



AI Policy

Adopted on:	Nov-25
Signed on behalf of the Governing Body	Mrs B Read Chair
Review Date	Nov-26

1. Introduction and Vision

1.1 Context

Artificial Intelligence (AI) is rapidly becoming an integral part of modern life and education. AI technologies—from generative tools like ChatGPT and Google Gemini to embedded AI within learning platforms—are increasingly accessible to schools, teachers, and pupils. This policy sets out how **Cherrywood Community Primary School** will responsibly harness AI to enhance teaching, learning, and school operations, whilst maintaining the highest standards of safeguarding, data protection, and educational integrity.

This policy recognises both the opportunities and challenges that AI presents. We acknowledge that many staff and pupils already use AI tools outside school, making it essential that our school community develops a clear, consistent, and supportive approach to their use.

1.2 Vision Statement

Cherrywood Community Primary School is committed to harnessing AI to support teaching excellence, personalised learning, operational efficiency, and future-readiness. This policy ensures the responsible, secure, and equitable use of AI across our school.

We use AI to:

- Enhance learning opportunities and personalise education
- Support staff workload and operational efficiency
- Develop pupils' AI literacy and critical thinking skills
- Prepare pupils for a technology-rich future
- Work more efficiently so we can focus more time on direct pupil engagement

This policy outlines our commitment to the responsible, secure, and fair implementation of AI throughout our school, in line with our values.

1.3 Aims

- To enhance teaching and learning outcomes for all pupils, particularly through personalisation and differentiation
- To support staff workload and administrative efficiency
- To educate staff and pupils about safe, responsible, ethical, and legal use of AI
- To protect the privacy, rights, and data of all stakeholders in line with UK GDPR
- To develop AI literacy across our school community
- To prepare pupils for a future in which AI technology will be integral
- To promote equity in education and prevent AI-related discrimination
- To maintain academic integrity and critical thinking

- To comply with all relevant legislation, including Keeping Children Safe in Education (KCSIE) 2025
-

2. Scope and Responsibilities

2.1 Who This Policy Applies To

This policy applies to:

- All staff (teaching, supply, trainees, temporary, administrative and support staff)
- All governors and trustees
- All volunteers and contractors working within our school
- All pupils
- Anyone using school systems or working on behalf of **Cherrywood Community Primary School**

These groups are collectively referred to as "the school community" throughout this policy.

2.2 Authorised AI Tools

Cherrywood Community Primary School recognises two categories of AI tools:

Authorised AI Tools: AI tools that have been formally assessed by school leadership, data protection officers, and safeguarding leads, with a Data Protection Impact Assessment (DPIA) completed. These tools have been evaluated for security, age-appropriateness, data handling practices, and alignment with school values. A list of these AI tools is detailed in appendix C.

Unauthorised AI Tools: Any AI tools not listed in appendix C. Unauthorised tools must not be used with school data or pupils' personal information and usage should follow the guidance and requirements in this policy.

2.3 Key Responsibilities

Headteacher / Senior Leadership Team

- Approve the AI policy and all decisions regarding AI use in school
- Ensure compliance with all relevant legislation
- Ensure adequate resources and training for staff
- Monitor and evaluate the impact of AI on pupils, staff, and school operations
- Review this policy annually and update as necessary

Data Protection Officer

- Advise on data protection obligations in relation to AI use

- Complete DPIAs for all new AI tools before they are authorised for use
- Review any incidents or concerns relating to data protection and AI
- Ensure compliance with UK GDPR

Designated Safeguarding Lead (DSL)

- Ensure AI tools do not expose pupils to harm, including harmful content, misinformation, deepfakes, and impersonation
- Review filtering and monitoring arrangements for AI tools in light of KCSIE 2025 requirements
- Investigate any safeguarding concerns relating to AI use
- Ensure staff understand their responsibilities in managing AI-related safeguarding risks

