Appendix: Artificial Intelligence (AI) – Safeguarding and Child Protection Considerations

As Artificial Intelligence (AI) tools become more widespread in education and everyday life, it is essential that their use within school is consistent with our safeguarding duties under *Keeping Children Safe in Education (KCSIE)* and the school's wider child protection responsibilities.

This appendix outlines key safeguarding principles relating to AI use by pupils, staff, and third-party providers.

1. AI and the Safeguarding Context

AI technologies — including chatbots, image generators, recommendation engines, and predictive tools — pose both **opportunities and risks** in a school setting. The school recognises that these tools can:

- Influence behaviour, attitudes, and beliefs.
- Generate content that is inappropriate, misleading, or harmful.
- Be used (deliberately or unintentionally) to bypass safety systems.

All use of AI must therefore be guided by a safeguarding-first approach.

2. Key Safeguarding Safeguards

a. Age-Appropriate Access

- Pupils will **not** be given access to any generative AI platform or tool that has an age restriction higher than their chronological age.
- Staff must verify the age suitability of any AI-enabled tool used in teaching or homework**.**

b. Supervised Use Only

- Pupils may only engage with AI tools under **direct adult** supervision and in pre-approved, curriculum-based activities (e.g. through Teach Computing).
- Unsupervised or unfiltered use of generative AI tools is not permitted.

c. No Sharing of Personal Information

- Pupils must not be asked to — and must be taught not to — enter personal information (e.g. names, photos, locations, or identifying facts) into AI platforms.
- Staff are strictly prohibited from entering personal, sensitive, or safeguarding-related information about pupils into any AI service.

3. Risk Areas for Safeguarding

The school recognises the following as emerging safeguarding risks associated with AI:

- **Exposure to inappropriate content:** AI tools may generate or suggest violent, sexual, or disturbing content, even in error.
- **Misinformation or bias:** AI may present fabricated or biased information that could mislead children.
- **Identity deception and impersonation:** AI-generated media can be used to mimic voices or faces (e.g. deepfakes).
- **Exploitation or manipulation:** Pupils may be targeted with AI-enhanced scams, grooming, or coercive behaviour, particularly outside of school.
- **Emotional or psychological impact:** Over-reliance on AI, or negative experiences with it, may affect self-esteem, relationships, or mental health.

4. Staff Responsibilities and Training

All staff must:

- Remain vigilant to signs that pupils may be misusing AI or encountering distressing content.
- Include discussion of AI risks in PSHE, computing, and online safety education.
- Report any concerns involving AI use — in or outside school — through the usual safeguarding procedures.
- Ensure they do not use AI to communicate with pupils or create educational materials that have not been reviewed for safeguarding risks.

5. Teaching and Education

- AI use is addressed as part of the school's **online safety curriculum,** helping children understand:
  - How AI works and what its limits are.
  - How to identify when something might be AI-generated.
  - Why they should never share personal information with online tools.
  - The importance of speaking to a trusted adult about anything that causes concern online.

6. Monitoring and Response

- All internet use on school devices is monitored through **Smoothwall**, including attempts to access AI tools.

- Safeguarding concerns involving AI will be treated in line with the school's Child Protection procedures and may involve referral to external agencies (e.g. police, LADO, CEOP).
- Where concerns involve out-of-school use of AI (e.g. harmful social media trends, AI-generated bullying content), staff will engage with families and support pupils as appropriate.

7. Oversight and Review

- The **Designated Safeguarding Lead (DSL)** and **Online Learning Lead** will oversee AI-related safeguarding risks and ensure staff are informed of new threats.
- This appendix will be reviewed annually or sooner in light of changes in technology or reported safeguarding incidents involving AI.

Key Contacts and Support

- **Designated Safeguarding Lead (DSL):** Hannah Smith
- **Deputy DSL(s):** Sarah Parkes, Emily Vivash, Julie Smith, Tracey Cadman, Amber Harris
- **Online Safety Lead:** Steve Butler
- **Data Protection Officer (DPO):** Elaine Pugh

Further reading:

- *Keeping Children Safe in Education (KCSIE)*
- UK Safer Internet Centre: https://www.saferinternet.org.uk/
- NSPCC AI and Online Safety: https://www.nspcc.org.uk