



Generative Artificial Intelligence (AI) Policy

Acting Headteacher: Charlotte Hughes

Member of Staff Responsible: Headteacher

Reviewing Committee: FGB

Effective Date of Use:

Term of Next Review: This policy will be reviewed (a) at least annually; (b) promptly following any update to KCSIE or other statutory guidance referenced in this policy; and (c) in response to any significant change in the AI tools approved for use by the school. Given the pace of change in this area, The Headteacher is authorised to make interim updates to this policy between formal governor reviews when required to ensure compliance with updated statutory guidance, with any such changes reported to the FGB at the next available meeting.

Non Statutory Policy

Version Control			
Version	Date	Notes and amendments	Approval
0.1	21/10/2025	Initial draft	FGB not Approved
0.2	05/11/2025	Edits following feedback from Governors	FGB Feb 26
0.3	12/01/2026	Edits following meeting with Vital and Diocese. Changed to Google Gemini, Added Policy links, added flourishing and strategy, sustainability. DFE updates.	FGB June 26
0.4	17/08/26	Edits following KSCIE 2026	21st Oct FGB

St Paul's C of E Primary School

A Place to Belong

Our Christian Vision

Our school is a family where everyone feels safe, happy and valued, and is supported to achieve their full potential.

We will develop compassionate and caring individuals who depend on one another, are highly motivated, and have a life-long love of learning in preparation for the future.

Our Core Values

All that we do is underpinned by the core Christian values of *Family (Koinonia)*, *Compassion*, *Perseverance and Forgiveness*

"Though we are many, we form one body, all joined together as members of the whole. We each have different gifts, according to the grace given to each of us. We must use them wisely."

Romans 12:5-8

Introduction and Scope

This policy provides a framework regarding our use of generative artificial intelligence (AI). Generative AI describes any type of artificial intelligence (AI) that can be used to create new text, images, video, audio, or code. Large Language Models (LLMs) are part of this category of AI and produce text outputs.

Generative AI is fast becoming an integral part of the workplace, offering powerful tools for various tasks such as content creation, data analysis, and problem-solving. To ensure its responsible and ethical use, employees must adhere to guidelines that promote accuracy, respect privacy, and minimise potential risks.

This policy outlines the school's expectations for AI use by students, staff, and visitors. The policy focuses on minimising risks, enhancing teaching, and learning practices, preparing staff and students for future use of technology, maximising benefits to staff workload and ensuring safety, professionalism, and privacy. This will be done in line with the DfE policy on AI in Education (Generative artificial intelligence (AI) in education).

This policy applies to all members of the school community, including:

- i) the workforce: employees, governors, contractors, agents, representatives, volunteers, and temporary staff working for or on behalf of the school — individuals found to knowingly or recklessly infringe this policy may face disciplinary action; and
- ii) pupils of the school, to the extent that this policy governs conduct during the school day or in connection with school activities, pupils found to breach this policy will be dealt with in accordance with the school's Behaviour Policy.

For the avoidance of doubt, the prohibition on direct pupil use of AI tools applies to pupils regardless of whether the device used is school-owned or personal.

Periodic assessments of AI systems' impact on education and ethics will be conducted, and adjustments to the policy will be made accordingly.

We recognise that the regulatory and guidance framework governing AI in education is evolving rapidly. This policy will be kept under active review and updated promptly in response to any revisions to statutory guidance, including but not limited to updates to Keeping Children Safe in Education (KCSIE), DfE AI in Education guidance, data protection guidance for schools, filtering and monitoring expectations, and the DfE Generative AI Product Safety Standards. Staff should seek advice from the Headteacher where they are unsure whether a proposed use of AI is permitted.

This policy should be read alongside other school policies. This includes but is not limited to -

- Safeguarding and Child Protection Policy
- Complaints Policy
- E Safety Policy
- Staff Code of Conduct
- Safer Recruitment Policy

- RSHE Policy

Legal, statutory and non-statutory framework

This policy is informed by the following legal requirements, statutory guidance and non-statutory Guidance:

Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR)

Equality Act 2010

Online Safety Act 2023

Copyright, Designs and Patents Act 1988

Keeping children safe in education 2026 (KCSIE) - in force from 01 September 2026

Data protection in schools - Generative artificial intelligence (AI) and data protection in schools (DfE, 03 February 2023, updated June 2026)

Generative artificial intelligence (AI) in education (DfE, updated 12 August 2025)

Generative AI: product safety standards (DfE, updated 19 January 2026)

Using AI in education settings: support materials (DfE, 10 June 2025, updated 19 May 2026)

Meeting digital and technology standards in schools and colleges - Filtering and monitoring: core standard (DfE, 23 March 2022, updated 24 June 2026)

Public Sector Equality Duty: guidance for public authorities (Government Equalities Office, 18 December 2023)

Flourishing and Vision

At the heart of our school is a commitment to being a family where every individual feels safe, happy, and truly valued. Guided by our core Christian values of Koinonia (Family), Compassion, Perseverance, and Forgiveness, we strive to create an environment where everyone is supported to reach their full potential. To fulfill this vision, we embrace innovation as a way to nurture a life-long love of learning and prepare both our students and staff for the future. By integrating AI into our daily practice, we aim to empower our educators, providing them with the tools necessary to unlock new levels of creativity and excellence in the classroom.

We believe that supporting the wellbeing of our staff is essential to maintaining a compassionate and caring community. By supporting staff to use AI to assist with routine, time-consuming tasks, we can reduce administrative burdens and allow our staff to focus on what matters most: building meaningful relationships, quality teaching and inspiring our pupils. This approach embodies the value of Perseverance, as we use modern technology to overcome challenges and create a sustainable, balanced environment where staff can flourish.