IT Lead / Technical Team

- Manage the technical implementation of authorised AI tools
- Ensure security patches and updates are applied
- Provide technical support and training to staff and pupils
- Monitor for security incidents
- Report any technical concerns to the Headteacher and Data Protection Officer

All Staff

- Read and understand this policy before using any AI tools
- Use only authorised AI tools, for school, staff, pupil and parent data
- Comply with data protection and safeguarding requirements
- Never upload school data or pupils' personal information to unauthorised AI tools
- Report any concerns or incidents to the Headteacher, DSL, or Data Protection Officer
- Model responsible AI use for pupils
- Engage with professional development opportunities
- Be transparent about where and how AI has been used

Pupils

- Use only authorised AI tools approved by staff
 - Never enter personal information into AI tools without explicit permission from staff
 - Use AI responsibly and ethically
 - Report any concerns or harmful content they encounter
 - Engage with learning about AI, including its capabilities and limitations
-

3. Use of AI by Staff

3.1 General Principles

All staff using AI will:

- Comply with UK GDPR, safeguarding legislation (KCSIE), intellectual property law, and this policy
- Use AI responsibly to complement, not replace, their professional judgment and expertise
- Review and edit all AI-generated content to ensure accuracy, appropriateness, and alignment with school values
- Remain accountable for all content produced with AI assistance
- Not use AI to make strategic decisions or decisions that significantly impact individuals
- Not allow pupils' work to be used to train AI models without appropriate consent
- Be transparent about AI use where relevant

3.2 Approved Uses: Teaching and Learning

Staff may use authorised AI tools to support teaching and learning, including:

- **Personalised learning:** Generating tailored resources and activities based on individual pupil needs
- **Lesson planning:** Creating or adapting lesson plans, learning objectives, and success criteria
- **Resource creation:** Generating images, text, multiple choice questions, word problems, spelling tests, and other teaching materials
- **Differentiation and SEND support:** Creating adapted resources, simplifying texts, or generating alternative formats (e.g., audio versions) to support pupils with different needs
- **Assessment and feedback:** Generating model answers, marking rubrics, or using AI-powered marking tools for objective assessments (e.g., multiple-choice), with staff review for subjective work
- **Pupil feedback:** Generating formative feedback suggestions for pupils on their work (to be reviewed by staff before sharing)
- **Report writing:** Using AI as a starting point for pupil reports, subject to full review and personalisation by staff

All AI-generated teaching content must be:

- Reviewed for factual accuracy
- Checked for bias or discriminatory content
- Edited to reflect the school's values and tone
- Age-appropriate and suitable for the intended pupils

- Credited where appropriate

3.3 Approved Uses: Workload and Administration

Staff may use authorised AI tools to support administration and reduce workload, including:

- **Drafting documents:** Creating draft policies, letters, emails, and guidance documents (subject to review and approval)
- **Summarising information:** Summarising meeting notes, documents, or online content to save time
- **Data analysis:** Identifying patterns in pupil attainment and progress data to inform interventions
- **Planning tools:** Creating overviews of units of learning as a starting point for planning
- **Email and communication:** Drafting internal communications (always subject to review before sending)

Staff must remember that they remain accountable for all content, and AI output should be seen as a starting point for professional consideration, not the final product.

3.4 What Staff Should Not Do

Staff must not use AI to:

- Replace human judgment in decisions affecting individual pupils or staff
- Make decisions on behaviour, safeguarding, assessment, or admission without human review
- Upload identifiable information about pupils (names, photos, addresses) to unauthorised AI tools
- Upload sensitive personal data about staff, pupils, or families
- Create, generate, or process content for training purposes without explicit consent
- Share confidential school data, policies, or sensitive information
- Bypass data protection or safeguarding procedures
- Generate content that is inappropriate, discriminatory, or harmful
- Make strategic school decisions without human involvement

3.5 AI Notetakers and Recording Tools

AI notetaking tools (e.g., Microsoft Copilot, Google NotebookLM, or third-party apps) may only be used in meetings if:

- A Data Protection Impact Assessment has been completed and approved
- All participants have been informed in advance that AI will be used
- All participants have consented to AI notetaking

- If any participant objects, the meeting organiser will consider whether the meeting can proceed without the tool

Where meetings include external participants (parents, governors, external professionals), staff should communicate in advance that AI notetaking will not be used unless all parties consent.

