Hawridge & Cholesbury CE School

AI - Artificial Intelligence Policy

Our Vision is for every child within the Hawridge & Cholesbury family to grow, flourish 'have life and … have it more abundantly' (John 10:10 KLV); to be fascinated, rounded, eager to make a difference, spiritual and have high aspirations through Jesus' teaching and our curriculum.

We live our vision through our natural setting and our school values:

Respect Teamwork Responsibility Understanding Peace Honesty

Adopted by the governing body on: 25 February 2026

Next review January 2027

1. Introduction & Aims

This policy provides the framework for safe, responsible and ethical use of Artificial Intelligence (AI) at Hawridge and Cholesbury CE School. We recognise that AI tools can support teachers, reduce workload and enhance learning. They can also produce inaccurate or inappropriate content and raise safeguarding, data protection, and integrity issues.

Our aims are to:

- Have robust processes in place to ensure the safe use of AI when used by pupils, staff, volunteers and governors.
- Teach pupils, in an age-appropriate way about how to use AI safely, ensuring pupils are aware of risks.
- Protect children from risks and uphold safeguarding responsibilities such as: misinformation, disinformation and deep fakes.
- Work alongside parents to ensure they understand both the opportunities and risks of AI.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) guidance for using Artificial Intelligence (AI) : Using AI in Education

It is also based on the statutory safeguarding guidance, Keeping Children Safe in Education (KICSE), and its advice for schools on Teaching online safety in schools as well as misinformation, disinformation and deep fakes.

The policy also takes into account the National Curriculum Computing programme of study which is taught through the National Centre for Computing Education (NCCE).

3. Roles and Responsibilities

The Governing Body

- The governing body has overall responsibility for monitoring this policy and holding the Headteacher accountable for its implementation.
- The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, monitoring online safety logs as provided by the designated safeguarding lead (DSL).
- The governing body should ensure children are taught how to keep themselves and others safe online as well as the misuse of AI.
- The governing body must ensure the school has appropriate systems in place on school devices and school networks and will regularly review their effectiveness.
- The school's filtering and monitoring systems are provided by the LGfL trust, which regularly update and provide guidance on the use of their systems.
- The governor who oversees online safety is the Child Protection Governor.
- All governors will: Ensure they have read and understand this policy.

The Headteacher & Senior Leaders

The Headteacher and Senior Leaders are responsible for ensuring that all staff understand the policy and consistently adhere to it across the school.

The designated safeguarding lead (DSL)

- Details of the school's designated safeguarding leads (DSLs) are set out in our child protection policy, as well as relevant job descriptions.
- The DSL takes lead responsibility for online safety in school.
- Work with the Headteacher, Computing Subject Leader and other staff, as necessary, to address any online safety issues or incidents
- Ensure that any online safety incidents are logged (see CP chronologies, Teams DSL) and dealt with appropriately in line with this policy, recording all incidents in CPOMS.
- Provide updates on reports on online safety and the use of AI in school to the Headteacher and/or governing body.
- Provide regular safeguarding and child protection updates, including online safety/AI risks, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

The School's External Support Organisations

The school's Education Focused ISP (LGfL) is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material. This can also include websites containing misinformation, disinformation and deep fake materials.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Periodically conducting a full security check and monitoring the school's firewall and internet connectivity systems.

The school's IT support provider (Wibird)

Wibird is responsible for:

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Working with the school to identify risks and implement updates to the school's systems.
- Taking proactive steps to protect the school's systems against the risk of malware.
- Providing the leadership team with advice and recommendations to ensure the safe use of computing at the school.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy, with specific note of the guidance and use of AI in a professional capacity.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (see the school online policy), and ensuring that pupils follow the school's terms on acceptable use (see school online policy)
- Working with the DSL to ensure that any online safety incidents are logged (see CPOMS & Excel CP chronologies in DSL folder on Teams) and dealt with appropriately in line with this policy
- Following the correct procedures by seeking permission from the Headteacher if they need to bypass the filtering and monitoring systems for educational purposes.

Subject Leader

- Subject leader/s will make sure all staff undergo Artificial Intelligence (AI) training as part of Safeguarding ensuring staff understand their roles and responsibilities around using AI safely.