Alongside these opportunities, the school takes a considered and cautious approach. The evidence base on the long-term impact of AI on children's learning, emotional development, and wellbeing is still developing, and we take seriously the advice of cognitive scientists and the DfE's own guidance that schools should 'act more slowly' and not feel pressurised to adopt AI tools before they are satisfied it is safe and appropriate to do so. Our Christian vision places human relationships, between teachers and pupils, between families and the school, and within our school community, at the centre of everything we do. AI must serve those relationships, not substitute for them. We will not introduce AI tools simply because they are available or because others are using

them, but only where we are satisfied they are safe, lawful, appropriate, and genuinely beneficial to our children and our staff.

Roles and Responsibilities

Overall responsibility for adherence to this policy lies with the Headteacher, who will designate responsible individuals to oversee AI-related decisions and ensure compliance with this policy. They will ensure the use of generative AI aligns with our educational objectives, legal obligations, and ethical principles.

AI technologies may be integrated into the curriculum to enhance learning experiences, provided that such use aligns with our educational objectives and goals. Appropriate guidance and training will be given to staff about the use of AI systems to ensure that AI tools are applied effectively, including the appropriate integration of these technologies into student education.

Staff must not use any personal accounts for AI use in school. Staff may only use platforms authorised by the Headteacher. Training will also include effective, safe prompting techniques and how to critically evaluate AI outputs for any mis-information, lack of accuracy or bias. This includes actively checking outputs to ensure they do not contain or promote misogyny, misandry, or gender-based stereotypes.

The school will comply with the DfE's Filtering and Monitoring Standards for Schools and Colleges, which are statutory under KCSIE. Leaders and governors will conduct an annual review of the school's filtering and monitoring provision, considering how it applies to any generative AI tools in use by staff or pupils. Reports from filtering and monitoring systems will be a standing agenda item at relevant leadership and governor meetings. Any use of generative AI tools by pupils will only be permitted through systems that provide appropriate filtering, activity monitoring and safeguarding alerts, in line with the DfE Generative AI Product Safety Standards.

All staff are responsible for adhering to this policy when using AI technology.

We will always seek advice and guidance from our Data Protection Officer (DPO) regarding our data protection obligations concerning AI use.

Visitor Responsibilities

- If visitors use AI to generate content (text, images, etc.) during their visit, they are responsible for ensuring this content is appropriate, respectful, and does not violate any school policies or legal regulations (e.g., copyright).
- Visitors must not use AI in ways that could compromise the privacy or security of student or staff data. This includes refraining from inputting sensitive personal information into AI tools while on school premises or using school resources.
- If visitors are supervising students who are using AI, staff must obtain the consent of the Headteacher for such use and the staff member concerned is responsible for ensuring the students' use aligns with the school's AI policy.

- Visitors should promptly report any concerns they have about the misuse of AI by others to a designated staff member.
- Visitors should not use school resources or interactions with students/staff to intentionally train or fine-tune external AI models.
- Visitors must comply with any specific instructions or guidance provided by school staff regarding the use of AI during their visit.
- If visitors use AI applications on their personal devices while on school premises, they are still expected to adhere to these guidelines.

Governors

The Governing Body is responsible for:

- approving this policy and any subsequent amendments, including interim updates made by the Headteacher in response to changes in statutory guidance;
- ensuring the policy aligns with current statutory guidance, including the most recent version of Keeping Children Safe in Education (KCSIE) and any DfE guidance on AI in education;
- receiving a report from the Headteacher at each FGB meeting on any significant developments in AI use within the school, any incidents involving AI, and any updates to the risk assessment in Appendix Two;
- confirming annually that a review of the school's filtering and monitoring provision has been completed and that it covers any AI tools in use by staff;
- ensuring that a named link governor holds responsibility for AI and digital technology, and that this governor receives appropriate briefing to fulfil that role;
- making and recording an explicit, informed decision as to whether direct pupil use of AI tools is permitted, noting that the current position is that it is not, except within structured online safety education delivered by a member of staff; and
- approving any future proposal to extend pupil access to AI tools, having first satisfied itself that the conditions set out in the Student Use section of this policy have been met.

The Governing Body may authorise the Headteacher to make interim amendments to this policy between formal FGB reviews where required to ensure compliance with updated statutory guidance. Any such interim changes must be reported to the FGB at the next available meeting.

Google Gemini

To ensure our staff can explore the benefits of AI with confidence, our school currently authorises the use of Google Gemini only through our managed Google Workspace for Education accounts. The school's educator accounts provide "enterprise-grade" data protection, meaning our conversations are kept within our school's secure "closed" environment and are not used by Google to train its public AI models or reviewed by human moderators.

However, in line with this policy, we still require all staff to remain vigilant. Even within this secure system, no personally identifiable information (such as pupil names, addresses, or sensitive staff data) should be entered into the AI under any circumstances. By treating the AI as a creative

partner rather than a database for sensitive records, we uphold our core value of Compassion, protecting the privacy of our school family while harnessing the best of modern technology to support our collective potential. Whilst staff have been instructed that no personal data be inputted or processed via the AI, a DPIA has been completed for Google Gemini. This serves as a secondary layer of governance, ensuring that the platform meets our data protection standards regardless of the specific nature of user prompts.

A copy of the DPIA is at appendix 3.

Staff must not use personal accounts for any school-related AI activity. Staff may only use the school's managed Google Workspace for Education Gemini accounts.

The school will configure its Google Workspace settings to ensure that Gemini activity logs are retained for an appropriate period, in line with the school's data retention schedule. Staff must not manually delete their Gemini activity history, as this record may be required in the event of a complaint, disciplinary matter, or data subject access request. The Headteacher will seek advice from the DPO on the appropriate retention period and configure workspace settings according.

