



Bristol Drive

Lincoln

LN6 7UE

Artificial Intelligence (AI) Policy

October 2025

Policy Owner	Data Protection Officer (DPO)
Version Number	V1.0
Governing Body Committee	Resources Committee
Date Approved by Governors	22 nd October 2025
Next Review Date	October 2026

Contents

Contents	Page 2
Introduction	Page 3
Scope	Page 3
Guiding Principles	Page 3
Roles and Responsibilities	Page 3
AI in Teaching and Learning	Page 3
Transparency	Page 3
Safeguarding and Compliance	Page 4
Data Privacy and Security	Page 4
Web-based vs Non-public Generative AI Tools in School Context	Page 4
Data Accuracy and Bias Mitigation Generative	Page 5
Copyright	Page 5
Student Use of AI	Page 5
Inappropriate Use of AI	Page 5
Monitoring and Review	Page 5
Appendix 1: Guide to the use of AI	Page 6

Introduction

This policy outlines the responsible, ethical, and safe use of Artificial Intelligence (AI) technologies within Sir Francis Hill Primary School. It reflects the latest guidance from the Department for Education (DfE), including the use of generative AI tools, and aligns with safeguarding, data protection, and educational standards. The school recommends the use of non-public AI services such as Microsoft Copilot due to its integration with the school's Microsoft staff accounts and data security.

Scope

This policy applies to all staff, students, volunteers, and contractors who interact with AI technologies in the school setting. It covers AI use in teaching, learning, administration, and communication.

Guiding Principles

- Human Oversight: AI is a supportive tool, not a replacement for professional judgement.
- Transparency: All AI use must be clearly acknowledged.
- Safeguarding: AI must not be used to create, share, or engage with harmful, discriminatory, or misleading content.
- Data Protection: The use of AI tools within school must be in line with the school's Data Protection Policy and relevant Data Protection legislation
- Academic Integrity: AI-generated content must be cited appropriately and not used to replace student work.

Roles and Responsibilities

Overall responsibility for this policy lies with the school's Data Protection Officer and Senior Leadership Team, 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 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.

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

AI in Teaching and Learning

- AI may be used to support lesson planning, resource creation, and differentiation.
- Students may use AI for research, concept exploration, and skill development.
- AI must not be used in assessments unless explicitly authorised by the school's Senior Leadership Team.
- All AI tools must be risk assessed.

Transparency

Information about using AI will be openly communicated to staff, students, and parents or carers. We will ensure procedures are in place for reporting and addressing concerns related to AI usage. Teachers, students, and parents will be encouraged to provide feedback on their experiences, possible areas of improvement, and any issues with the generative AI tools used.

Safeguarding and Compliance

- Deepfake creation, nudification apps, and covert recording using AI are strictly prohibited.
- Wearable AI devices are banned unless authorised by the Senior Leadership Team for accessibility purposes.
- Staff should not use new AI tools which the school hasn't authorised for use within school, without seeking guidance from the school's Data Protection Officer and Senior Leadership Team.
- Any misuse of AI will be treated under the school's Behaviour and Safeguarding Policies.

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.

Web-based vs Non-public Generative AI Tools in School Context

Web-based generative AI tools (e.g., ChatGPT, Bard, Copilot via public web access) are publicly available and hosted by third-party providers. These tools often retain user inputs to improve future versions of the model.

Staff Guidance: Any information entered into web-based generative AI tools may be stored and used to train future versions, which poses a risk that sensitive data could be incorporated into future outputs. Staff must ensure that any data input into free or public generative AI applications is fully anonymised, and must not include names of individuals, groups, or organisations, or any information that could reasonably be used to identify such individuals.

Non-public Generative AI Tools (Including Microsoft Copilot accessed via staff Microsoft account)

Non-public generative AI tools are those accessed within secure, school-managed environments. These include AI systems hosted locally or provided under strict data protection agreements.