Parents/Carers:

Parents are expected to;

- Supervise their child's use of AI tools and ensure they do not share personal information such as names, locations, or photos when using online AI platforms.
- Ensure their child only uses age-appropriate and school-approved AI tools, supporting responsible and safe technology use.
- Help their child understand that AI responses may not always be accurate and encourage them to verify information using trusted sources.
- Guide their child to use AI ethically, ensuring it supports learning rather than completing work on their behalf, and reinforcing expectations about academic integrity.

4. Data Protection and Cyber-Security

At Hawridge and Cholesbury CE School we recognise the potential benefits of Artificial Intelligence (AI) in enhancing teaching, learning, and operational efficiency. However, it is essential that all staff and school stakeholders use AI tools in a responsible, safe, and ethical manner that protects pupils, staff, families, and the school community.

- **No personal or sensitive data about pupils, staff, or families will be entered into AI tools.**

Staff and stakeholders must take all reasonable precautions to ensure that any information entered into AI systems does not include names, addresses, contact details, images, or other personal or sensitive data. Protecting confidentiality and maintaining the privacy of the school community is a non-negotiable requirement.

- **Any use of AI must comply with the school's Data Protection Policy**

All AI use must adhere to statutory obligations, including GDPR and the school's internal data protection procedures and online safety policy.

- **Staff must be alert to cyber-security risks such as AI-generated scams.**

  AI technologies can introduce new risks, including fraudulent or misleading content, phishing, and other forms of cyber threats. Staff must remain vigilant, critically evaluate AI outputs, and follow school guidance to mitigate potential risks to the school's systems and the wider school community.

- **Pupils' work will not be used to train AI tools.**

  Staff must ensure that students' work, data, or submissions are never input into AI systems for the purposes of training or improving external AI models. Protecting pupils' intellectual property and personal contributions is central to maintaining trust and ethical practice.

All staff and stakeholders are expected to act as positive role models, demonstrating responsible and safe use of AI, and to support pupils in understanding the benefits, limitations, and risks of AI technologies.

5. <u>Guidance and the use of Artificial Intelligence (AI) Tools</u>

<u>Guidance to the use of AI:</u>

All staff and pupils at Hawridge and Cholesbury CE School must be aware that AI systems have limitations and risks. All stakeholders should follow the guidance below in order to adhere to the Government advice for the use of AI in schools. At Hawridge and Cholesbury we adopt the model 'FACTs' as outlined in the recent guidance. (appendix 1).

- AI can produce inaccurate, biased, or inappropriate content.
- Outputs generated by AI tools may not always be correct or suitable.
- Staff and pupils must critically evaluate content before using it for learning, communication, or decision-making.
- Verification with trusted sources or professional judgement is essential when using AI.
- AI should never be relied upon as the sole source of information or guidance.
- AI cannot replace human judgement or subject knowledge.
- It is used as a support tool, not a substitute for professional expertise, critical thinking, or the teacher-pupil relationship.
- Staff remain responsible for teaching decisions, safeguarding, and ensuring high-quality learning experiences.

<u>Artificial Intelligence (AI) Tools:</u>

AI may be used at Hawridge and Cholesbury CE School in carefully controlled and approved ways to support learning and school operations, while always maintaining high standards of safeguarding, professional practice, and ethical use.

- AI may be used to assist staff with drafting resources, lesson planning, or reducing administrative tasks, enabling educators to focus on teaching, pastoral care and pupil engagement. If teaching staff use AI to support with tasks listed above, they should

consider how this is presented to the children so that it is shared in an appropriate format and not necessarily just copied from the AI system.
- AI may be incorporated into lessons to provide pupils with practical, hands-on experience of emerging technologies, algorithms, and problem-solving tools. This will be taught as part of or in addition to the NCCE (National Centre for Computing Education) scheme.
- AI may be used to illustrate the role of technology in modern life, exploring both its benefits and potential challenges, and supporting pupils in becoming informed, responsible digital citizens.
- Children will be taught about plagiarism in an age-appropriate manner to teach them acceptable use of AI preparing them for work outside of school such as homework.

6. Risks and Misuse of Artifical Intelligence

Key risks identified around AI as stated in the Government Guidance for AI in schools: Using AI in Education

- Pupil or student exposure to inappropriate or harmful content
- Pupil or student exposure to inaccurate, misleading or biased content
- Data protection breaches
- Intellectual property infringements (copyright)
- Academic integrity challenges

Misuse of AI:

Misuse of AI can compromise the safety, privacy, and well-being of pupils, staff, and the wider school community.

