St. Peter's C.E. Primary School and Nursery

ST. PETER'S CE PRIMARY SCHOOL & NURSERY

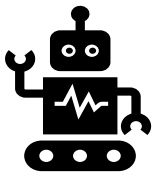
EDGMOND

School Artificial Intelligence (AI) Policy

AI-26 v1.1

IMPORTANT: AI may assist you, but it does not replace your professional judgement. You are responsible for checking its output before using, sharing, publishing or relying upon it. Never assume that a statement, quotation, calculation, legal authority, source or recommendation is correct merely because an AI system presents it confidently. Failure to undertake the checks required by this policy is a breach of the policy and may result in removal of AI access and formal action.

1. Introduction



AI - the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. includes, but is not limited to, systems that generate content, answer questions, analyse data, automate tasks, create images, audio or video, transcribe meetings, assist with coding, or act autonomously on behalf of users. Examples include Microsoft Copilot, ChatGPT, Google Gemini, Claude, GitHub Copilot, Microsoft Designer, Copilot Studio Agents, AI-powered business applications and any future products offering similar AI capabilities.

1.1 There are clear benefits and risks associated with processing data (including voice data) using Artificial Intelligence ("AI") solutions/technologies.

1.2 St. Peter's CE Primary School and Nursery is committed to taking a risk-based approach to the implementation and use of AI. This means:-

- Assessing the risks to the rights and freedoms of individuals that may arise when using AI;
- Assessing the legislative and copyright risks; and
- Implementing appropriate and proportionate technical and organisational measures to mitigate these risks.

1.3 This policy is written to ensure that the use of AI is compliant with all applicable laws, regulations and school policies. It supports the ethical and moral use of AI when undertaking school business or on behalf of the school.

1.4 This policy provides a framework for the use of AI solutions/technology by school employees (whether temporary or permanent), Governors, contractors, agents, vendors and anyone else processing information in pursuit of the schools activities.

1.5 Given the pace of AI development, this policy will be continually developed to ensure it mirrors legislative/regulatory requirements and best practice.

2. Use of AI

2.1 The use of AI solutions/technologies should always support the school's objectives.

2.2 School staff that are considering the use of AI should engage with internal stakeholders as part of their due diligence. As a minimum, the schools Data Protection Officer and IDT support should be consulted on all AI projects.

2.3 In the feasibility stage of plans to use AI, school must consider the relevant governance requirements, the provider's data-handling practices and contractual arrangements where an 'off the shelf' applications and/or technology is proposed, copyright, confidentiality, disclosure, accuracy and potential integration with other tools.

2.5 The AI solution should have appropriate logging and auditing mechanisms in place to capture activities related to AI usage.

3. Governance Requirements for Using AI

3.1 Any stakeholder looking to use/implement an AI solution/technology must be fully aware of the schools policies and procedures relating to data. As a minimum, the stakeholder must have a good understanding of the requirements detailed in the following documents:

- Data Protection Policy
- School Information Security Policy
- Records Management Policy
- Information Sharing Policy
- School Information Retention Schedule

3.2 The risks associated with the introduction and use of an AI solution/technology need to be assessed and managed. To assist in the identification, mitigation and management of AI-associated risks, the school intending to use AI must complete:

- AI Risk Assessment
- AI Data Protection Impact Assessment
- Equality Impact Assessment (where applicable)

These assessments will, as a minimum, cover any lawful basis for processing, purpose limitation, data minimisation, retention, privacy notices and data controller and processor roles.

AI projects involving children, education, safeguarding, etc must be treated as higher risk and must not proceed without enhanced DPIA review, equality consideration, senior approval and clear human oversight.

Assessments require approval before the school implements the AI solution/technology.

Appendix A sets out the workflow to adopt AI.

3.4 There are a number of key governance stakeholders where the use of AI is concerned, these include:

- Headteacher – key interest in information risk relating to the introduction of AI solutions
- Data Protection Officer – key interest in the processing of personal data by AI solutions
- IDT – key interest in the technical elements of the AI solution including security

4. Supplier/Vendor

4.1 Where a school looks to procure AI solutions/technology, engagement should be established with the relevant stakeholders.

4.2 In addition where a supplier is bidding for any school contract, the supplier must divulge if it has used AI to help support the creation of its bid.

