ST GREGORY'S CATHOLIC PRIMARY SCHOOL

ARTIFICIAL INTELLIGENCE (AI) POLICY AND PROCEDURES

At the time of publishing the following roles were held:	
Head of School	**Antonella Fulton**
Designated Safeguarding/Online Safety Lead	**Lucie Thornthwaite**
Data Protection Officer	**Veritau**
Governor with online safety responsibility	**Veronica Morgan**

Approved by[1]			
Name:	**Veronica Morgan**		
Position:	Vice Governor		
Signed:	V. Morgan		
Version Date:	September 2026	**Version No:**	**1**
Review date[2]**:**	September 2027		

[1] This document requires approval from either the Governing Body or Proprietor
[2] This document must be reviewed annually

[1] This document requires approval from either the Governing Body or Proprietor
[2] This document must be reviewed annually

REVIEW SHEET

The information in the table below provides details of the earlier KAHSC versions of this document and brief details of reviews and, where appropriate amendments which have been made to later versions.

Version Number	KAHSC Version Description	Date of Revision/Review
1	Original	July 2026
2		

Contents

Introduction **1**

1. Legislative background and key documents **1**

2. Statement of intent **1**

3. Related policies **1**

4. Guiding principles **2**

5. Generative AI **3**

6. Responsibilities **4**

6.1 Head teacher and senior leaders 4

6.2 Designated safeguarding Lead/Online Safety Lead 4

6.3 Data Protection Officer (DPO) 4

6.4 Technical Staff 4

6.5 Staff 4

6.6 Governors 4

6.7 Parents/carers 4

7. Vulnerable groups **5**

8. Reporting **5**

9. Responding to an incident or disclosure **5**

10. Risk assessment **5**

11. Education **5**

12. Training **6**

Appendix A – Use of Artificial Intelligence in school (model risk assessment)

For school use only:

KAHSC Model Staff/volunteer ICT Acceptable Use Agreement
KAHSC Model Secondary school pupil/parent ICT Acceptable Use Agreement
KAHSC Model EYFS, Primary & Special school pupil/parent ICT Acceptable Use Agreement

This model Policy and procedures has been formulated using the SWGfL model AI Policy as a foundation.

This page is blank for printing purposes

Introduction

The integration of Artificial Intelligence (AI) in UK schools has evolved significantly over recent years, reflecting both technological advances and the educational community's response to the opportunities and challenges it presents.

A consensus is emerging about the benefits of AI to enhance personalised learning and streamline administrative tasks, while also raising concerns around data privacy, ethical use, and the preparedness of teachers to effectively integrate AI tools into classrooms.

This ongoing dialogue reflects the recognition of AI's transformative potential in education, balanced with a need for careful implementation to protect learner welfare and promote equitable outcomes. These considerations are shaping a pathway for embedding AI in schools, focusing on teacher training, ethical guidelines, and fostering digital competency among students.

1. Legislative background and key documents

The UK Online Safety Act 2023 is designed to make the internet safer, particularly for children and vulnerable users, by regulating online content and holding tech companies accountable for harmful material. It is still yet to be fully understood where there may be gaps in regulation to protect children and young people from possible harm caused by AI. Ofcom is the online safety regulator in the UK and is responsible for publishing codes of practice and guidance on how companies can comply with their duties.

There is currently little in the way of specific legislation regarding the use of AI in schools, but guidance has been developed and is being regularly updated as the technology evolves. As a result, we will consult and consider information from the following sources:

- AI Roadmap - GOV.UK
- DfE Using AI in education settings: support materials
- National AI Strategy - GOV.UK
- EU Artificial Intelligence Act 2024 - Useful high-level 4-point summary of considerations
- UNESCO AI Competency Framework for Students (Guidance)
- UNESCO AI Competency Framework for Staff (Guidance)
- Responsible AI Toolkit - GOV.UK
- Data protection in schools - Artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK
- Understanding AI for school – Tips for School Leaders - ASCL, NAHT, CST, and others
- SWGfL – Artificial Intelligence and Online Safety
- UKSIC – Protecting your setting's images from AI manipulation and abuse: guidance for schools

2. Statement of intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and pupils about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and pupils will, as always, be at the forefront of our policy and practice.

3. Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff Discipline policies and Codes of Conduct

- Behaviour policy (including anti-bullying)
- Online safety policy
- Acceptable Use Agreements
- Curriculum Policies

4. Guiding principles

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and pupils for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to DfE statutory guidance contained in Keeping Children Safe in Education.
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our school curriculum, pupils understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping pupils with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of our pupils, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.

The following bullet points can be added by the school where appropriate:

- *The school will support parents and carers in their understanding of the use of AI in the school*
- *AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support pupils to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk*
- *Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance.*

Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.

- *We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.*
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

5. Generative AI

Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources.

ChatGPT, Microsoft Copilot and Google Gemini are generative AI tools, built on large language models (LLMs). LLMs are a category of foundation models trained on large amounts of data, enabling them to understand and generate human-like content.

Tools such as ChatGPT, Microsoft Copilot and Google Gemini can:

- answer questions
- complete written tasks
- generate images, text or code
- respond to prompts in a human-like way

Other forms of generative AI can produce:

- audio
- simulations
- videos

AI is the defining technology of our age, and it is evolving at incredible speed. This technology has the potential to benefit the economy and meet societal challenges. This is not new, and we already use AI in everyday life for:

- email spam filtering
- media recommendation systems
- navigation apps
- online chatbots

Advances in technology mean that we can now use these tools to produce AI-generated content. This creates opportunities and challenges for the education sector. Further information and resources to support staff in school are available from the DfE collection '[Using AI in education settings: support materials]'

Safety is our top priority and will not be compromised when deciding whether to use generative AI in our school. Any use of generative AI by staff, students/pupils will be carefully considered and assessed, evaluating the benefits and risks of use in the school. The intended use will be specified and have clear benefits that outweigh the risks. Different considerations will apply depending on whether it is staff or pupils using AI tools.

Risk assessments will include plans for mitigating against unauthorised use cases. For example, students may use generative AI to create emails from the school to parents that seem realistic.

6. Responsibilities

6.1 Head teacher and senior leaders

Head teachers and senior leaders are responsible for the strategic planning of how AI will be used in the school, establishing the use of AI procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

6.2 Designated safeguarding Lead/Online Safety Lead

Our Designated Safeguarding Lead (DSL) / Online Safety Lead (OSL) has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

6.3 Data Protection Officer (DPO)

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

6.4 Technical Staff

Technical staff / IT Leads will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems.

6.5 Staff

It is the responsibility of **all** staff to have read and understood these procedures and associated Acceptable Use Agreements. School staff can use AI to help with things like planning lessons, creating resources, marking work, giving feedback and handling administrative tasks but are required to use their professional judgement and check that anything AI generates is accurate and appropriate. The final responsibility always rests with the staff member and the school. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- pupils understand their responsibilities

6.6 Governors

We ensure that our Governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

6.7 Parents/carers

We work hard to engage parents and carers by:

- *regular in school sessions*
- *sharing newsletters*
- *sharing information online e.g., website, social media*
- *providing curriculum information*
- ***Half termly curriculum overview***
- ***Parents evenings***

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their child's learning or safety. They are

encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

7. Vulnerable groups

We recognise that vulnerable pupils are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable pupils are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

8. Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, pupils and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- nominated member of staff
- established school reporting mechanisms
- support from IT provider
- safety alert on devices

9. Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems.

