BORDEN GRAMMAR SCHOOL

AI Policy

Review Responsibility:	AI Lead
Frequency of Review:	1 year
Date Approved:	Sep 25
Approved By:	Board of Trustees
Next Review Due By:	Sep 26

Contents

1. Aims & Scope

Here at Borden Grammar School we understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. For example, it can be used to enhance pedagogical methods, customise learning experiences and progress educational innovation.

We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations.

Therefore, the aim of this policy is to establish guidelines for the ethical, secure and responsible use of AI technologies across our whole school community.

This policy covers the use of AI tools by school staff, trustees and pupils. This includes generative chatbots such as ChatGPT and Google Gemini (please note, this list is not exhaustive).

This policy aims to:
- Support the use of AI to enhance teaching and learning
- Support staff to explore AI solutions to improve efficiency and reduce workload
- Prepare staff, trustees and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Ensure that AI technologies are used ethically and responsibly by all staff, trustees and pupils
- Protect the privacy and personal data of staff, trustees and pupils in compliance with the UK GDPR

1.1 Definitions

This policy refers to both 'open' and 'closed' generative AI tools. These are defined as follows:
- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- **Closed generative AI tools** are generally more secure, as external parties cannot access the data you input

2. Legislation

This policy reflects good practice guidelines/recommendations in the following publications:
- [AI regulation white paper](#), published by the Department for Science, Innovation and Technology, and the Office for Artificial Intelligence
- [Generative artificial intelligence (AI) and data protection in schools](#), published by the Department for Education (DfE)
- [ICO guidance in relation to AI](#)

This policy also meets the requirements of the:
- UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020](#)
- [Data Protection Act 2018 (DPA 2018)](#)
- [Data (Use and Access) Act 2025](#)
- [Keep Children Safe in Education 2025](#)

3. Regulatory Principles

We follow the 5 principles set out in the [AI regulation white paper](#).

REGULATORY PRINCIPLE	WE WILL …
Safety, security and robustness	● Put measures into place to help ensure that AI solutions are secure and safe for users and protect users' data ● Put measures in place to help ensure we can identify and rectify bias or error through professional judgement ● Anticipate threats such as hacking
Appropriate transparency and explainability	● Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	● We will aim to use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate
Accountability and governance	● Ensure that the trust board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	● Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology ● Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

4. Roles & Responsibilities

4.0 AI Lead
Our generative AI lead is The Head of Computing. They are responsible for the day-to-day leadership, ownership and management of AI use in the school in their role as the Head of Computing. The Headteacher is responsible for agreeing the use of new AI tools and softwares, taking advice from the AI Lead.

4.1 Trust Board

The trust board will:
- Take overall responsibility for monitoring this policy and holding the headteacher to account for its implementation in line with the school's AI strategy
- Ensure the headteacher and/or AI lead is/are appropriately supported to make informed decisions regarding the effective and ethical use of AI in the school
- Adhere to the guidelines below to protect data when using generative AI tools:
  - Use only approved AI tools (see section 5 and appendix 1)
  - Seek advice from the data protection officer / AI lead and the designated safeguarding lead, as appropriate
  - Check whether they are using an open or closed generative AI tool
  - Ensure there is no identifiable information included in what they put into open generative AI tools
  - Acknowledge or reference the use of generative AI in their work
  - Fact-check results to make sure the information is accurate

4.2 Headteacher

The headteacher will:
- Liaise with the data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation
- Liaise with the DSL to ensure that the use of AI is in accordance with Keeping Children Safe in Education and the school's child protection and safeguarding policy
- Ensure that the guidance set out in this policy is followed by all staff
- Arrange the reviewing and update this AI policy as appropriate, and at least annually
- Ensure staff are appropriately trained in the effective use and potential risks of AI
- Make sure pupils are taught about the effective use and potential risks of AI
- Sign off on approved uses of AI, or new AI tools, taking into account advice from the DPO Coordinator, AI, and data protection impact assessments

4.3 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

Our DPO is Invicta Law and is contactable via email: dpo@invicta.law. Our DP Coordinator is contactable via dpcoord@bordengrammar.kent.sch.uk .

4.4 Designated Safeguarding Lead (DSL)

The DSL is responsible for monitoring and advising on our compliance with safeguarding requirements including in relation to the use of AI, such as:
- Being aware of new and emerging safeguarding threats posed by AI
- Updating and delivering staff training on AI safeguarding threats
- Responding to safeguarding incidents in line with Keeping Children Safe in Education (KCSIE) and the school's child protection and safeguarding policy
- Understanding the filtering and monitoring systems and processes in place on school devices

The school's DSL is contactable via safeguarding@bordengrammar.kent.sch.uk

4.5 All Staff

As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must

follow the guidelines set out in this policy. Parents should be aware that staff will use AI to support some administrative tasks that do not share sensitive data such as letter writing.