- **Link:** [Gemini for Google Workspace - Education](#)
- **Link:** [Privacy & Security FAQs - Google for Education](#)
- **Link:** [Bringing Gemini to Google Workspace for Education](#)

Quick Security Checklist for Staff

Safe to Use	Do Not Enter
General lesson planning ideas and scaffolds	Full names of pupils or staff
Newsletter drafting & editing	Home addresses or contact details
Suggested wording for generic policies (staff must review and edit all AI-generated policy text before adoption; AI output does not constitute legal advice and must be checked against current statutory guidance before use)	Specific SEND or safeguarding concerns

Data analysis	Pupil Data even if anonymised, Photographs where faces/individuals are identifiable
---------------	--

Safeguarding

In alignment with Keeping Children Safe in Education (KCSIE) 2025, our school remains steadfast in its commitment to protecting our pupils in an evolving digital landscape. While we embrace AI to enhance learning and wellbeing, we recognise that its use must be governed by robust safeguarding frameworks. All staff are expected to use AI tools in strict accordance with this policy, our Safeguarding and Child Protection Policy and the updated Staff Code of Conduct, ensuring that professional boundaries are maintained and that no identifiable pupil data is ever entered into unauthorised generative AI platforms. For a detailed breakdown of our preventative measures, staff should refer to the Risk Assessment in Appendix 3, which outlines our protocols for mitigating risks.

When assessing any AI tool for use in the school, particularly any tool that will be accessible to pupils, staff must have regard to this policy and the DfE's Generative AI: Product Safety Standards, which set out the minimum capabilities and features that AI products should meet to be considered safe for use in educational settings, including standards on filtering, monitoring, data protection, cognitive development, emotional and social development, mental health, and manipulation.

Staff and governors should also be aware that certain generative AI services that allow users to share content or that search live websites fall within the scope of the Online Safety Act 2023, which requires providers to take proportionate steps to tackle illegal content and protect children from harmful content. Where the school uses or considers using any such service, compliance with the Act's requirements should form part of the tool assessment process.

The school will comply with the minimum age requirements of any AI tool used. Before granting pupils access to any AI system, staff must confirm the applicable minimum age limit and, where required, obtain parental consent. Any tool whose minimum age requirement exceeds the age of pupils in the school must not be made directly accessible to those pupils.

The school will not use, or permit pupils to use, any AI-powered application or online tool that purports to offer mental health support or therapeutic intervention, unless that tool has been regulated by the Medicines and Healthcare products Regulatory Authority (MHRA) and has been assessed as safe through a full Data Protection Impact Assessment (DPIA) process. The risks associated with unregulated AI mental health tools, including failure to identify disclosures or patterns indicating a safeguarding concern, are considered too significant to manage without regulatory oversight.

At the time this policy was last reviewed, the applicable version was KCSIE 2026. An updated version of KCSIE is anticipated annually and this policy will be reviewed and amended accordingly once any new version is published. In the interim, staff should continue to apply the most current version of KCSIE in force.

Beyond our internal operations, we believe that education is the most powerful tool for protection. We are committed to teaching our children how to navigate AI with discernment, helping them

understand both its creative potential and its inherent risks, such as misinformation and deepfakes. Recognising that safeguarding is a partnership, we will also host parent workshops to empower families with the knowledge they need to keep children safe with AI at home as well as add regular updates from ScreenSafe to the newsletters. By fostering a culture of transparency and vigilance, we ensure that our technological advancements always serve to uphold our vision of a safe, happy, and protected school family.

Transparency

Information about using AI will be openly communicated to staff, students, and parents or guardians upon approval of the policy by governors, the policy will be uploaded onto the website. Please see Appendix One and Appendix Two for acceptable uses of AI.

Concerns and feedback about AI use should be reported as follows:

- **Safeguarding concerns:** Any concern that a pupil has been harmed, is at risk of harm, or has made a disclosure, whether arising from or in connection with AI, must be dealt with immediately in accordance with the school's Safeguarding and Child Protection Policy and reported to the Designated Safeguarding Lead (DSL). Such concerns must be recorded on CPOMS as a safeguarding matter and are not governed by this policy alone.
- **Staff concerns about AI use:** Staff who have concerns about the misuse of AI by a colleague, contractor, or visitor should report these to the Headteacher.
- **Pupil concerns:** Where a pupil raises a concern about AI that does not engage safeguarding procedures, this should be reported to the class teacher, who will refer it to the Headteacher as appropriate.
- **General feedback:** Staff, pupils, and parents are encouraged to share feedback on AI-related matters. This should be directed to the class teacher or Headteacher and will be considered as part of the annual policy review.

CPOMS is a safeguarding case management system and must not be used to record general feedback or non-safeguarding AI concerns

In the spirit of our school family and the value of Koinonia, we ask that parents and carers model transparency in their own use of AI when communicating with the school, ensuring that the technology is used to support, rather than replace, genuine human connection.

We recognise that complex or sensitive matters are often best resolved through personal dialogue; therefore, in line with our Complaints Policy, we warmly encourage parents to come into school and speak directly with a member of staff to share their concerns if they find written communication a barrier. This face-to-face approach ensures that every voice is heard with the compassion and empathy that AI cannot replicate, helping us to reach a resolution that truly supports the wellbeing of the child and supports the family.

Data Privacy and Security

We will comply with all relevant data protection laws, including the UK GDPR and the Data Protection Act 2018, to safeguard the privacy of students and staff.

Staff should be aware that many web-based generative AI tools, including free consumer tools such as ChatGPT, Copilot, or public versions of Gemini, may store information entered into them and use it to train future versions of the model, thereby incurring a risk that data will be incorporated into later outputs. This is precisely why the school permits only the use of Google Gemini through the school's managed Google Workspace for Education accounts, which operate within an enterprise-grade closed environment. However, even within this environment, the re-identification and memorisation risks described below mean that no pupil or staff personal data should be entered under any circumstances.