A key example is:

Microsoft Copilot, when accessed via a staff Microsoft account within the school's secure Microsoft 365 environment, is considered a non-public AI tool. This version of Copilot operates within the school's data governance framework and does not share data externally for training public models.

Use of Non-public AI Tools for Reports and Documents

Staff may use non-public AI tools such as Microsoft Copilot to assist in drafting reports, documents, or communications that include personal data (e.g. pupil reports, safeguarding notes, internal communications).

However, the following principles must be followed:

- Only include the minimum necessary personal data required for the task.
- Ensure the AI tool is accessed via the school's secure system (e.g., logged in with a staff Microsoft account or a password protected AI account).
- Review all AI-generated content carefully before sharing or storing.
- Do not use non-public AI tools for tasks involving sensitive data unless the tool is approved by the school and compliant with data protection regulations (e.g., UK GDPR).

These tools can support efficiency and consistency, but staff remain responsible for ensuring accuracy, appropriateness, and data security.

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.

To mitigate any legal risks, staff should always review AI-generated material for potential copyright infringement. AI-generated material should also be customised and modified to guarantee it is sufficiently distinct from any existing copyrighted works it draws upon.

Student Use of AI

Students will learn to use AI tools responsibly and think critically about them. They will be taught to respect intellectual property, avoid plagiarism, spot bias in AI outputs, and check the accuracy of AI-generated information. This will be part of their digital literacy education, helping prepare them for future careers where AI is widely used. AI tools should be age-appropriate and align with our safeguarding policies.

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 report any concerns with AI usage.

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

We will ensure we comply with DfE and ICO guidance on using AI, regularly review legislation and best practices, and update this policy as necessary.

Monitoring and Review

Governors will review the AI Policy, and DPIAs will be reviewed annually or sooner if required.

Guide to the Use of AI Staff Guidance

This guide supports staff in using Artificial Intelligence (AI) tools responsibly, safely, and effectively within Sir Francis Hill Primary School. It outlines best practices, approved tools, and key considerations for day-to-day use.

Approved AI Tools

Staff must only use AI tools that are:

- Approved by the Senior Leadership Team (SLT)
- Logged in the school's Information Asset Register
- Accessed via secure school accounts (e.g., Microsoft Copilot via staff Microsoft 365 login)

Examples of approved tools:

- Microsoft Copilot (via school account)
- AI features embedded in Microsoft 365 (Word, Excel, PowerPoint)
- Other tools explicitly authorised by SLT and DPO

Permitted Uses of AI

Staff may use AI to:

- Draft lesson plans, worksheets, and differentiated resources
- Generate ideas for classroom activities
- Support administrative tasks (e.g., report writing, internal communications)
- Translate or summarise non-sensitive content
- Explore curriculum topics for professional development

Prohibited or Restricted Uses

Staff must not:

- Input personal, sensitive, or identifiable data into public AI tools (e.g., ChatGPT, Bard)
- Use AI to generate safeguarding reports or sensitive communications unless explicitly authorised
- Rely solely on AI for decision-making or professional judgement

Data Protection and Privacy

- Staff should not use new AI tools which the school hasn't authorised for use within school
- Use only the minimum necessary data when working with AI
- Ensure outputs are reviewed and edited before sharing or storing
- Do not use AI tools for tasks involving sensitive data unless the tool is compliant with UK GDPR and approved by the school

Accuracy and Bias

- Treat AI outputs as drafts, not final products
- Cross-check facts and sources before using AI-generated content
- Be aware of potential bias in AI outputs and avoid reinforcing stereotypes
- Avoid using AI to generate content for external publication without SLT review

Copyright and Plagiarism

- Review AI-generated content for potential copyright infringement
- Modify and personalise outputs to ensure originality
- Cite sources where appropriate and avoid replicating existing works

Professional Conduct

- Follow the school's Acceptable Use Policy and Code of Conduct
- Report any misuse or concerns to the DPO or SLT
- Engage in ongoing training and CPD related to AI use
- Encourage open dialogue with colleagues about AI experiences and best practices