ecp safeguarding
EMPOWER · CARE · PROTECT

AI and Safeguarding

A practical checklist

Navigating AI Safely: A School Leader's Checklist

The integration of AI into education brings both exciting opportunities and critical safeguarding challenges. As technology evolves, so must our approaches to protecting pupils and promoting safe, meaningful learning. This checklist is designed to help you navigate the responsible use of AI by highlighting key risks, legal obligations, and best practices across safeguarding, data protection, and digital wellbeing. It supports leaders, staff, and governors in making informed decisions that keep pupils safe and uphold educational integrity.

General safeguarding principles

[ ] Ensure all staff understand safeguarding is a shared responsibility.
[ ] Align all AI use with Keeping Children Safe in Education guidance.
[ ] Restrict pupil access to free AI tools without verified safeguards or data protections.
[ ] Enforce age restrictions and obtain parental consent for users under 18.
[ ] Promote deeper learning and avoid over-reliance on AI for educational content.

Identifying AI-Related Risks

[ ] Recognise potential for harmful, inaccurate, biased, or offensive content.
[ ] Monitor for learning shortcuts (e.g. AI giving answers without explanations).
[ ] Stay vigilant about AI-generated scams or manipulative content.
[ ] Maintain human oversight and quality control in all AI-assisted tasks.

Online Safety & Image Use

[ ] Train staff, pupils, and parents about AI-generated images and deepfakes.
[ ] Ensure staff are prepared to handle risks such as sextortion or image misuse.
[ ] Treat pupil photos as personal data - ensure proper consent and legal use.
[ ] Avoid publishing pupil names with images unless absolutely necessary and with parent consent.

Incident Response

[ ] Report indecent content involving minors to the Internet Watch Foundation (IWF).
[ ] Use the CEOP Safety Centre for cases of online sexual exploitation.
[ ] Follow school's established safeguarding and reporting protocols.
[ ] Escalate any potential criminal activity to law enforcement promptly.

Policy & Staff Training

[ ] Update school policies to reflect AI-related safety and behaviour considerations.
[ ] Conduct annual reviews of filtering, monitoring, and online safety provisions.
[ ] Utilise assessment tools such as 360safe and London Grid for Learning audits.
[ ] Schedule regular training to stay ahead of emerging digital threats.

Continued on next page...

Selecting AI Tools Safely

[ ] Complete a Data Protection Impact Assessment (DPIA) prior to use.
[ ] Ask:
- Does this tool solve a genuine need?
- Is it UK GDPR compliant and secure?
- Is it safe, ethical, and cost-effective?

[ ] Ensure transparency and human supervision remain central to decision-making.

Mental Health Applications

[ ] Exercise caution with AI tools aimed at student wellbeing or mental health.
[ ] Verify such tools are approved by the Medicines and Healthcare Products Regulatory Authority (MHRA) and comply with regulations.

AI and Data Oversight

[ ] Use AI to assist with data trend analysis, not to replace professional judgement.
[ ] Never delegate final decisions (e.g. admissions or grades) to AI alone.
[ ] Empower leaders to use AI tools for interpreting data in accessible language.

Resources

Child Exploitation and Online Protection (CEOP)
Internet Watch Foundation
London Grid for Learning (LGFL)
360Safe
Keeping Children Safe in Education (KCSIE)
Using AI in Education Settings
AI in schools support
AI policy Paper
Product Safety Framework