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

10. Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

We understand that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

11. Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This Policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support the following aims:

- **Enhance academic outcomes**: Improve educational experiences and performance for pupils.
- **Support teachers**: Assist in managing workloads more efficiently and effectively.
- **Educate on AI use**: Promote safe, responsible, and ethical AI practices among staff and pupils.
- **Develop AI literacy**: Incorporate AI as a teaching tool to build AI skills and understanding.
- **Prepare for the future**: Equip staff and pupils for a future where AI is integral.
- **Promote educational equity**: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing
- PHSE
- Cross curricular programmes
- Visits from outside agencies
- Assemblies

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by pupils and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- *Learner assessment*
- *Critical evaluation of emerging trends and research findings*
- *Surveys*
- *Focus groups*
- *Parental engagement*
- *Staff consultation*
- *Engaging with pupils*
- *Staff training*

The following resources are used:

- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people
- UKSIC – Protecting your setting's images from AI manipulation and abuse: guidance for schools
- Project EVOLVE - https://projectevolve.co.uk
- UKCIS DSIT "Education for a Connected World"

In line with good practice, we have created child-friendly versions of key safeguarding policies, produced and regularly evaluated in consultation with young people. List those that are available below.

12. Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity. We will:

- provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Children Safe in Education".

- ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.
- empower educators to teach pupils about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

St Gregory's Catholic Primary School Risk Assessment

Appendix A

Activity:	**Use of Artificial Intelligence in school**	**Assessment carried out by:**	Antonella Fulton		
Date assessment carried out:	September 2026	**Date for next review:**	September 2027	**Doc. ref. no. (if any):**	

What are the hazards	Who might be harmed and how?	What are we already doing to control the risks?	What else do we need to do or explain to control the risks?	Action by whom	Action by	Date done
Data protection and privacy breaches	Staff, pupils and others. Entering pupil or staff data into public AI models resulting in accidental data breaches. Unauthorised external access to sensitive or personal information and images, leading to safeguarding concerns and commercial risk	• Conduct Data Protection Impact Assessments (DPIA), share with staff and ensure compliance with UK GDPR. • Only use approved enterprise-tier AI tools that agree not to use school data for external model training. • Implement strong encryption, regular audits and UK GDPR compliant data management policies. • Conduct regular privacy audits. • Restrict public access to identifiable pupil and staff images to prevent harvesting images from school websites or social media to create deepfakes, unauthorised AI-generated media or extortion materials. • Consider guidance from the UKSIC on Protecting your school's images from AI manipulation and abuse. • Ensure any adverse data protection issues are reported to the DPO and where necessary the Information Commissioner. • Provide training for all staff on the appropriate and responsible use of AI.	• Replace images of pupils openly available on the school website/social media with alternative school content	DPO		
Cyberbullying	Staff, pupils and others. Increased potential for bullying through AI-mediated communication tools.	• Monitor AI communication tools. • Implement clear and transparent reporting mechanisms for any safeguarding or wellbeing concerns linked to AI and provide student and staff support where required. • Collaborate with parents/carers to raise awareness about AI risks and best practices.	Internet safety week Assembly	Lucie Thornthwaite		
Over-reliance on AI	Staff and pupils. Educational purpose for use of AI ill-defined. Over reliance on AI tools reducing interpersonal interactions among pupils hindering critical thinking.	• Audit the curriculum to identify where AI related issues might be incorporated into existing or new curricular programmes. • Discuss with staff the introduction of any new AI product explaining how it will benefit teaching and learning. • Clearly defined intended educational purpose for the use of AI in curricular activities. • Ensure that any generative AI used by staff or pupils has been approved by the school in advance.	Review 'Teach Computing' curriculum	Ryan O'Connor Computing Lead		