Staff must not enter pupil or staff personal data into AI tools. This includes information that directly identifies an individual and information that could identify an individual when combined with other information. Even where information appears anonymised, staff must consider the risk of re-identification, particularly in small school communities or where details relate to SEND, safeguarding, behaviour, attendance, health or family circumstances.

Even when data is anonymised AI systems may re-identify individuals that were believed to be anonymised by linking information with other data sets, or information made available when it was trained. In addition, large language models including, Google Gemini, may 'memorise' sensitive or personal information contained within their training data sets and leak this private information during their operation.

Staff should therefore treat all models that have been trained on data about people as though they potentially contain personally identifiable data, and make security and risk-based decisions accordingly.

Staff wishing to use any teaching application or tool incorporating AI must follow the process below before the tool is used:

1. Submit a written request to the Headteacher identifying the tool, its intended use, and the categories of data that may be processed.
2. The Headteacher will consult with the DPO to determine whether a DPIA is required. Where there is any doubt, a DPIA will be completed.
3. The DPIA must be completed using the school's standard DPIA template and reviewed by the DPO before approval is given.
4. No personal data may be entered into any AI tool until the Headteacher has confirmed approval and the DPO has signed off the DPIA.

Staff who use an unapproved AI tool in a manner that involves personal data will be in breach of this policy and may be subject to disciplinary action. Any suspected data breach arising from AI use must be reported to the Headteacher and DPO immediately, a failure to do so may also be the subject of disciplinary action.

The Headteacher will maintain a central record of approved AI tools and uses. The record should include the tool name, intended purpose, approved users, data categories, outcome of any DPIA or data protection assessment, product safety assessment, filtering and monitoring considerations, approval date, review date, and any restrictions on use. This record will support governance oversight, complaints handling, data protection accountability and review by governors.

Data Accuracy and Bias Mitigation

Generative AI tools choose words from a series of options and classify them as plausible based on probabilities. Although the outputs can appear credible and convincing, they may derive their answers from sources staff would not normally trust during their work.

Staff will review AI-generated content to ensure its accuracy if it is intended for further education or employment purposes. Staff will always treat the outputs with caution and apply their own judgment and knowledge. All facts and assertions should be cross-checked, no matter how authoritatively they appear to be presented. In cases where the information lacks verification from a trusted and reliable source, the information should not be included.

AI systems can also perpetuate biases present in their training data. We will actively work to identify and mitigate biases in any AI systems used.

Copyright

Outputs from AI chatbots could potentially include text that would constitute plagiarism. This is because some outputs may replicate, mimic, or closely resemble existing copyrighted material.

Staff should also be aware of the risk of secondary copyright infringement. This can arise where an AI tool has been trained on unlicensed material and outputs are then published or used in educational settings. Examples include publishing a school policy generated by AI that drew on another school's policy without permission, or using an AI-generated image on the school website where the underlying copyright owner has not consented. Staff should seek assurance from any AI tool provider that inputs are not used for model training without consent, and should not publish or distribute AI-generated content without satisfying themselves that there is no copyright risk.

Any intellectual property generated by staff using school-managed accounts for work purposes remains the property of St Paul's C of E Primary School.

Student Use of AI & E-Safety

In line with our E-Safety Policy, we empower our pupils to become "Digital Detectives" within an increasingly complex online landscape. While AI is a fascinating tool for creativity and learning, we teach children that it is not always a source of truth.

Through age-appropriate lessons, pupils develop the critical thinking skills needed to identify "hallucinations" or "deepfakes"-content that looks realistic but may be inaccurate or intentionally misleading. Our curriculum ensures students learn to:

- **Evaluate & Verify:** Move beyond the first answer by spotting bias and checking the accuracy of AI outputs.
- **Respect Integrity:** Understand intellectual property and the importance of avoiding plagiarism.
- **Navigate Safely:** Apply the "Stop, Think, Check" rule. If something feels "off" or uncomfortable, students are encouraged to pause and speak to a trusted adult immediately.

We foster a culture where no question is too small and no worry is too silly. This is a team effort; we ensure all AI tools used in school are age-appropriate and strictly aligned with our safeguarding protocols. To support this partnership, we have offered workshops for parents and carers from Screensafe, ensuring our families stay informed as technology evolves. Together, we help our children remain confident, resilient, and, most importantly, protected.

The school recognizes that major search engines (such as Google) now feature integrated, automated AI tools (e.g., AI Overviews) that generate content automatically during standard internet research.

- **Student Guidance:** Pupils are explicitly taught that these automated summaries are not always reliable. They will be regularly reminded not to trust or copy this information blindly and to cross-reference facts using verified, reliable sources.
- **Staff Oversight:** Staff will actively monitor research sessions to ensure pupils are critically evaluating search engine outputs rather than accepting AI-generated text as fact.

Pupil Use of AI. School Position

The school does not permit pupils to use generative AI tools directly. This applies in all settings, including during lessons, for homework, and for any assessed work. This decision reflects both the safeguarding risks associated with pupil-facing AI and the cognitive development concerns set out in this policy.

The only exception is structured online safety education, where pupils may be shown examples of AI outputs by a member of staff for the purpose of developing critical digital literacy, for example, to identify hallucinations, deepfakes, or AI-generated misinformation. In these sessions, the AI tool is operated solely by the supervising member of staff; pupils do not interact directly with any AI system.

Any proposal to permit wider direct pupil access to AI tools must be submitted in writing to the Headteacher and approved by the Full Governing Body before any access is granted. Such approval may only be given once the relevant tool has been assessed against the DfE Generative AI Product Safety Standards, a DPIA has been completed, the minimum age requirement has been confirmed, and parental consent has been obtained.

