Forest Edge Learning Federation

AI Policy

Name of School:	Breamore CE Primary, Hale Primary and Hyde CE Primary
Name of Responsible Manager/Headteacher:	Tracy Allen – Executive Headteacher
Date Policy approved and adopted:	November 2025
Date Due for review:	November 2026

At Forest Edge learning federation,
we grow and learn together with ***grace*** *and love.*
Our nurturing and inclusive culture enables every member of our school family to be valued and ***respect****ed unconditionally.*
Our ambitious and forward thinking curriculum provides every child with the ***courage*** *to be successful and confident to make their own individual difference to the world.*

This policy should be read alongside The Forest Edge Learning Federation's policies and procedures on online safety and acceptable use of ICT.

1. Purpose

This policy sets out how Forest Edge Learning Federation uses generative artificial intelligence (AI) tools (for example, AI-chatbots, content-generation tools, lesson-planning assistants, pupil-facing AI applications) in a safe, responsible and pedagogically effective way, in line with our safeguarding, data protection and online-safety obligations.
It ensures that use of generative AI is consistent with our duty under KCSIE to safeguard children and promote their welfare, including online safety.

2. Scope

This policy applies to all staff, volunteers, governors, contractors and pupils (where relevant) at Forest Edge who use generative AI (hereafter "AI tools") either on school premises, in remote learning settings or for school-related activities.

It covers:

- AI tools used by staff (for planning, assessment, teaching resources, professional development)
- AI tools used by pupils (with supervision)
- AI tools used by third-party providers engaged by the school
- Data, safeguarding and ethical issues arising from AI use.

3. Definitions

- **Generative AI**: software systems that generate text, images, audio, video or other content in response to prompts or user inputs, including — but not limited to — large language models, generative chatbots, AI-assistants and content-generation tools.
- **Safeguarding**: in line with KCSIE, protecting children from maltreatment, preventing impairment of children's mental and physical health or development, ensuring children grow up in circumstances consistent with safe and effective care, and taking

action to enable all children to have the best outcomes.

- **Online safety**: protection of children when using the internet, mobile devices or other technologies, including risks from harmful or inappropriate content, contact, conduct and commerce. KCSIE 2025 updates include reference to misinformation/ disinformation and generative AI.

4. Rationale

- Our schools recognise that generative AI offers many educational opportunities: enhancing creativity, supporting differentiated teaching, enabling efficient preparation of resources, offering new forms of pupil interaction.

- However, we also recognise that AI tools carry specific risks: inappropriate or inaccurate content generation, bias, data privacy issues, pupils becoming over-reliant on tools, safeguarding risks (including exposure to harmful content, manipulative or biased outputs, children's data misuse), and challenges to academic integrity.

- In line with KCSIE 2025, our schools must ensure that any AI tool is treated as part of our online safety and safeguarding framework, including risk assessment, filtering/monitoring, staff training and pupil education.

5. Roles and Responsibilities

- The Governing Body has overall oversight of this policy and ensures appropriate resources and accountability mechanisms are in place.

- The Executive Headteacher and Computing Lead are responsible for implementing the policy, ensuring staff awareness, monitoring compliance, and reporting to governors as part of any online safety monitoring carried out by the safeguarding governor.

- The Designated Safeguarding Lead (DSL) works alongside the IT team to ensure AI risk assessments are completed (where necessary), appropriate filters/monitoring systems are in place, and any safeguarding concerns linked to AI usage are addressed.

- The school's IT and broadband providers are responsible for ensuring that the school's digital infrastructure supports the safe use of AI tools, including filtering, monitoring, logging, securing data, and ensuring vendor/third-party compliance. Filtering and monitoring reports are checked regularly by the Executive Headteacher.

- All staff must understand the policy, receive appropriate training on AI tools and associated risks, and ensure safe, pedagogically appropriate use of AI.

- Pupils will be educated about safe, responsible use of AI tools, their rights and responsibilities during online safety lessons.

6. Acceptable Use – Staff

When staff use AI tools, the following practice must apply:

- Before implementing any AI tool for classroom or pupil-use, a risk assessment must be completed (see section 7). At Forest Edge, AI tools will not be regularly used by the children during lessons due to the age range of our children, and to minimise risks.

- Staff remain ultimately responsible for the educational integrity of their work: AI outputs must be reviewed, edited and validated by a human (human-in-the-loop).

- Staff must ensure that any content generated by AI is age-appropriate, pedagogically sound, unbiased and verified for accuracy.

- Staff must ensure pupils' data (including personal data) is not input into AI systems inappropriately; confidentiality and data protection must be maintained.

- Staff must not use AI tools in a way that replaces professional judgement in safeguarding matters (for example, making decisions about a pupil's welfare).

- Staff should follow the school's acceptable use policy for technology, and this AI policy, when using AI tools.

- If using external/third-party AI tools or services, staff must check that the vendor complies with data protection law (UK GDPR/UK Data Protection Act 2018) and that the school holds a valid contract and data-processing agreement.

- Any concerns or incidents relating to the use of AI (for example inappropriate output, suspected data breach, pupil distress) must be reported to the DSL/Computing lead immediately.