What are the hazards	Who might be harmed and how?	What are we already doing to control the risks?	What else do we need to do or explain to control the risks?	Action by whom	Action by	Date done
	Reduction in teacher autonomy and critical decision-making by overusing AI tools.	• Encourage collaborative learning activities and balance AI use with social engagement. • Define clear boundaries for AI use and regularly review its impact on pedagogy. Make use of resources such as the DfE/Chartered College of Teaching's Safe Use of AI framework to train staff on pedagogy-appropriate AI. • Adopt clear guidelines on preventing AI misuse and require pupils to document their AI usage transparently. • Implement authentic assessments and utilise plagiarism detection tools.	The Joint Council for Qualifications has a guide – AI Use in Assessments: your role in protecting the integrity of qualifications			
Emotional manipulation and mental health impacts	Pupils and staff. AI systems unintentionally affecting student mental health through curated content. Overuse of AI tools causing stress, anxiety, or dependency in pupils.	• Conduct annual reviews of AI tools and their impact on pupil and staff wellbeing ensuring the tool avoids prompting personal or emotional disclosures. • Regularly monitor AI-generated content and usage patterns. • Provide mental health resources and, where necessary, involve mental health professionals. • Set expectations on use of AI systems. • Promote media literacy.		Ryan O'Connor and Lucie Thornthwaite		
Inappropriate Content or Conduct	Pupils. AI exposing pupils to harmful or unsuitable materials / behaviour.	• Conduct rigorous testing of AI tools. • Where possible, ensure the tool has built-in content filtering in addition to effective filtering and monitoring at the school level and ensure regular human oversight. • Ensure filtering is persistent throughout a session or conversation and that it is effective across text, images, multiple languages and misspellings. • Ensure filtering works on BOYD, mobile devices and off-site use. • Prompts and responses logged by the school system are logged appropriately with safeguarding concerns or disclosures detected automatically. • Any alerts are passed to the DSL by the IT manager or external IT provider • All staff are made aware of what reports or alerts mean and the process for flagging these with the DSL.	Our IT provider to ensure filtering and monitoring systems are securely in places Teachers to report and issues	Teachers and System IT		

What are the hazards	Who might be harmed and how?	What are we already doing to control the risks?	What else do we need to do or explain to control the risks?	Action by whom	Action by	Date done
Bias and discrimination	Pupils and staff. AI systems propagating biases that impact pupil wellbeing or inclusion. AI models producing discriminatory or biased outcomes.	• Regularly audit AI algorithms for bias. • Provide inclusive media literacy education and training.		Ryan O'Connor Computing Lead		
Misuse of AI	Pupils and staff. Pupils using AI tools for harmful, unethical or illegal purposes (e.g. nudification).	• Educate pupils and staff on responsible and appropriate AI use. • Establish clear usage policies. • Ensure acceptable use agreements are provided for staff and pupils.	Taught through the curriculum	Ryan O'Connor		
Misinformation and data accuracy	Pupils and staff. Creation or spread of harmful or misleading AI-generated content. AI systems generating inaccurate or misleading recommendations	• Educate staff and pupils to verify AI outputs. • Establish clear policies for verifying content authenticity. • Regularly validate AI outputs. • Involve human oversight in decision-making.		Computing Lead		
Digital divide	Pupils. Inequitable access to AI tools among pupils from diverse demographic groups.	• Provide equitable access to AI resources and ensure alternative solutions are available to all pupils.		Ryan O'Connor		
AI ethics awareness	Pupils and staff. Lack of awareness among staff and pupils about ethical implications of AI.	• Learner and staff content is excluded from model training by default with explicit consent required for any reuse of content. • Provide training and education on AI ethics and its responsible usage. • Establish an 'Ethics in AI' group.		Computing Lead		
Legal compliance	Pupils and staff. Non-compliance with laws regarding AI usage and learner data.	• Ensure leaders, staff and pupils understand legal requirements. around the use and application of AI tools. • Conduct legal reviews and consult experts on AI-related regulations.		Ryan O'Connor System IT		

What are the hazards	Who might be harmed and how?	What are we already doing to control the risks?	What else do we need to do or explain to control the risks?	Action by whom	Action by	Date done
Cyber-security	Whole school. Increased use of AI tools in cyberattacks targeting school systems and data.	• Strengthen cyber-security protocols. • Updates and patches are applied regularly. • 'Prompt injection' and jailbreaking' protections are in place. • Educate staff and pupils on safe online practices.	Internet safety week awareness Discuss internet safety throughout the curriculum.	System IT provider Teachers		

Other Details, Reviews, or Additional Action Required	Date RA Reviewed	Significant Changes Y/N	Shared with Staff Date or N/A
This risk assessment seeks to identify significant hazards associated with this activity, who they might harm and how, and proportionate controls to reduce risk. All relevant parts and any other suitable risk assessments must be followed.			