Our AI policy has been updated to ensure we are in line with current legislation, KCSIE 2026 — Review Sept 2027

Policy status: This policy reflects Keeping Children Safe in Education (KCSIE) 2026, which applies from 1 September 2026, and the Independent School Standards (Part 3: welfare, health and safety of pupils). It forms part of BT&E's safeguarding and online safety arrangements and must be read alongside the Safeguarding and Child Protection Policy, Online Safety Policy, Behaviour Policy, Anti-Bullying Policy, Acceptable Use Policy, Mobile Phone Policy, Assessment Policy, Data Protection Policy and Staff Code of Conduct.

Purpose:

To help students use Artificial Intelligence (AI) tools (like ChatGPT, Grammarly, or image generators) safely, responsibly, and in ways that support learning.

AI use is part of BT&E's wider safeguarding and online safety arrangements. AI-related risks, including AI-generated abuse, deepfake or manipulated images, impersonation, misinformation, harmful content, grooming risks, child-on-child abuse and harmful sexual behaviour, are treated as potential safeguarding concerns and are managed in line with the Safeguarding and Child Protection Policy.

1. Why We Use AI

- To support learning — help with brainstorming, summaries, and practice questions.
- To improve accessibility — e.g., text-to-speech or simplified reading materials.
- To save teacher time — e.g., lesson planning or grading ideas.

AI is always used to enhance teaching, not replace teachers or real student learning.

AI must not be used in a way that replaces professional judgement, pastoral oversight, safeguarding decision-making, assessment of risk, or direct support from staff. Staff remain responsible for checking AI-generated content for accuracy, bias, age-appropriateness, safeguarding risk and accessibility before it is used with learners.

2. What is Allowed



Students may use AI for:

- Drafting ideas, checking grammar, or creating study notes (with teacher approval).
- Getting examples or explanations when learning a new topic.

Students may only use AI tools that have been approved by BT&E, are age-appropriate, and are used under staff direction or supervision. Where AI tools require accounts, data sharing or content uploads, approval must be obtained through the school's safeguarding, data protection and IT approval processes before use.



Teachers may use AI for:

- Generating teaching resources or differentiating content for learners.

AI use must always follow classroom rules and assignment instructions.

Any use of AI in teaching, learning or administration must comply with the school's safeguarding, behaviour, online safety, acceptable use, mobile phone, assessment, data protection and information security policies.

3. What is Not Allowed



Students must not:

- Submit AI-generated work as their own.
- Upload personal data (names, photos, addresses) to AI tools.
- Use AI to create harmful, misleading, or inappropriate content.
- Use AI to create, alter, share or threaten to share images, audio, video or text that bullies, harasses, humiliates, impersonates, sexualises, coerces, blackmails or otherwise harms another person, including AI-generated or deepfake content.



Teachers must not upload student data to unapproved AI tools.

Staff must not use unapproved AI tools to make safeguarding decisions, profile learners, generate behaviour or risk judgements, process special category data, or produce content about individual children without appropriate authorisation and a data protection impact assessment (DPIA). Staff misuse of AI, including creating or sharing inappropriate content involving learners, will be managed under the Staff Code of Conduct and the procedures for managing allegations and low-level concerns about adults.

4. Academic Integrity

- Students must declare when AI was used (for example: “I used ChatGPT to brainstorm ideas”).
- Undeclared or dishonest use may count as academic misconduct.
- Teachers will design assessments to test real understanding — not AI skill.

Assessment guidance will make clear when AI may and may not be used, how students must acknowledge AI support, and how staff will respond to suspected misuse. For qualifications, the Joint Council for Qualifications (JCQ) guidance on AI use in assessments and the relevant awarding body requirements will be followed. Staff will design tasks that allow students to demonstrate genuine understanding and will not rely solely on AI-detection tools when making academic misconduct decisions.

5. Privacy & Safety

- The school only uses AI tools that comply with UK GDPR and the Data Protection Act 2018 and that meet the Department for Education's generative AI product safety expectations.
- Personal or sensitive student data is only processed by AI tools where there is a lawful basis, a completed DPIA where required, and clear information in the school's privacy notices. Parental consent will be sought where consent is the appropriate lawful basis.
- Any AI-related concerns can be reported to the AI/Data Protection Lead.
- AI-related concerns, including suspected AI-generated abuse, deepfakes, impersonation, grooming, coercion, blackmail, harassment, misinformation, harmful sexual behaviour or child-on-child abuse, must be reported immediately to the Designated Safeguarding Lead using the setting's normal safeguarding reporting route.