4. Use of AI by Pupils

4.1 General Principles

Pupils will only use AI tools that have been explicitly authorised by **Cherrywood Community Primary School** for educational purposes. Pupils will:

- Use only approved AI tools during supervised learning time
- Only use AI with explicit permission and guidance from staff
- Never enter personal, sensitive, or identifiable information into AI tools
- Be transparent about their use of AI in schoolwork
- Not use AI to plagiarise, cheat, or submit work as entirely their own
- Engage with learning about AI, including its capabilities, limitations, and ethics

4.2 Age-Appropriate Access

Most commercial AI tools (including ChatGPT, Copilot, and Gemini) have age restrictions (typically 13+ or 18+). **Cherrywood Community Primary School** currently uses AI as follows:

- **Key Stage 1 and 2:** Do not allow pupils to independently use commercial generative AI tools. Pupils may experience AI through teacher-guided demonstrations and supervised activities only.

4.3 Pupil Learning About AI

All pupils will learn about AI as part of their computing curriculum and digital literacy development:

- Understanding what AI is and how it works
- Recognising the presence of AI in everyday life
- Understanding the capabilities and limitations of AI
- Understanding bias, hallucination, and accuracy issues with AI
- Ethical considerations: privacy, intellectual property, consent
- Safe and responsible use of AI
- Recognising harmful or inappropriate content
- Developing critical thinking skills to evaluate AI outputs

4.4 AI in Assessments

- Pupils must not use unauthorised AI tools during formal assessments, exams, or tests unless explicitly permitted by staff

4.5 Pupil Use Does Not Include

- Pupils creating AI-generated content for public sharing (e.g., social media, websites) without staff approval
 - Pupils using AI to generate entire pieces of work without their own thinking and creativity
 - Pupils using AI to access, create, or share inappropriate content
 - Any pupil use of unauthorised AI tools
-

5. Safeguarding and Child Protection

5.1 Regulatory Context

Keeping Children Safe in Education (KCSIE) 2025 explicitly references artificial intelligence for the first time. This means that AI tools, content generated by AI, and pupil interactions with AI systems are now part of the school's online safety and safeguarding framework.

5.2 Key Safeguarding Risks

The school recognises the following risks associated with AI:

- **Harmful or inappropriate content:** Generative AI may produce offensive, violent, sexual, or otherwise inappropriate material
- **Hallucination and misinformation:** AI can generate false information presented as fact, including deepfakes and fabricated sources
- **Impersonation and deception:** AI can be used to create deepfake videos or audio of real people, or to impersonate individuals
- **Conspiracy theories and radicalisation:** AI can be used to generate or amplify misinformation, conspiracy theories, or radicalising content
- **Bias and discrimination:** AI models may replicate or amplify existing biases, producing discriminatory content
- **Grooming and exploitation:** AI may be used by individuals to generate inappropriate content or to impersonate safeguarders
- **Privacy breaches:** Unauthorised sharing of pupil data with AI platforms
- **Exposure to unfiltered content:** AI chatbots may bypass school filters if not properly configured

5.3 Safeguarding Measures

Cherrywood Community Primary School will implement the following safeguarding measures:

Filtering and Monitoring

- All AI tools accessed by pupils will have appropriate content filtering and moderation enabled
- School networks will use web filtering software to monitor AI tool access
- Logs of pupil interactions with AI tools will be reviewed regularly for signs of risk or misuse
- Staff will remain "in the loop" to supervise AI use and intervene if necessary