7. Risk Assessment and Safe Implementation

- Before deploying any AI tool for staff or pupil use, the school will conduct a documented risk assessment that considers:

    - Safeguarding risks: Could the tool expose pupils to harmful content, manipulation, or bias?
    - Online-safety and content risks: Does the tool generate unsupervised content? Could it allow inappropriate contact/interaction?
    - Data protection risks: What personal data is processed, how is it stored, is it transferred externally?
    - Intellectual property issues: Is the output safe, legally usable, appropriately attributed?
    - Pedagogical risks: Might pupils misuse the tool (e.g., for plagiarism)? Are staff trained to supervise it properly?
    - Technical/monitoring risks: Does the school's filtering/monitoring system recognise AI-generated content? Is there logging of use and prompts?
    - Vendor/third-party risks: Does the supplier meet the DfE's Generative AI: Product Safety Expectations?
- Based on the risk assessment, the school will decide whether the AI tool may be used, under what conditions, and what safeguards to deploy (for example, restricted access, supervised sessions, logging of prompts/actions, training for users).
- The school will keep a register of approved AI tools and their risk assessment status.
- Risk assessments will be reviewed at least annually, or sooner if a new tool is introduced or a safeguarding/ data incident occurs.

8. Filtering, Monitoring, Logging & Review

- In line with KCSIE 2025 and the DfE's expectations, the school will ensure that its filtering and monitoring systems are capable of addressing risks posed by generative AI tools (including real-time and near-real-time monitoring of pupil and staff use, logging of AI prompts and outputs where feasible).
- The school will ensure roles and responsibilities for filtering/monitoring are clearly defined (see online safety policy).
- Any significant incidents (e.g., inappropriate AI output, safeguarding concern triggered by AI use, data breach involving AI system) will be investigated and recorded; relevant lessons will inform review of this policy and future risk assessments.

9. Pupil Use of AI Tools

- Pupils may only use AI tools under the supervision of a teacher or designated adult, and only when the tool has been approved by the school.

- Before use, pupils will be given clear guidance on safe and appropriate use of the tool, including:

    - Explaining what generative AI is, the benefits and risks (age-appropriate)

    - How to treat AI output critically (the tool may be wrong, biased or inappropriate)

    - What data they must not input into the tool (personal data, sensitive information, names/addresses etc.)

    - The importance of academic integrity (e.g., not mis-representing AI-output as wholly their own)

    - How to report concerns (e.g., inappropriate output, unexpected contact, discomfort) to a teacher or adult.

- The school's computing and RSHE (Relationships, Sex and Health Education) curriculum will include aspects of digital literacy, critical thinking about AI-generated content, and safe/ethical use of technology, aligned with KCSIE's emphasis on misinformation, disinformation and AI risk. At Forest Edge, we use the ProjectEvolve resources to support this teaching.

10. Vendor/Third-Party AI Services

- Any procurement of AI tools or services must follow the school's procurement/safeguarding/data-protection policy.

- The school must carry out due diligence on the vendor, including checking:

    - The vendor's safeguarding measures (content-filtering, logging, moderation)

    - Compliance with UK data-protection law (UK GDPR, Data Protection Act 2018)

    - Security of the AI system, including resilience against misuse or malicious prompts.

- Contracts must include data-processing agreements, clear roles & responsibilities, and ensure school retains overall control of pupil data and adult-user data.

- The vendor must allow the school to audit or review logs or evidence of use, or allow export of logs for safeguarding review if necessary.

11. Data Protection and Privacy

- Use of AI tools must comply with the school's Data Protection Policy and UK GDPR/data protection legislation.

- Staff must not input personal, sensitive or special category data about pupils or staff into AI tools unless the tool is explicitly approved for that purpose and adequate safeguards are in place (e.g., anonymisation, encryption, consent).

- Where pupil data is processed externally (for example cloud-based AI service), the school must ensure appropriate safeguards, data-processing agreements, lawful bases for processing, information to parents/carers, and encryption/international-transfer safeguards as necessary.

- The school will keep a record of where AI tools process pupil/staff data, the legal basis for processing, retention period and deletion process.

12. Training and Professional Development

- The school will provide training for staff on:
    - What generative AI is and how it works (basic level)
    - The opportunities and risks of AI in the school context
    - The school's policy on AI and the safe, responsible use of AI tools
    - How to support pupils in using AI tools safely and responsibly
    - How safeguarding and online-safety frameworks link to AI usage (including KCSIE obligations)

- The school will include AI-awareness within its safeguarding/online-safety induction for new staff, and update CPD at least annually.

13. Monitoring, Review and Enforcement

- This policy will be reviewed at least annually (or sooner if there are major changes in AI use, new tools, or a safeguarding/data-incident) and shared with the Governing

Body.

- Compliance with the policy will be monitored by the Headteacher, DSL and Computing Lead who will report to governors/trustees.

- The school will maintain a register of incidents linked to AI use (including close-calls, investigations, remedial actions) and this will feed into the annual review and risk assessment process.