4.3 Any use of AI should be undertaken with full knowledge of the policies, practices and terms and conditions of the relevant supplier/vendor. This includes an understanding of the supplier/vendors approach to data privacy, ethics, security and environmental/social impacts. The school must consider the supplier/vendors:

- Explanation of the AI models decision making
- Approach to addressing potential bias
- Adherence to ethical principles
- Commitment to reducing environmental impact of AI
- Ability to contribute to the regeneration of ecosystems and natural resources such as optimising energy use and improving resource management

By incorporating these considerations when procuring AI solutions, the school can ensure that suppliers/vendors contribute to a more equitable, sustainable and inclusive future.

5. Copyright Considerations

5.1 Copyright law must be complied with when using AI.

5.2 AI must not be used for generating content that infringes upon the intellectual property rights of others including, but not limited to, copyrighted materials. If the school is unsure as to whether the intended use of AI may infringe copyright, they should contact their legal support.

5.3 AI should not be used to generate logos or brand identities as the school would not own the copyright to these.

6. Accuracy of AI Output

6.1 Information produced by using an AI solution/technology **must** be reviewed by the relevant school officer for accuracy prior to sharing or using the information.

6.2 If the school has any doubt about the accuracy of AI output, then AI solutions/technology should not be used.

6.3 AI must not be used to take a significant decision about an individual solely through automated processing. Also, it must not be used in a way that, in practice, determines the outcome of a decision through a recommendation, ranking, score, classification or triage process that merely needs to be agreed, approved or otherwise 'rubber-tamped' by an authorised human.

6.4 An exception may be made only where the proposed use has been expressly approved, in writing, by the Headteacher/Data Protection Officer and supported with a documented the AI DPIA and documented automated decision-making assessment addressing Articles 22A to 22D, the lawful basis, any Article 9 or 10 condition, meaningful human involvement, safeguards, transparency and routes for challenge.

6.5 In any case where an exception to 6.3 has been granted, individuals must be provided with meaningful and clear information, a mechanism by which they can make representations, seek a human review and a route to challenge the decision.

6.6 Additionally, any automated decision-making (or ranking, scoring, triaging, recommending) must be tested for accuracy, bias, discrimination and unintended consequences and must be subject to continuous monitoring, auditing and be accompanied by a process for suspending the system and returning to human intervention.

Risk of hallucinations and inaccuracies

6.7 AI output must be treated as unverified draft material. It must not be assumed to be accurate, complete, current or lawful simply because it has been created by an approved AI system in use within the organisation.

6.8 The person using or adopting AI output remains personally responsible for the accuracy, completeness, legality and appropriateness of the resulting work. The use of AI does not transfer responsibility to the AI provider or the school involved in approving the use of the technology.

6.9 All teams and AI users must remain alert to the risks of AI systems making errors or creating 'hallucinations'. Those staff members with professional obligations must remain abreast of their relevant professional regulators' views and position on the use of AI and ensure that they use AI in accordance with any guidance issued by their professional body.

6.10 Before AI output is used, shared, published, entered into a school system or otherwise relied upon, the user must:-

- Verify factual claims against reliable and, where possible, primary sources;
- Open and verify every citation, quotation, hyperlink, case, statute, policy reference or otherwise attributed material;

- Independently check names, dates, figures and calculations;
- Check that relevant information has not been omitted;
- Check for bas, discriminatory assumptions, inappropriate language and accessibility issues;
- Check for any personal confidential, sensitive or copyrighted information;
- Correct or reject any unreliable material or output; and
- Where the output materially influences advice, a decision or service provided to an individual, record checks that have been undertaken and any corrective actions needed.

For the avoidance of doubt, any output that cannot be verified must not be relied upon.

6.11 Output used for legal, financial, safeguarding, employment, regulatory, technical or other high-risk purpose must be reviewed by a suitably qualified person independent of the person who generated the output.

6.12 Where an AI error has already affected a communication, record, recommendation or decision, the user must immediately notify their manager and the Data Protection Officer with consideration being given regarding any remedial action needed.

7. Confidentiality

7.1 Personal and confidential information must not be processed using public AI solutions such as ChatGPT, as this may enter the public domain.

7.2 If the school is planning to use a non-public AI solution, and this will include processing personal data, then as a minimum an AI Data Protection Impact Assessment must be completed.

7.3 Any processing of personal data using an AI solution must comply with the principles of the UK Data Protection Act/GDPR 2018 and Data Use and Access Act 2025.