Some AI tools are designed, whether intentionally or otherwise, in ways that may encourage emotional attachment or dependence. AI tools that use human names, avatars, 'I-statements' or conversational behaviours that imply personhood or agency should be treated with particular caution when used with children.

AI tools will not be used to replace human social, emotional, or mental health support. Staff will explicitly teach pupils- particularly vulnerable learners- to understand the distinction between human interaction and algorithmic responses to prevent inappropriate emotional attachment to technology.

Inappropriate Use of AI

Inappropriate use of AI refers to actions that violate this policy, ethical standards, or legal regulations governing the responsible use of AI tools. Examples include breaches of copyright or

data protection laws, or the circulation of inaccurate information that could lead to reputational damage.

Other inappropriate uses involve deploying generative AI tools for unethical, illegal, or malicious activities. This includes using AI to create content which would harm or embarrass another individual. We will ensure that staff can provide feedback and report any concerns with AI usage.

AI must not be used to: decide or influence pupil behaviour sanctions or disciplinary actions; grade, mark, or assess pupil work; or make any judgements about a pupil's special educational needs. These decisions require professional human judgement and may never be delegated to or determined by an AI system. This applies both to Google Gemini and to any AI functionality embedded within third-party teaching platforms. These prohibitions should be read consistently with the equivalent prohibitions in Appendix One, which sets out additional detail on individual activities that staff are not permitted to use AI for.

We will ensure that staff understand that when using generative AI, they must comply with Acceptable Use Policies, Codes of Conduct, and relevant standards and ethics.

The Headteacher is responsible for monitoring updates to DfE and ICO guidance on AI and for bringing significant changes to the attention of the FGB. In addition to the review cycle set out in the metadata table at the front of this policy, the policy will be reviewed:

- following any significant incident involving AI use at the school;
- whenever the school considers approving a new AI tool for staff use; and
- whenever a proposal is made to extend pupil access beyond the limited online safety education context currently permitted.

The Headteacher is authorised to make interim updates between formal FGB reviews where required by changes in statutory guidance, with any such changes reported to the FGB at the next available meeting.

Sustainability

As we embrace these new technologies, we remain committed to our stewardship of the world around us, mindful of the environmental impact of AI. Our school vision for the future includes a responsibility to use digital tools sustainably, recognising that the significant energy and water resources required to power large AI models should be used with intention rather than habit.

To support this, we encourage staff to adopt a "purposeful use" approach which includes using AI where it adds genuine value to wellbeing and learning, while remaining conscious of the carbon footprint of digital tasks. By teaching our children about the intersection of technology and the environment, we help them become not just technologically capable, but also compassionate global citizens who understand how to balance innovation with the preservation of our planet for future generations.

Appendix One – Staff Acceptable Use

AI Staff Acceptable Use Overview

FGB Governor Approved 24.02.26

Using AI

Staff must ensure they follow the AI Policy for any work they produce with the assistance of AI or when using AI as part of their lessons.

Staff are authorised to use their official St Paul's Google Gemini educator accounts for general, non-personal-data tasks that support teaching, administration and communication, provided that all

outputs are reviewed by a member of staff before use and the use complies with this policy.

Staff are authorised to use their official St Paul's Google Gemini educator accounts for:

- generating ideas or resources for lessons.
- lesson planning.
- creating differentiated learning materials.
- policy or process writing.
- producing ideas and content for training and presentations.
- drafting **generic** administrative communications.
- drafting **generic** report statements

When producing work with the assistance of Google Gemini, staff should be mindful of the following:

- Staff must acknowledge the use of AI in their work. The way in which this is done depends on the nature of the output:
 - **Lesson resources and planning:** a brief note in the lesson plan or resource file confirming that AI was used in its preparation is sufficient.
 - **Communications to parents:** any letter, newsletter, or other communication drafted with AI assistance must be personally reviewed, edited, and approved by the responsible member of staff before it is sent. No disclosure to parents is required provided the content has been genuinely reviewed and reflects the member of staff's own professional judgement.
 - **Policy documents:** any policy drafted with AI assistance must be marked as 'AI-assisted draft' until it has been reviewed and formally approved through the school's policy approval process.
 - **Pupil-facing resources:** staff must satisfy themselves that any AI-assisted resource is accurate, age-appropriate, and free from bias before use. AI assistance need not be disclosed on the resource itself.

In all cases, the professional and legal responsibility for the accuracy and appropriateness of any AI-assisted output rests with the member of staff who uses and approves it.

- Any materials produced using AI should be checked for copyright infringement. Any third-party property should not be used without appropriate approval.
- Staff must be aware of biases and inaccuracies of AI. Any information produced by AI must be checked for accuracy.

- Staff must be mindful of the privacy of other staff members and students. Staff must not enter any information that would identify individuals or our organisation.
- Remember that AI should be used as a supportive tool, not a replacement for professional judgment.
- When using AI to translate materials for EAL pupils, staff must tailor the output to the pupil's literacy level. To prevent misleading translations, the output should be cross-checked by a fluent speaker where possible, or verified by 'reverse-translating' the text back into English.

Staff are not permitted to use any AI tool, including free consumer tools or the school's authorised platform, for personal data relating to pupils, staff, parents or other individuals; individual pupil or parent correspondence; decisions or recommendations about pupils or staff; SEND judgements; behaviour sanctions; disciplinary decisions; recruitment decisions; marking, grading or assessing pupil work; or any safeguarding, welfare or mental health judgement.

A number of teaching applications and tools incorporate AI and involve personal data. If staff wish to use any such applications or tools, they must first seek permission from the Headteacher and then together complete a Data Protection Impact Assessment (DPIA).

Staff will report any potential misuse or concerns about AI usage to the Headteacher.

Staff will only use approved AI platforms and adhere to this and all other related policies when using AI.