Assessment and Authorisation

- Before authorising any AI tool for use by pupils, staff will assess:
 - Age-appropriateness and suitability
 - Content filtering and safeguarding features
 - Security and data protection practices
 - Potential risks and how these will be mitigated
- All authorised tools for pupil use will have completed a DPIA and safeguarding risk assessment

Staff Training

- All staff will receive training on recognising and responding to AI-related safeguarding risks
- The DSL will receive enhanced training on new AI-related threats
- Staff will be alert to potential deepfakes, impersonation, and misinformation

Pupil Education

- Pupils will be taught to recognise and report harmful, inappropriate, or suspicious AI interactions
- Pupils will understand the concept of deepfakes and how to identify potentially fabricated content
- Pupils will be encouraged to tell a trusted adult if they encounter any concerning content online, including content generated by AI

Incident Response

- Any safeguarding incident involving AI will be reported immediately to the DSL
- The DSL will investigate in line with the school's Child Protection Policy
- Where appropriate, external agencies (police, CSAM reporting, local authority) will be contacted

- Any AI tool responsible for exposing pupils to harmful material will be reviewed, adjusted, or permanently removed

5.4 Parental Awareness

- Parents will be informed about the school's use of AI in teaching and learning
 - Parents will be made aware of any safeguarding risks associated with AI
 - The school will provide guidance to parents on how to support safe AI use at home
 - Where pupils are using AI tools as part of their learning, parents will be informed and given the opportunity to discuss any concerns
-

6. Data Protection and Privacy

6.1 Legal Framework

All use of AI must comply with all legal requirements including those detailed in appendix D.

6.2 Key Principles

Personal data will not be shared with unauthorised AI tools. Specifically:

- Staff and pupils must not enter identifiable information (names, addresses, email addresses, phone numbers, dates of birth, etc.) into unauthorised AI tools
- Staff and pupils must not upload school documents, pupil records, or confidential information to unauthorised AI tools
- Staff and pupils must not process special category data (information about race, ethnicity, religion, political views, physical/mental health, sexual orientation, etc.) using unauthorised AI tools

Cherrywood Community Primary School has approved a limited set of AI tools that have been assessed as compliant with data protection requirements. These tools:

- Do not retain personal data for training purposes
- Have appropriate security measures in place
- Have transparent privacy policies
- Are backed by Data Protection Impact Assessments (DPIAs)
- Are only used by authorised staff for authorised purposes

6.3 Data Protection Impact Assessment

Before any new AI tool is authorised for use, a DPIA will be completed covering:

- The nature, scope, purpose, and necessity of data processing

- Individuals' reasonable expectations about data use
- The potential impact on individuals' rights and freedoms (both individual harms and systematic harms)
- Potential for bias or discrimination in AI algorithms
- How individuals' consent or rights will be respected
- Mechanisms for addressing concerns or complaints
- Whether processing is proportionate (i.e., the benefits outweigh the risks)
- Security and safeguarding measures

6.4 Handling of AI Tool Selection

When selecting AI tools:

- Leadership will review the privacy policy and terms of service
- A DPIA will be completed before any use with pupil or staff data
- The Data Protection Officer will advise on compliance
- The DSL will assess safeguarding implications
- Staff will not be expected to independently assess tools; leadership will do this

6.5 Staff Responsibilities

All staff will:

- Read and understand the privacy implications of AI tools before use
- Not assume an AI tool is secure or compliant without confirmation from school leadership
- Not enter personal data into AI tools unless explicitly authorised
- Report any suspected data breaches or privacy concerns immediately
- Not download or export personal data to use with unauthorised AI
- Ask the Data Protection Officer or Headteacher before using any new tools

6.6 Pupil Data

- Pupils' names should not be entered into unauthorised tools
- Where assessment information is shared with AI tools, identifying information should be removed
- Parents' personal data (email addresses, phone numbers, addresses) should not be shared with AI tools
- Special category data about pupils (SEN information, safeguarding concerns, health information) should not be processed by unauthorised AI tools

