI prompts, uploaded files, outputs, account histories, monitoring logs and audit trails may constitute personal data or school records. Where they do, they must be managed under the

school's Data Protection Policy, retention schedule, privacy notices and records-management arrangements.

Personal data must not be retained in an AI service for longer than necessary for the approved purpose. The school will check supplier arrangements for retention periods, deletion, backups and caches, account closure, termination of contract, return/export of school data and final deletion.

Suppliers used to process personal data must be capable of supporting the school in responding to subject access requests, rectification, erasure, restriction, objections and other applicable individual rights. Relevant records must not be deleted once the school knows that they are required for a safeguarding matter, complaint, subject access request, investigation or legal hold.

20. Training and Awareness

Staff will receive proportionate training on safe and effective AI use, including safeguarding, data protection and confidentiality, intellectual property, bias and accuracy, cyber security, pupil-facing AI, the approved-tool process and school procedures for reporting concerns. AI-related online-safety updates will form part of wider safeguarding and digital training where appropriate.

Pupils will develop age-appropriate AI literacy through computing and online-safety education. Governors will receive sufficient information and training to provide effective oversight and challenge.

21. Breaches and Incidents

Suspected breaches of this policy will be considered under the relevant safeguarding, staff conduct, disciplinary, behaviour, data-protection or cyber-security procedure. A suspected personal-data breach involving AI must be reported immediately under the school's personal-data-breach process. A safeguarding concern must be referred to the DSL or deputy without delay.

22. Linked Policies

This policy should be read alongside the:

- Safeguarding and Child Protection Policy.
- Online Safety Policy.
- Computing Policy and Acceptable Use / BYOD arrangements.
- Filtering and Monitoring Policy.
- Data Protection Policy, privacy notices and retention schedule.
- Staff Code of Conduct.
- Staff and Governor Social Media, Messaging & Online Conduct Policy.
- Behaviour Policy and mobile-phone arrangements.
- Teaching and Learning Policy.
- CCTV Policy where AI-enabled recording or surveillance is relevant.
- Educational Visits Policy where school technology is used off-site.

23. Review

This policy will be reviewed at least annually and sooner where there is a significant change in law, statutory guidance, Department for Education standards, the school's use of AI, supplier functionality, safeguarding risk, data-protection risk or relevant technology.

24. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR).
- The procedures and practice created by this policy have been reviewed in the light of our Data Protection Policy.
- All data will be handled in accordance with the school's Data Protection Policy.

Data Audit For This Policy					
What ?	**Probable Content**	**Why ?**	**Who ?**	**Where ?**	**When ?**
Approved use of AI tools	Details of approved AI tools, approved purposes and any relevant risk assessment/DPIA information	To ensure AI tools are used safely, lawfully and for an approved purpose	Headteacher, SLT, DPO, DSL, IT support and relevant staff	Secure school systems and approved platforms	When an AI tool or new use is considered, approved or reviewed
Personal data processed through approved AI use	Minimum necessary pupil, staff or other personal data where a specifically approved use requires it	To support an authorised educational or operational purpose	Authorised staff and approved providers/processors where applicable	Approved AI platforms and secure school systems	Only when necessary for the specifically approved purpose
AI-related safeguarding, data-protection or security incidents	Relevant incident details, actions taken and associated records	To meet safeguarding, data-protection, cyber-security and accountability requirements	DSL, Headteacher, DPO and other authorised staff as appropriate	School safeguarding, data-protection or incident-recording systems	When an incident or concern occurs
Training and governance records	Staff training, approvals, reviews and	To demonstrate appropriate	Headteacher, SLT, governors, DPO and relevant staff	Secure school systems	As required and during

	monitoring information	oversight, staff competence and compliance			policy/tool reviews

- As such, our assessment is that this policy :

Has Few / No Data Compliance Requirements	Has A Moderate Level of Data Compliance Requirements	Has a High Level Of Data Compliance Requirements
	✓	