Appendix Two - Risk Assessment for AI Uses

AI Use	Details	Possible Risk	Risk Level	Possible Impacts	Impact Level	Risk Management Actions
Use of built in AI within teaching platforms	AI tools embedded in programmes	Personal information being shared or	Medium	Data privacy breaches	High	Ensure any programmes using AI have

	used to assist with data analysis or scaffolding learning	given access to.				undergone a thorough DPIA with the DPO.
Staff or student research or summarising tool	AI tools used to assist in research and summarise documents.	Bias in data sources or inaccuracies	Medium	Inaccurate and misleading data	Low	Staff to review any output generated from AI. Teach pupils to recognise AI inaccuracies.
Generating images	AI tools used to create visual content	Generation of inappropriate or biased images	Medium	Damage to reputation and supporting inaccuracies and deepfakes.	Medium	Educate users on responsible use of AI for image generations, including deep fakes and 'hallucinations' of the real thing
Generating written content	AI tools used to draft letters, correspondence from school, policies	Plagiarism or generation of low quality work that is potentially not aligned with school context/vision. Work not checked to ensure appropriate	Medium	Legal issues, errors distributed.	Medium	Ensure all output from AI is reviewed and checked.
Inputting third party content to edit/adapt	Inputting worksheets into AI tool to adapt resource	Copyright breach	Medium	Legal issues	High	Ensure Copyright is reviewed before images are placed into an AI tool.
Student Malpractice / Plagiarism	Students using Generative AI to complete independent work, homework, or assessments.	Submitting AI-generated work as their own original output.	Medium	Compromised student assessment accuracy; loss of independent learning skills.	High	Teach pupils academic integrity and how to be "Digital Detectives". Staff trained to recognize AI markers. Report incidents to Headteacher

						.
Loss of Teacher Personalisation	Over-reliance on AI for drafting communications or student report statements.	Generic, automated, or impersonal outputs that do not reflect the teacher's authentic knowledge of the child.	Low	Weakened parental engagement ; erosion of the school's "Family/Koinonia" core values.	Medium	Maintain the "creative partner" rule. Forbid fully automated student reports. Require all final outputs to be manually customized and personalised by staff
Pupil safeguarding disclosure made to AI tool	A pupil discloses a safeguarding concern to an AI chatbot rather than to a member of staff	AI tool fails to alert the DSL or does not route the disclosure appropriately	High	Safeguarding failure; child left at risk	High	Only ever permit pupils to interact with AI under direct staff supervision in the very limited online safety education context permitted by this policy. Ensure DSL training covers AI-related disclosure scenarios. No unsupervised pupil access to any AI chatbot
Emotional dependence by vulnerable pupils	A pupil forms emotional attachment to an AI chatbot	AI tool designed with human-like features that encourage attachment	High	Harm to emotional development ; reduced help-seeking from human sources; potential safeguarding disclosures missed	High	Maintain the school's position of not permitting direct pupil use of AI. Staff to teach pupils explicitly about the distinction between AI and human relationships

						. Do not use or permit any AI tool that anthropomorphises or implies emotions or personhood.
Sexualised deepfake images involving pupils	AI image generation tool used to create sexualised deepfake images of a pupil	Unmonitored access to AI image tools; pupil or external misuse	High	Serious safeguarding incident; potential criminal offence	High	No AI image generation tool to be permitted for pupil use under any circumstances. Online safety curriculum to include deepfake risk. Any incident to be reported to the DSL immediately. Apply DfE and UKCIS guidance on nudes and semi-nudes
History/audit trail deletion	Member of staff deletes Gemini activity history, removing evidence needed for a complaint or disciplinary investigation	Misunderstanding of school's instructions on data management	Medium	Inability to investigate complaint or disciplinary matter; potential data governance failure	High	Configure Google Workspace to manage retention centrally. Instruct staff in writing not to delete Gemini history manually. Headteacher to confirm retention settings with DPO annually

Appendix Three - DPIA Google Gemini

Data Protection Impact Assessment - Google Gemini

Data Controller: St Paul's CE Primary School

1.1 Explain the purpose of the project and what it aims to achieve.

The school proposes to use Google Gemini, an AI-powered educational platform, to support teaching and learning activities. Gemini provides AI tools that would assist/support teachers in creating educational content and resources.

1.2 What will the benefits be to the school or Trust, and to individuals such as pupils or parents?

- Reduced workload for staff
- Support pupils through scaffolded and adapted work following the creation of resources by the teachers.

1.3 Explain why a DPIA is necessary. Please refer to the DPIA screening checklist if you completed one.

A DPIA has been identified as necessary because:

The processing involves the use of new technology (AI-based tool)

The processing may involve personal data of children (pupils), who are considered vulnerable data subjects being entered accidentally. Staff have been advised not to enter any PI into Gemini, however it has been highlighted as a risk.

The school acts as data controller and needs to assess risks associated with using

a third-party processor

The processing involves automated decision-making or profiling through AI technology

There is a need to ensure compliance with UK GDPR and Data Protection Act

2018, particularly regarding children's data

Question	Response
Nature and scope of the processing	

2.1 Who are the data subjects?	Teachers, however no personal data will be inputted
2.2 How many data subjects will be affected by this project?	All teachers/TA's/Admin will have access
2.3 What personal information will be processed?	☐ Name ☐ Contact details ☐ Date of birth ☐ Gender ☐ Visual images ☐ ID numbers ☐ Online identifiers ☐ Location data ☐ Pupil premium status ☐ Free school meal status ☐ Looked after status ☐ Attendance data ☐ Attainment data ☐ EAL data ☒ Other – list below: No personal information, randomised on anonymised data may be inputted.
2.4 What special category data will be processed?	☐ Sex life or sexual orientation ☐ Religion or philosophical beliefs ☐ Political opinions ☐ Trade Union membership ☐ Race or ethnic origin ☐ Physical or mental health data ☐ Biometric data ☐ Criminal convictions or offences
Lawfulness of processing	