6.7 Intellectual Property and Copyright

- Staff and pupils must respect copyright and intellectual property rights
 - AI tools should not be used to process copyrighted material without permission
 - Pupils' work must not be used to train AI models without appropriate consent from parents/carers
 - Where AI has been used, staff will be transparent about this
-

7. Ethical Use of AI

7.1 General Principles

All staff and pupils using AI will be mindful of the following ethical considerations:

- AI systems are trained on data that may contain human biases (e.g., racism, sexism, discrimination against people with disabilities, socioeconomic bias)
- AI may replicate or amplify these biases, potentially producing discriminatory outputs
- AI systems can produce highly plausible but false information (hallucination)
- AI may cite sources that do not exist or misquote actual sources
- AI models are trained on data up to a certain date and may not reflect current information
- AI should augment human expertise, not replace it
- Staff must apply their professional judgment to all AI outputs
- AI cannot replace human decision-making in matters affecting individuals (e.g., behaviour, assessment, safeguarding decisions)
- Teaching staff remain the key decision-makers in evaluating pupil progress and needs
- Leadership and staff will not rely solely on AI to make significant decisions
- The European Union's AI Act restricts the use of emotion recognition systems (tools that infer or identify emotions based on facial recognition or biometric data)
- Although this Act does not apply in the UK, **Cherrywood Community Primary School** will not use emotion recognition systems in any context

7.2 Understanding AI's Limitations

All staff and pupils should understand that:

- **Current AI is "narrow AI":** It is specialised to perform one task (e.g., text generation, image creation), not multiple tasks like human intelligence
- **AI is not sentient:** It does not have feelings, consciousness, understanding, or intentions. Any appearance of understanding is a reflection of patterns in training data

- **AI does not "think"**: It predicts the next likely word or output based on patterns, similar to a sophisticated autocorrect
 - **AI can be confidently wrong**: AI will often produce plausible-sounding but entirely false information with no awareness that it is wrong
-

8. Preventing Misuse of AI

8.1 Pupil Misuse

Pupils must not use AI to:

- Complete assignments or homework entirely without their own thinking
- Plagiarise or claim AI-generated work as entirely their own
- Create inappropriate, offensive, or harmful content
- Impersonate others
- Access, create, or share explicit, violent, or otherwise harmful material
- Bully or harass other people
- Bypass school security or filtering systems

Teaching staff will:

- Clearly communicate expectations about appropriate AI use
- Teach pupils about the risks and consequences of AI misuse
- Employ diverse assessment methods to verify pupils' own understanding
- Use formative assessment to catch misconceptions early
- Emphasise critical thinking, creativity, and originality in pupil work
- Encourage pupils to be transparent about AI use

Where misuse is suspected:

- Staff will investigate in line with the school's Behaviour Policy
- Staff will discuss the incident with pupils to understand their actions
- Where cheating is suspected, this will be treated as an academic integrity issue and managed through the school's assessment policies
- In serious cases, this may be escalated to parents/carers and leadership
- Continued misuse may result in loss of access to AI tools

8.2 Staff Misuse

Staff must not use AI to:

- Bypass data protection or safeguarding requirements
- Generate inappropriate content (e.g., sexual, violent, discriminatory material)
- Replace professional judgment in decision-making
- Plagiarise or claim AI-generated work as entirely their own in formal contexts
- Use AI for personal gain or in contravention of applicable laws
- Share confidential school or pupil information
- Generate content for external distribution without approval

Where misuse is suspected:

- The Headteacher or relevant leader will investigate
- This will be managed through the school's IT Acceptable Use Policy and/or Disciplinary Policy as appropriate
- Serious breaches may result in disciplinary action up to and including dismissal

9.3 Approved AI Tools

Staff and pupils must not use any AI tools not listed in Appendix C using any of the information below:

- Pupils' personal or academic information
- Identifiable information about staff or families
- Confidential school documents or data
- Sensitive or special category data

If staff wish to use an AI tool using this information, they must:

1. Contact the Headteacher or IT Lead with details of the tool and intended purpose
2. Leadership will assess the tool for:
 - Suitability and educational value
 - Data protection and security compliance
 - Safeguarding implications
 - Licensing and terms of service
3. A DPIA will be completed (where necessary)
4. The tool will be added to the approved list in appendix C or rejected based on the assessment

10. Training and Professional Development

10.1 Induction for New Staff

All new staff will receive:

- A copy of this AI policy during their induction
- An overview of authorised AI tools and their uses
- Training on data protection and safeguarding considerations
- Guidance on the school's expectations for AI use
- An opportunity to ask questions and raise concerns

10.2 Ongoing Professional Development

Cherrywood Community Primary School will provide staff with:

- Annual training updates on AI, including new developments and guidance changes
- Specific training on using authorised AI tools effectively
- Training on recognising and responding to AI-related safeguarding risks
- Opportunities to share good practice and learn from colleagues
- Access to external training or resources (e.g., DfE training modules, HIAS guidance)

10.3 Pupil Education

Pupils will receive age-appropriate education about AI, including:

- What AI is and how it works
- Examples of AI in everyday life
- How to use approved AI tools safely and responsibly
- Understanding bias, accuracy, and limitations of AI
- Ethical considerations (privacy, intellectual property, consent)
- Recognising harmful or suspicious AI interactions
- Developing critical thinking skills to evaluate AI outputs
- How to report concerns about AI

10.4 Parental Engagement

Parents will be informed about the school's use of AI through:

- Information in the school newsletter or parent communications
- Parent information evenings (where appropriate)
- Guidance on AI use and safe practices
- Opportunities to discuss concerns with school leadership
- Information about how they can support AI literacy at home

11. Monitoring and Accountability

11.1 Monitoring Compliance

Cherrywood Community Primary School will monitor compliance with this policy through:

- Regular audits of authorised AI tool usage
- Review of incidents and concerns reported by staff, pupils, or parents
- Monitoring of web filtering logs for AI tool access
- Annual policy review and staff feedback
- Discussions with pupils about their experience with AI
- Parent feedback through surveys or informal consultation

11.2 Reporting Concerns

Any staff member, pupil, or parent with concerns about AI use should report to:

- Their immediate line manager or teacher
- The Designated Safeguarding Lead (for safeguarding concerns)
- The Data Protection Officer (for data protection concerns)
- The Headteacher (for general policy concerns)

All concerns will be taken seriously and investigated promptly.

11.3 Incidents and Breaches

Where a potential breach of this policy, data protection law, or safeguarding is identified:

- The incident will be reported immediately to relevant leaders
- An investigation will be conducted
- Where necessary, the Data Protection Officer and/or DSL will be involved
- Staff and/or pupils involved will be supported and disciplined as appropriate
- Parents/carers will be informed where pupils are affected

11.4 Policy Review

This policy will be reviewed:

- Annually as a minimum, and potentially more frequently as AI and guidance develops
- Following any significant incident or concern

- When new guidance is released (e.g., from DfE, Ofsted, ICO)
 - When new AI tools are introduced
 - When feedback from staff, pupils, or parents suggests amendments are needed
-

12. Definitions

Algorithm: A set of rules or instructions that a computer follows to perform a task.

Artificial Intelligence (AI): An umbrella term for computer systems designed to perform tasks that typically require human intelligence, including learning, reasoning, problem-solving, and decision-making.

Bias (in AI): When an AI system produces unequal, prejudiced, or discriminatory results, often because it was trained on biased data.

Chatbot: An AI-powered conversational tool that can respond to text or voice input, mimicking human conversation.

Content Filtering: Technology that blocks or restricts access to certain types of content online (e.g., inappropriate material, harmful websites).

