

Whole-School Approach to AI

Statement of intent

AI is everywhere, and it's becoming an increasingly important part of learning and education. Generative AI allows for the creation of new content, like written materials or images, based on vast amounts of existing data. This technology presents exciting opportunities for both staff and students at our school.

We recognise that AI has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload. This guidance outlines how we will use AI responsibly and effectively to improve teaching, learning, and school admin. It's about harnessing AI's potential while being aware of its evolving nature and associated risks of use. We 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 students about the 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 students will, as always, be at the forefront of our guidance and practice.

How do we want to use this guidance?

- To enhance academic outcomes and educational experiences for students
- To support teachers in managing their workload more efficiently and effectively
- To educate staff and students about safe, responsible and ethical AI use
- To incorporate AI as a teaching and learning tool to develop staff and students' AI literacy and skills
- To prepare staff and students for a future in which AI technology will be a major part
- To use AI to address learning gaps and provide personalised support to our disadvantaged students
- To improve and streamline school operations to minimise cost and maximise efficiency.

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. We may wish to consult the following:

- [AI Roadmap - GOV.UK](#)
- [National AI Strategy - GOV.UK](#)
- [Ofcom's 2024 Online Nation Report](#)
- [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
- [SWGfL – Artificial Intelligence and Online Safety](#)
- [Keeping Children Safe in Education 2026](#)

Areas to consider

1. Scope and Responsibilities
2. Use of AI by Staff
3. Use of AI by students
4. Potential Misuse of AI
5. Ethical Use of AI
6. Data Protection implications of using AI
7. Cyber security
8. Reporting
9. Restricting Access

1. Scope and Responsibilities

Headteacher and Senior Leaders

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Lead / Online Safety Lead

Our Designated Safeguarding Lead / Online Safety Lead 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.

Data Protection Officer

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).

IT support Staff

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

Staff

It is the responsibility of all staff to have read and understood this guidance and associated Acceptable Use Agreements. 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
- students understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and the potential benefits and risks of its use. They will 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, admin and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated.

Parents/carers

We will engage parents and carers by:

- Regular online safety sessions
- Sharing information in newsletters
- sharing information online e.g., website, social media
- providing curriculum information

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 children'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.

2. Use of AI by Staff

2.1 Permitted Use and Tools

Staff are able to explore and utilise AI-based tools and technologies to assist in managing their work. Examples of such tasks include:

- Administrative Tasks: Report writing, facilities management.
- Teaching Support: Lesson planning, gathering educational resources, creating extension or scaffolded tasks.
- Assessment: Marking, feedback, and analyzing pupil attainment data.
- Professional Development: Supporting personal training needs and opportunities.

Note: AI tools must complement staff professional judgment and expertise; they must not replace them.

Approved AI Tools

Staff are currently only permitted to use the following AI-based tools:

- Google Gemini
- TeachmateAI
- csuk.io

2.2 Professional Accountability and Transparency

Staff remain professionally responsible and accountable for the quality and content of any output generated by AI, however generated or used.

- Review and Verification: Staff must always review and verify AI-generated content (e.g., marks, reports, plans) to ensure accuracy, factual correctness, and alignment with their professional observations and expertise.
- Transparency: Where AI has been used as part of their work, staff will be clear where it has been used and what additional professional review or revision has been carried out.

2.3 Application in Teaching and Learning

Lesson Planning and Resource Creation

AI tools can assist teaching staff by:

- Gathering and creating relevant educational resources.
- Creating whole group or personalised lesson plans.
- Generating extension tasks or scaffolded work.
- Identifying potential knowledge gaps (e.g., through suggested topics or learning activities).

Teaching staff are permitted to use these suggestions as a starting point, incorporating their professional expertise to customise and adjust the materials to ensure pupil learning objectives are met.

Assessment and Feedback

AI can automate certain aspects of marking, particularly for objective or fact-based responses (e.g., multiple-choice or fill-in-the-blank assessments).

- Objective Marking: AI-powered software can speed up scoring, providing more time for individual pupil support.
- Subjective Feedback: For more subjective or open-ended written answers, teaching staff can use AI to identify areas for improvement, but they must review and verify all AI-generated marks or feedback, adding their professional judgment and deeper analysis.

Pupil Self-Assessment

Teaching staff can support students to gain feedback on their work using AI, replicating peer assessment processes. This allows students to receive instant, personalised feedback and improvement strategies.

- **Staff Role:** Teaching staff must play an integral role in this process, spot-checking the feedback provided to students, just as they would with traditional peer assessment.

Pupil Reporting and Progress Analysis

Staff can use AI to assist in writing pupil reports, ensuring accuracy and efficiency. Staff must always review and modify AI-generated reports to ensure they reflect their own observations, assessments, and personalised feedback.

In pupil progress analysis, AI can gather information and identify patterns, but staff must rely on their expertise to provide a comprehensive and holistic evaluation. Staff remain the key decision-makers in evaluating and providing feedback on students' academic achievements.

2.4 Training and Professional Development

Staff will receive appropriate training and support to effectively integrate AI into their work.

- **Focus:** Training will focus on approved AI tools and their effective integration into school administrative and teaching practices.
- **Planning:** Training will be planned as part of staff personal development reviews and appraisals or on an as-needed basis.
- **Staff Responsibility:** Staff have a responsibility to identify any training and development needs to ensure they adhere to this guidance and should discuss these with their line manager.