2.5 What is the Article 6 lawful basis for processing personal information?	☐ (a) Consent ☐ (b) Contract ☐ (c) Legal obligation ☐ (d) Vital interests ☒ (e) Public task ☐ (ea) Recognised legitimate interest ☐ (f) Legitimate interest Provide details:
2.6 What is the Article 9 lawful basis for processing special category information?	☐ (a) Explicit consent ☐ (b) Employment, social security or social protection ☐ (c) Vital interests ☐ (d) Not-for-profit bodies ☐ (e) Made public by the data subject ☐ (f) Legal claims or judicial acts ☐ (g) Substantial public interest ☐ (h) Health or social care ☐ (i) Public health ☐ (j) Archiving, research and statistics Provide details: Schedule 1 condition(s):

Question	Response	Risk
Lawfulness, fairness and transparency		
3.1 If relying on consent, how are you collecting this?	☒ Not applicable Or provide details:	☐

3.2 If relying on consent, what is the process to allow individuals to withdraw their consent?	☒ Not applicable Or provide details:	☐
3.3 If relying on legitimate interests, what was the outcome of the legitimate interest assessment (LIA)?	☒ Not applicable Or provide details:	☐
3.4 How will you inform individuals about the processing?	Refer to the school's AI Policy	☐
Necessity and proportionality		
3.5 How long will the personal data be held?	Data will be held as long as necessary, however no personal data will be held.	☐
3.6 How will you ensure you are only processing information necessary and proportionate for this specific purpose?	N/A No personal information used	☐
3.7 How will you prevent function creep?	Ensuring staff follow the AI Code of Conduct and regular reminders to staff.	☐
3.8 How will you ensure the personal information is kept accurate and up-to-date?	N/A. In the event of data/statistic used, ensure only most recent data used.	☐
3.9 How will you manage individual rights requests?	No personal/identifiable data will be input.	☐
Integrity and confidentiality		

3.10 Where will the personal data be stored?	Electronic systems: ☐ Internal system ☒ Cloud-based application or server Hard copies: ☐ Internal secure storage ☐ External secure storage ☐ Other – provide details:	☐
3.11 Who will have access to the personal information within the school or Trust?	Anybody with an @stpaulsprimaryyork account. No students will have access.	☐
3.12 What security controls are in place to protect and limit access to the information?	Password protected accounts	☐
3.13 How will you securely destroy the records when required?	Records kept as long as necessary but can be deleted if a record is found to need immediate deletion.	☐
3.14 What training will staff be undertaking to use the new system or process?	Staff have completed/signed an AI code of conduct.	☐
3.15 Is there an audit trail function so access to personal information can be monitored?	☐ Yes ☒ No Not applicable, only person areas.	☐
3.16 Does the system allow you to amend and delete information as necessary?	☒ Yes ☐ No	☐

--	--	--

Question	Response	Risk
Sharing with other data controllers		
4.1 If sharing data with another controller, what is the lawful basis for sharing?	Provide Article 6 lawful basis: N/A Provide Article 9 lawful basis: N/A Provide Schedule 1 condition, if applicable: ☒ Not applicable	☐
4.2 Is there an Information Sharing Agreement (ISA) or other sharing protocol in place with the controller?	☐ Yes Provide details: ☐ No ☒ Not applicable	☐
Sharing with data processors		
4.3 If using a data processor, do you have a written contract in place with them?	☐ Not applicable Contract in place: ☒ Yes ☐ No	☐

<p>4.4 Are there any known risks associated with this data processor?</p>	<p>☐ Yes Provide details:</p> <p>☒ No</p> <p>☐ Not applicable</p>	<p>☐</p>
<p>4.5 What is the outcome of the review of the contract to check it includes the mandatory data processing clauses?</p>	<p>Contract assurance rating: Full assurance</p> <p>Provide details:</p> <p>☐ Not applicable</p>	<p>☐</p>
<p>4.6 Has the processor provided information regarding their security measures?</p>	<p>☒ Yes Provide details:</p> <p>☐ No</p> <p>☐ Not applicable</p>	<p>☐</p>
<p>International transfers</p>		
<p>4.7 If transferring data to another controller or processor, where are they based?</p>	<p>☐ UK</p> <p>☐ EU</p> <p>☒ Other, provide details: Google is global</p> <p>☐ Not applicable</p>	<p>☐</p>

<p>4.8 If transferring data outside of the UK, what appropriate safeguards are in place for the transfer?</p>	<p>☐ Transfers approved by regulations</p> <p>☐ Data Privacy Framework</p> <p>☒ 2021 EU SCCs & UK Addendum</p> <p>☐ International Data Transfer Agreement (IDTA)</p> <p>☐ Binding Corporate Rules (BCRs)</p> <p>☐ Other, provide details:</p> <p>☐ Not applicable</p>	<p>☐</p>
<p>4.9 If transferring data outside of the UK and EU, has a Transfer Risk Assessment (TRA) been completed?</p>	<p>☐ Yes</p> <p>Provide TRA outcome:</p> <p>☐ No</p> <p>☒ Not applicable</p>	<p>☐</p>
<p>4.10 What are the arrangements of the server provision?</p>	<p>☐ Controller or processor's own servers</p> <p>☐ AWS</p> <p>☒ Google</p> <p>☐ Microsoft</p> <p>☐ Other, provide details:</p> <p>☐ Unknown</p>	<p>☐</p>
<p>4.11 In which country are the servers that hold the data?</p>	<p>☐ UK</p> <p>☐ EU</p> <p>☒ Other, provide details: Global</p>	<p>☐</p>

4.12 What is Veritau's assessment of the international transfer arrangements?	Compliance rating: Fully compliant ☐ Not applicable	☐
---	---	--------------------------