Data Protection Impact Assessment (DPIA): A process for assessing how data processing activities (including AI) might affect individuals' rights, and identifying measures to mitigate any risks.

Deepfake: Synthetic media (video or audio) created using AI to depict someone saying or doing something they did not actually say or do. Can be used to spread misinformation or impersonate someone.

Generative AI: AI systems that can create new content (text, images, code, audio, video) based on patterns learned from training data.

Hallucination: When an AI system produces information that sounds plausible but is actually false or inaccurate.

Large Language Model (LLM): An advanced AI system trained on vast amounts of text data, capable of understanding and generating human language (e.g., ChatGPT, Gemini, Copilot).

Machine Learning: A subset of AI where algorithms improve their performance by learning from data, rather than being explicitly programmed.

Natural Language Processing (NLP): The ability of AI to understand and process human language (written or spoken).

Personal Data: Any information relating to an identified or identifiable person (e.g., name, address, email, pupil record).

Special Category Data: Sensitive personal information including data about race, ethnicity, religion, health, disabilities, sexual orientation, or biometric data.

Transparency: Being clear and open about how AI is being used, what it is used for, and what the limitations are.

UK GDPR: UK General Data Protection Regulation, the UK's data protection law that sets rules on how personal data must be handled.

9.3 Approved AI Tools

Staff and pupils must not use any AI tools not listed in Appendix C using any of the information below:

- Pupils' personal or academic information
 - Identifiable information about staff or families
 - Confidential school documents or data
 - Sensitive or special category data
-

Appendices

Appendix A: AI Literacy Framework for Pupils

Pupils should develop understanding across four domains:

Engaging with AI: Using AI tools as a resource, evaluating outputs for accuracy and relevance, and understanding AI's capabilities.

Creating with AI: Using AI collaboratively to solve problems or create content, providing feedback and refinement, and ensuring outputs are ethical and fair.

Managing AI: Intentionally choosing when and how to use AI, delegating appropriate tasks to AI so humans can focus on higher-order thinking, and reflecting on whether AI use aligns with personal values.

Designing AI: Understanding how AI works, recognising how data, design, and training affect AI behaviour, and understanding the social and ethical impacts of AI.

Appendix B: Good Practice in Using AI

Before using AI:

- Clarify your purpose: What exactly are you trying to achieve?
- Identify the audience: Who is this for?
- Consider alternatives: Is AI the best option, or would another approach be better?
- Plan for review: How will you check, edit, and verify the AI output?

When using AI:

- Be specific and clear in your instructions (prompts)
- Provide context and constraints to guide the AI
- Be prepared to iterate and refine your requests
- Review the output carefully

After using AI:

- Fact-check information against reliable sources
- Review for bias, accuracy, and appropriateness
- Edit to match your style, tone, and purpose
- Attribute AI use where relevant
- Remember: You are responsible for the final product

Appendix C: Approved AI tools

The following AI tools have been assessed and authorised for use by **Cherrywood Community Primary School**:

AI Tool	Authorised Users	Approved Purposes
Microsoft 365 Copilot	Staff	Lesson planning, resource creation, administrative support
Arbot	Staff	Data analysis, pupil progress monitoring
[Other approved tool]	Staff / Pupils	[Specific uses]

Appendix D: Referenced Policies and Legislation

- Department for Education (DfE) guidance on Generative AI in education (2025)
- Ofsted's approach to AI inspection and regulation
- Hampshire Inspection and Advisory Service (HIAS) AI Policy Guidance (2025)
- The Institute for Ethical AI in Education framework
- UK General Data Protection Regulation (UK GDPR)
- Keeping Children Safe in Education (KCSIE) 2025
- Our school's existing safeguarding, data protection, and IT security policies
- Data (Use and Access) Act 2025
- Information Commissioner's Office (ICO) guidance
- School's Data Protection Policy