- **The school will restrict access where appropriate by** limiting or blocking access to AI tools if their use is deemed unsafe, inappropriate, or in violation of school policy.
- Staff will provide guidance and supervision to ensure that pupils use AI responsibly and safely during lessons or school activities.
- Any reported or observed misuse of AI will be taken seriously. The school will investigate incidents in accordance with safeguarding procedures and implement appropriate interventions or disciplinary measures.

7. Safeguarding and Artificial Intelligence (AI)

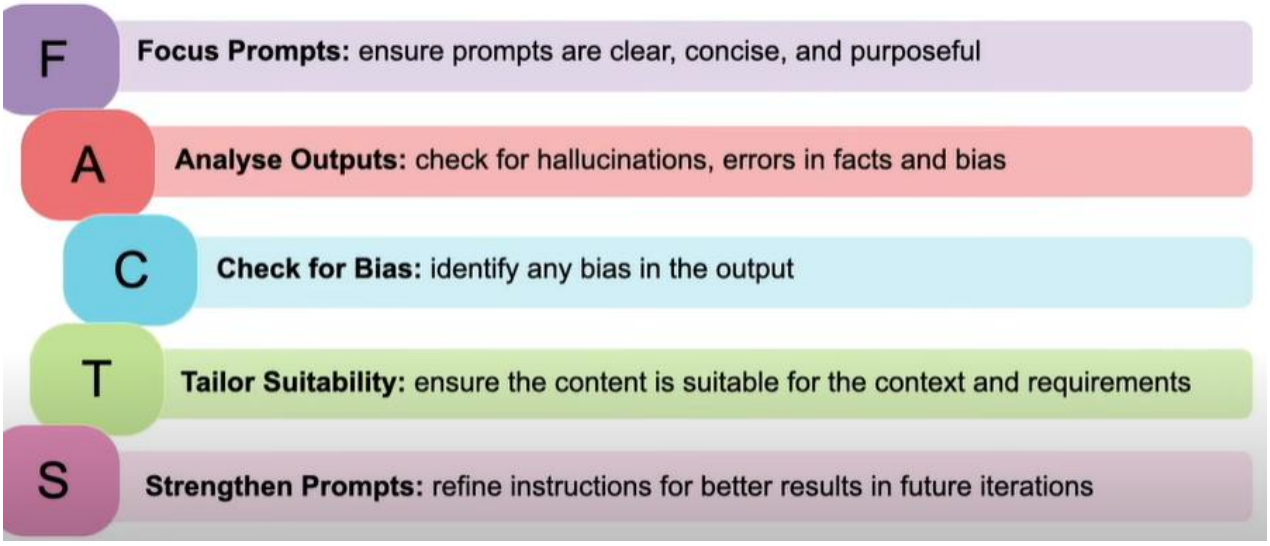
- Any harmful or inappropriate content generated through the use of AI will be treated as a safeguarding concern and managed in line with school safeguarding procedures.
- Staff will receive regular training to understand the risks associated with AI and how to support pupils in using AI safely and responsibly.
- Pupils will be taught about online safety as part of their Computing and PSHE lessons.
- Parents and carers will be provided with information about AI-related risks and supported in promoting safe and responsible AI use at home.
- Appropriate filtering and monitoring systems will be in place to manage and oversee pupil access to AI technologies.
- Pupils will be taught to critically evaluate digital media, understand how deep fakes are created, and seek help from a trusted adult if they encounter suspicious or potentially harmful content online.

8. Updates and Review

This policy will be reviewed annually or sooner if significant changes occur in AI technology. Updates will reflect current best practice, emerging risks, and developments in educational use of AI. When further guidance is shared, subject leaders will review and consider the safest, recommended AI systems to be used in schools.

Appendix 1: FACTS

The approach used by staff when using AI to support teaching and learning. This approach is taken directly from the guidance and advice given during training: The Use of AI in Education.



F **Focus Prompts:** ensure prompts are clear, concise, and purposeful

A **Analyse Outputs:** check for hallucinations, errors in facts and bias

C **Check for Bias:** identify any bias in the output

T **Tailor Suitability:** ensure the content is suitable for the context and requirements

S **Strengthen Prompts:** refine instructions for better results in future iterations