Question	Response	Risk
Context of the processing		
5.1 Is the personal data being provided by a third party rather than collected directly from the data subject?	☐ Yes Provide details: ☒ No	☐
5.2 Are you going to use information you already hold about individuals for a purpose it is not currently used for?	☐ Yes Provide details: ☒ No	☐
5.3 Would individuals expect you to use their personal information in this way?	☐ Yes Provide details: ☒ No Not using Personal Information	☐
5.4 Are there any prior concerns over this type of processing?	☒ Yes Provide details: There is a risk of inputting PI into AI so needs to be monitored closely. ☐ No	☐

5.5 Will the processing involve any automated decision-making (ADM), including profiling?	☐ Yes Provide details: ☒ No	☐
5.6 If ADM will be used, what process is in place to ensure data subjects can request human review of the decision?	☒ Not applicable Or provide details:	☐
5.7 Does the processing involve any data matching?	☐ Yes Provide details: ☒ No	☐
Biometric data		
5.8 If collecting biometric data, please confirm that the consent process is compliant with government guidance?	☐ Yes ☐ No Provide details: ☒ Not applicable	☐
5.9 What alternative arrangements are being offered where consent has been withheld?	☒ Not applicable Or provide details:	☐
Surveillance		
5.10 If the system involves CCTV, what signage is in place?	☒ Not applicable Or provide details:	☐

5.11 If the system involves e-monitoring, how are individuals informed when they log on to the system that they are being monitored?	☐ Not applicable Or provide details:	☐
5.12 Does the project involve any other type of surveillance?	☐ Yes Provide details: ☐ No ☒ Not applicable	☐
5.13 Have you provided meaningful information about the functionality of the surveillance system?	☒ Not applicable Or provide details:	☐
Artificial intelligence (AI)		
5.14 Identify and describe the AI processes involved.	☐ Not applicable Or provide details: Google Gemini will be used to support staff within their roles, including admin, lessons, adapted work.	☐
5.15 Identify the stages and degree of human intervention or review.	☐ Not applicable Or provide details: Ensuring teachers check that they have not included any PI.	☐

5.16 Is any information available about the accuracy or margin of error in the AI system, which could result in unfair outputs?	☐ Not applicable ☐ No information available Or provide details: Ensuring teachers check any outputs for bias and accuracy	☐
5.17 Is any information available about potential bias in the AI system, which could result in unfair outputs?	☐ Not applicable ☐ No information available Or provide details: Ensuring teachers check any outputs for bias and accuracy	☐
5.18 If bias or inaccuracy is present in the AI system, what impact does this have on individuals?	☐ Not applicable Or provide details: No personal data will be used but there is chance of inaccurate learning resources being made.	☐
5.19 Would individuals reasonably expect AI to be used this way?	☒ Yes ☐ No ☐ Not applicable Provide details:	☐
5.20 How are you explaining to individuals the logic behind the decisions made by the AI?	☐ Not applicable Or provide details: Refer to AI Policy	☐

5.21 Why is it necessary and proportionate to use AI for this processing?	☐ Not applicable Or provide details: Takes away some time/stress for staff to complete their role.	☐
Other technologies		
5.22 Will you be using any other novel technology not listed above?	☐ Yes Provide details: ☒ No	☐
Other risks		
5.23 Are there any other risks you have identified with this project?	☐ Yes Provide details: ☒ No	☐
5.24 If you are using an Information Society Service, are you satisfied that it complies with the Information Commission's age appropriate design: a code of practice for online services?	☒ Not applicable ☐ Yes Provide details: ☐ No	☐

Part 6: Accountability			
6.1 As a result of this project do you need to update any of the following?	☐	Information Asset Register	☐
	☐	Data Processor Register	
	☒	Policies	
	☒	Procedures	

6.2 If needed, have you consulted relevant stakeholders and/or the Information Commission? What was the outcome?	☐ Yes Who did you consult? Please add outcome details: ☒ No	☐
---	---	--------------------------

Identified risk	Rating	Measures to reduce or eliminate risk	Residual risk	Outcome	Responsible individual	Date complete
R3.6 It is unclear how it will be ensured that only information necessary for this specific purpose will be processed.	Medium	A process will be implemented to ensure no person data will be shared with Google Gemini	Low	Reduced		
R5.15 It has not been identified the stages and degree of human	Low	Due to the nature of the processing and types of data involved, the risk to data	Low	Accepted		

interventi on or review in the AI process.		subjects is low.				
R5.16 There is no informati on available about the accuracy or margin of error in the AI system, which could result in unfair outputs.	Low	Due to the nature of the processing and types of data involved, the risk to data subjects is low.	Low	Accepted		
R5.17 There is no informati on available about potential bias in the AI system, which could result in	Low	Due to the nature of the processing and types of data involved, the risk to data subjects is low.	Low	Accepted		

unfair outputs.						
R6.1 The AI Policy has not been updated to cover this processing.	Medium	The AI Policy will be updated as necessary.	None	Eliminated		

Internal	
SPOC:	
Name:	
Job title:	
Email:	
SIRO:	
Name:	
Job title:	
Email:	
IAO:	
Name:	
Job title:	
Email:	
External	
Data Processor(s)	
Name:	
Contact details:	
Data Controller(s)	
Name:	
Contact details:	
Data Protection Officer	
Name:	Veritau Limited

Contact details:	West Offices, Station Rise, York, North Yorkshire, YO1 6GA schoolsdp@veritau.co.uk / 01904 554025
-------------------------	--

Item	Name/date
Measures and actions approved by:	
Residual risks approved by:	
Summary of DPO advice:	
DPO advice given on:	
DPO advice accepted or overruled by:	
Comments:	
This DPIA will be kept under review by:	
Date of next planned review:	