8. Disclosure and Transparency

8.1 If AI is used to create content or support decision making, the content should be disclosed to individuals/recipients as containing AI-generated information. Any documents and/or publications that include AI-generated content should include a statement to make this clear to the reader; an example statement is detailed below:

Note: *This document contains content generated by Artificial Intelligence (AI). AI generated content has been reviewed by the author for accuracy and edited/revised where necessary. The author takes responsibility for this content.*

9. Integration with Other Tools

9.1 API and plugin tools enable access to AI and extended functionality for schools. Schools planning to integrate AI should follow Open AI's Safety Best Practices:

- **Adversarial testing** – testing AI should include typical scenarios as well as tests to 'break' the system
- **Human-in-the-loop (HITL)** – a person should review AI output before it is used more widely

- **Prompt engineering** – prompt design may reduce the chance of producing undesired content
- **Know your customer (KYC)** – AI users should have to register to use the AI solution and have a unique user ID
- **Constrain user input and limit output tokens** – limiting the amount and type of input/output can reduce the likelihood of misuse/error
- **Allow users to report issues** – a mechanism should be available to allow AI users to log concerns they have while using the AI solution
- **Understand and communicate limitations** – consider whether the AI solution has limitations that could create offensive and/or discriminatory content
- **End-user IDs** – the use of unique user IDs can help detect improper use of AI

9.2 Any relevant API and plugin tools must be rigorously tested for:

- **Moderation** – AI handles inappropriate input that can be categorised as hate, discriminatory, threatening, etc
- **Factual responses** – establish a ground of truth for the API and review responses against this

10. AI Risks

10.1 The use of AI carries inherent risks. Before AI solution/technology is implemented, a thorough risk assessment should be completed. See 3.2 for what assessments are required. The assessments required as set out in section 3.3.

10.2 Each new AI project will have its own context, data flows, output requirements and therefore needs to be assessed individually against the core requirements of this policy. The completion of the risks assessment and AI Data Protection Impact Assessment will assist the school to manage each AI project.

10.3 The use of AI systems should be periodically reviewed for accuracy, bias and continued suitability. In addition, risks associated with the use of the AI should be kept under review.

11. Compliance with Legal and Regulatory Requirements

11.1 Data processed by public facing AI solutions may enter the public domain resulting in potential personal data breaches, breaches of confidentiality compromise of intellectual property rights.

11.2 Schools using AI solutions/technology must ensure that this use complies with all applicable laws, regulations and school polices at all times.

11.3 Unauthorised use of copyrighted material or the creation of content that infringes on the intellectual property of others is strictly prohibited.

11.4 Any AI-generated content constitutes school information if held and is therefore subject to the Freedom of Information Act 2000 and the Environmental Information Regulations.

12. Bias and Discrimination

12.1 Some AI solutions may use and/or generate biased, discriminatory or offensive content. Therefore, the school using AI need to understand this and ensure any AI output is

comprehensively checked by a human to ensure biased, discriminatory or offensive content can be identified, corrected, rejected or removed.

13. Security

13.1 The school is committed to protecting the confidentiality, integrity and availability of its data.

13.2 AI solutions may store personal, sensitive and/or confidential information which could be at the risk of unauthorised disclosure through cyber-attack, misconfiguration or insecure integration of the AI technology being hacked.

13.3 Schools looking to use AI solutions must ensure that the relevant technology in place is secure. Technical controls must be commensurate with the level of risk associated with the information being processed by the AI solution.

13.4 Where the AI solution processes personal data, the school must investigate whether this data can be anonymised.

13.5 Any data processed by an AI solution should be encrypted in transit and at rest.

13.6 The AI solution should have the appropriate security accreditations such as ISO27001, Cyber Essentials+, etc. If the solution uses cloud computing, then this should comply with the NCSC Cloud Security Principles. In addition, solution suppliers should confirm if their AI solution has been developed in line with the NCSC Guidance for Secure AI System Development.

13.7 The school should check the level of security of any proposed AI solution with IDT and their Data Protection Officer.

14. Data Sovereignty and Protection

14.1 Many AI solutions will be hosted internationally. However, under data sovereignty rules any information created or collected in the originating country will remain under the jurisdiction of that country's laws.

14.2 Any AI solution used should be checked for its data sovereignty practices prior to use. If the practices cannot be determined, then the school contact their Data Protection Officer for further advice.

15. Acceptable/Unacceptable Use of AI

15.1 There are both acceptable and unacceptable uses of AI solutions at the school.

15.2 Details on what is acceptable use are included in Appendix B.

15.3 In summary, unacceptable use covers these main areas:

- Inputting personal data into public AI tools
- Using AI for surveillance/behaviour profiling
- Generating legal decisions without review
- Creating misleading or deceptive content

15.4 Where AI is used to aid decision-making, a record should be kept of the AI prompt used, the AI output and any associated decision made.

16. Training and Awareness

16.1 All users of AI solutions must receive training on the responsible and secure use of AI. This training should cover topics such as ethical considerations, risk management, security and compliance requirements.