Before approving any AI tool, BT&E will complete appropriate checks, including a DPIA, age suitability, information security, safeguarding risks, record keeping, retention, bias, transparency and whether content may be used to train external systems. Checks will take account of the Department for Education's generative AI product safety expectations, including filtering, monitoring and reporting, security, privacy, and protection of learners' wellbeing and emotional development. A register of approved AI tools will be maintained.

6. Governance and Review

The proprietor has overall responsibility for AI-related safeguarding risks and for ensuring that the Independent School Standards and KCSIE 2026 are met. The proprietor approves this policy, oversees the approval of AI tools, ensures policy links are maintained, and receives regular assurance from the Designated Safeguarding Lead and senior leadership that staff training, reporting routes, filtering and monitoring, and data protection checks are effective. This policy is reviewed annually and after any significant AI-related incident.

7. Staff Training and Awareness

All staff receive safeguarding and online safety training at induction and at regular intervals that includes AI-related risks. Training covers how to recognise AI-generated or manipulated content, how to respond to disclosures or concerns, how to escalate incidents, and how AI links to child-on-child abuse, harmful sexual behaviour, bullying, grooming, misinformation and data protection. Training records are kept.

8. Online Safety, Filtering and Monitoring

AI tools and AI-generated content are included in BT&E's online safety arrangements and meet the Department for Education's filtering and monitoring standards. The named senior leader responsible for filtering and monitoring is [Name/Role]. The effectiveness of filtering and monitoring is reviewed at least once every academic year. The review is led by this senior leader and supported by the Designated Safeguarding Lead and IT support. Each review, the risks identified and the actions taken are recorded and reported to the proprietor.

9. Responding to AI-Related Safeguarding Incidents

- All AI-related concerns are reported immediately to the Designated Safeguarding Lead and recorded on the school's safeguarding recording system.
- AI-generated sexual images or videos of children are child sexual abuse material and are illegal, even when they are wholly or partly computer-generated. Staff must not view, copy, print, forward or save such content, and must not ask learners to send or show it. Incidents are managed in line with the UKCIS guidance on sharing nudes and semi-nudes, with referral to the police and children's social care where required.
- Incidents involving learners are also managed under the Behaviour and Anti-Bullying Policies, with support for both the child who has been harmed and the child who has caused harm.
- Concerns about a member of staff or adult misusing AI are reported to the Headteacher (or to the proprietor if the concern is about the Headteacher) and managed under the procedures for allegations and low-level concerns, including referral to the Local Authority Designated Officer (LADO) where required.

10. Teaching Learners About AI Risks

Learners are taught, in age-appropriate ways and through the online safety curriculum and relationships, sex and health education (RSHE), how to use AI safely and critically. This includes recognising misinformation and manipulated or deepfake content, understanding the risks of AI chatbots and "companion" apps, protecting their personal information, understanding consent and the law around creating and sharing images, and knowing how and where to report concerns.

11. Fairness & Inclusion

- All students should have equal access to learning tools.
- The school will provide supervised access or alternatives if needed.
- AI can assist students with additional learning needs where appropriate.
- Reasonable adjustments and supervised alternatives should be available where AI tools support accessibility or additional needs, while ensuring that use remains safe, proportionate, transparent and compliant with data protection requirements.

12. Parents & Guardians

We encourage you to:

- Talk to your child about safe and honest AI use.
- Ask teachers if you're unsure how AI is used in class.
- Read the information we provide about any tools that may need limited data sharing and complete consent forms where we ask for them.
- Be informed where AI tools are used in ways that may involve student accounts, personal data, images, voice, work samples or other identifiable information, and be told how consent, privacy and safeguarding concerns will be managed.

13. Contact

For questions or concerns, contact:

Designated Safeguarding Lead: [Name] – [Email] – [Phone]

Deputy Designated Safeguarding Lead(s): [Name(s)]

AI/Data Protection Lead: [Name]

Email: [School contact]

Phone: [Number]

Safeguarding concerns about AI use must be reported to the Designated Safeguarding Lead immediately. Data protection or tool approval questions must be referred to the AI/Data Protection Lead before any new AI tool is used with learners or learner information.

Our goal is to prepare students for a future where AI is part of everyday life — safely, ethically, and with integrity.