3. Use of AI by students

Students are currently blocked from using AI tools in school, see **10. Future Strategy**

4. Potential Misuse of AI

Students will be taught to use AI responsibly and ethically, understanding the risks and consequences of using AI tools to complete assignments, coursework, or homework entirely. (all students but specifically computing year 9 - before they start their GCSE's)

Staff will encourage students to be transparent, clearly stating when AI has assisted in their work.

Teaching staff will emphasise critical thinking, creativity, and originality in pupil work and the misuse of AI for plagiarism or academic dishonesty is strongly discouraged and will incur sanctions.

Clear guidelines on the appropriate use of AI tools during assessments will be provided to students, ensuring their work reflects their own efforts and understanding.

Key messages about AI use will be delivered through the Computing Curriculum (KS3) and reinforced in all subjects where students are completing work for external grading.

The school will comply with all rules and guidance from the Joint Council for Qualifications (JCQ) and individual Exam Boards regarding AI use in assessments. [JCQ guidance](#)

Teaching staff will use different assessment methods to evaluate pupil understanding and confirm genuine comprehension of the subject matter. These methods may include class discussions, oral presentations, practical demonstrations, written reflections, and project-based assessments. This approach helps verify pupil comprehension beyond what AI tools can assess, fostering deep learning and authentic engagement.

Teaching staff will educate students about the potential misuse of AI by individuals attempting to deceive or trick them into unintended actions, such as interacting with those who are not genuinely who they claim to be, but who use AI to imitate them.

5. Ethical Use of AI

The use of AI systems, especially Generative AI, must be approached with caution and an awareness of their limitations. Whether staff are using AI for teaching or school administrative purposes, or with students who will make use of this technology, they should be mindful of and instruct students about the following considerations:

- Data bias and information generated by AI will reflect any inherent biases in the data set accessed to produce it. This could include content which may be discriminatory based on factors such as race, gender, or socio-economic background.
- Information generated/provided may be inaccurate so any content should be fact-checked.
- Some AI models only collate data prior to a certain date so content generated may not reflect the most recent information. (Should we limit use to certain ones?)
- Content produced could be inappropriate or unsafe as AI technology can be used to generate harmful content, including deepfakes and impersonation materials. Deepfakes are synthetic media that can create realistic videos or audio of people saying or doing things they haven't, which can be used to spread misinformation.
- Any information entered into a Generative AI model is no longer private or secure. Personal, sensitive, or confidential data should not be entered into these tools. (See next section)
- AI content can infringe on intellectual property as you don't know if the material being used to train the model was given with permission.

6. Data Protection implications of using AI

Staff and students should be aware that any information entered into non-school approved Generative AI models is no longer private or secure.

Staff who wish to use AI tools must only use those that have been approved by the IT Support team by raising a ticket, who will only approve those tools that adhere to the school data and security requirements.

7. Cyber security

We will take appropriate measures to guarantee the technical robustness and safe functioning of AI technologies, including:

- Implementing cybersecurity protocols and access controls through measures such as encryption, security patches/updates and secure storage.
- Establishing procedures and controls around data practices, system changes, and incident response to maintain integrity.
- Ensuring that any suspected or confirmed security incidents are reported to the IT Support team.
- Maintaining vigilance against material that may be a deepfake which can be used to spread misinformation or impersonate someone to commit cyber fraud). This includes AI-generated child sexual abuse material (AICSAM)
- Training staff and students to be aware of the importance of Cyber Security and the potential involvement of AI to carry out cyber-crime.

8. Reporting

All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the IT Support team. 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.

9. Restricting Access

Our approach to AI access is built on a layered security model that uses internet filtering to restrict access to public AI and app level security within our Google Workspace to restrict access to Gemini for students and to allow use for staff. This aids us to prioritise immediate data protection and academic integrity while preserving the option for future student use of AI to aid their education.

Internet Filtering

Using our existing internet security and filtering systems we can restrict access to websites and web applications.

Blocking Public AI: Working with our filtering partner Cisco Umbrella, we are able to enforce our 'deny-by-default' policy for unauthorised Generative AI (GenAI) access. Cisco Umbrella uses live web filtering information from sources including the UK Government to ensure all generative AI systems are blocked automatically. (See our Internet Usage and Filtering policy for more information)

Allowing Google Gemini: Staff are specifically allowed access to Google Gemini.

Comprehensive Coverage: Filtering is applied to all school devices even when used by staff or students at home.

Google Workspace Domain-Secured Gemini

Through our Google Workspace we can control which users have access to Gemini AI.

Secure Staff Access: Access to domain-secured Gemini is currently allowed for staff only via their Calday Google Workspace accounts. This access is governed by our enterprise agreement, ensuring no data is used for model training and all activity remains within our secure domain for audit purposes.

Student Restriction: All AI access remains blocked for students at this time, maintaining control over academic integrity and safety.

This two-pronged approach, blocking access and preventing unsanctioned system use significantly mitigates the risks associated with unsupervised staff and student use of AI, such as plagiarism, data privacy concerns, and exposure to unvetted content.

10. Future Strategy

Enhancing Teaching & Learning with Controlled Student AI

While currently restricted, the technical framework is designed to allow for controlled student integration in the future.

Strategic Goal: The school to develop a school-wide approach and curriculum framework to safely integrate domain-secured Gemini access for students to enhance teaching and learning.

Phased Rollout: Future student access will be managed through the Google Workspace Organisational Units (OUs), allowing for a phased rollout to specific year groups or classes only when supporting training, policy, and curriculum guidelines are fully established.

Outcome: This ensures that when students do gain access, it will be in a structured, supervised, and secure environment that aligns with our educational goals.