16.2 Training should be role-based, e.g. general end user, developers, decision makers, etc.

17. Compliance

17.1 This policy applies to all schools uses of AI solutions/technology.

17.2 Any suspected or confirmed security incidents related to AI usage must be reported to the Data Protection Officer.

17.3 Failure to comply with this policy may result in disciplinary action being taken. A breach of this policy may include, but is not limited to:-

- Using an AI system that has not been approved for such use;
- Bypassing any approval or assessment processes for the implementation of AI systems;
- Entering personal, confidential or sensitive information into an unauthorised system;
- Failing to carry out or record the accuracy and quality checks referred to within this policy;
- Presenting unverified AI output as fact or professional advice;
- using AI to make, or materially influence a decision about an individual without the appropriate approvals in place;
- Failing to report a known or suspected material error, data breach, discriminatory output or security incident arising out of the use of AI; or
- Deliberately disabling or circumventing security measures or other controls.

Any disciplinary action taken will be taken fairly, proportionately and in accordance with the relevant employment procedures in place.

18. Policy Review

18.1 This policy will be reviewed periodically and updated where necessary to ensure ongoing compliance with all relevant legislation, regulations, other school policies and best practice.

Acceptable Use of AI

Key Messages

1. The school's AI Policy must be followed when using AI technology.
2. Data Protection Impact Assessments and AI Risk Assessments must be completed and signed off by the Headteacher and Data Protection Officer.
3. All other school related policies must be complied with at all times
4. IDT and Data Protection Officer must be consulted with before any AI solution is considered
5. Any staff member using an AI solution must be up to date with their data protection training and must have acknowledged and signed up to the School Information Security Policy as required

Staff using AI must comply with this acceptable use document as well as all other related school policies including:

- St. Peter's School and Nursery AI Policy
- School Information Security Policy (SISP)
- Data Protection Policy
- Records Management Policy
- Information Sharing Policy
- School Information Retention Schedule

Conditions on the Use of AI

The following are conditions of use that must be complied with when individuals use AI.

Records Management	**Accuracy of Outputs** – Outputs from any AI solution can: • Be made up, false or misleading – these are referred to as 'hallucinations' • Omit key information • Introduce bias and discrimination It is essential that any output from using AI is checked for accuracy and completeness. Users **MUST** thoroughly quality check all output from using AI.
	Management of Information – AI output must be saved in the relevant shared area, i.e. shared network drive, SharePoint, MS Teams channel, etc.

Security	**Unauthorised Access** – AI can access a number of locations to undertake its processing including potentially accessing information you should not have access to. If this occurs, contact the Data Protection Officer immediately.
	Confidential Data – Should the use of AI result in a data breach/incident, e.g. personal data has been included in a draft document in error, then this must be reported to the Data Protection Officer immediately.

Acceptable Use of AI

A1	-	Drafting correspondence (avoid including identifiable special category personal data where possible)
A2	-	Drafting general presentations
A3	-	Conducting research
A4	-	Developing lesson plans
A5	-	Creating summaries and meeting notes for internal use
A6	-	Ideas generation
A7	-	Reviewing school policies
A8	-	Writing (non-sensitive/confidential) documents
A9	-	Summarising/writing emails and Teams chat

The above is not an exhaustive list but care must be taken to, where possible, only use AI for non-sensitive / non-confidential purposes.

Unacceptable Use of AI

U1	-	Processes that could have an impact on rights and freedoms of individuals
U2	-	Processing legal information on specific cases
U3	-	Processing sensitive/confidential/identifiable information that could have a significant impact on an individual
U4	-	Using unapproved AI-generated translation tools for public-facing or client communications

---

Declaration of AI Use

All users of AI solutions must:

- Have read and agree to comply with this Acceptable Use document
- Have read and agree to comply with the latest School Information Security Policy
- Have completed relevant data protection training
- Have completed relevant AI training before use
- Only use AI for their job role

- Understand AI could access personal/confidential/sensitive information and agree to maintain the necessary measures to protect this information

- Not use AI to process any data labelled as ‘Secret’ or ‘Top Secret’

- Thoroughly check all output from using AI to ensure it is relevant and accurate

- Report any data protection issues when using AI to the Data Protection Officer as soon as they are identified

- Save AI output to the relevant shared drive, SharePoint location and/or IT system in use

- Understand that any misuse of AI may result in disciplinary action being taken and removal of access to AI on a temporary or permanent basis

Version	Date	Author	Sent To	Comments
1.1	30/9/26	R Montgomery	Schools	AI Policy compliant with best practice and legislation