To protect data when using generative AI tools, staff must:

- Use only approved AI tools (see section 5 and appendix 1)
- Seek advice from the data protection officer / IT / AI lead, as appropriate
- Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy
- Check whether they are using an open or closed generative AI tool, as a school we should only be using the approved AI tools listed in Appendix 1.
- Ensure there is no identifiable information included in what they put into any generative AI tools, even if you believe it is a closed AI system.
- Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

4.6 Pupils

Pupils must:

- Follow the guidelines set out in section 7 of this policy ('Use of AI by pupils')

4.7 Parents/ Carers

The policy will be shared with parents via the school website. They should be aware that staff will use AI to support some administrative tasks that do not share sensitive data such as letter writing.

5. Staff and Trustees' Use of AI

5.1 Approved Use of AI

We are committed to helping staff and trustees reduce their workload. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert.

Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it.

Any member of staff or trustee using an AI-generated plan, policy or document should only share the AI-generated content with other members of the school community for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Always consider whether AI is the right tool to use. Just because the school has approved its use doesn't mean it will always be appropriate.

Given how rapidly AI is evolving, we would ask staff to contact the DPO Coordinator and AI Lead as and when you come across a new AI tool that you'd like to approve in our school so a DPIA (Data Protection Impact Assessment) can be carried out. The approved list of AI tools and software in school is listed in appendix A.

5.2 Process for Approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. Staff should contact the AI lead initially to discuss any ideas they may have with regards to using AI, so the AI Lead can take the suggestions forward if they deem it to be a satisfactory new method of working.

The headteacher is responsible for signing off on approved uses of AI, or new AI tools, taking into account advice from the AI Lead, the DPO Coordinator and data protection impact assessments.

5.3 Data Protection and Privacy

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into any generative AI tools or chatbots.

If personal and/or sensitive data is entered into any generative AI tool, Borden Grammar School will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy. Please also refer to section 10 of this policy.

5.4 Intellectual Property

Most generative AI tools use inputs submitted by users to train and refine their models.

Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice answers..

Pupils' work must not be used by staff to train generative AI models without appropriate consent or exemption to copyright.

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

5.5 Bias

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output.

We will ensure we can identify and rectify bias or error by training staff in this area.

We also regularly review our use of AI to identify and correct any biases that may arise.

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

5.6 Raising Concerns

We encourage staff and trustees to speak to the headteacher in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

Safeguarding concerns arising from the use of generative AI must be reported immediately to the DSL in accordance with our school's child protection and safeguarding policy.

5.7 Ethical and Responsible Use

We will always:
- Use generative AI tools ethically and responsibly
- Remember the principles set out in our school's equality policy when using generative AI tools
- Consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- Fact and sense-check the output before relying on it

Staff and trustees must not:
- Generate content to impersonate, bully or harass another person
- Generate explicit or offensive content
- Input offensive, discriminatory or inappropriate content as a prompt
- Or in any way that may breach the staff code of conduct

6. Educating Pupils About AI

Here at Borden Grammar School we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI. Students will be taught about:
- Creating and using digital content safely and responsibly
- The limitations, reliability and potential bias of generative AI
- How information on the internet is organised and ranked
- Online safety to protect against harmful or misleading content
- How to use prompts effectively to get the best results with AI tools
- How to use AI responsibly, in line with our behaviour policy and acceptable use policy

7. Use of AI by Pupils

We recognise that AI has many uses to help pupils learn.
Pupils may use AI tools:
- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs.

AI may also lend itself to cheating and plagiarism. To mitigate this, pupils **may not use** AI tools:
- During assessments, including internal and external assessments, and coursework
- To write their homework or class assignments, where AI-generated text is presented as their own work
- To complete their homework, where AI is used to answer questions set and is presented as their own work (for example, maths calculations)

This list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

We consider any unattributed use of AI-generated text or imagery to be plagiarism and will follow our plagiarism procedures.

Pupils must consider what is ethical and appropriate in their use of AI and must not:
- Generate content to impersonate, bully or harass another person
- Generate or share explicit or offensive content, including, but not limited to, generating inappropriate or sexualised images of pupils
- Input offensive, discriminatory or inappropriate content as a prompt

8. Formal Assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.
We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on AI use in assessments.

9. Staff Training

At Borden Grammar School we will use CPD and whole staff training time to train staff in the appropriate, safe and ethical uses of AI within teaching. This will include personal CPD time and whole school training. Important updates to AI will be shared during weekly staff briefings, email updates, meetings and during whole school training.

Teaching and Learning CPD time will be, in part, used to share best practice on how AI can be used to reduce staff workload. Safeguarding training time will include important updates regarding the safe use of AI and potential risks and there will be some compulsory individual CPD time for online courses and updates.

A working group made up of teaching and support staff will be formed to share best practice, ideas and research periodically throughout the year.

10. Referral to our Child Protection and Safeguarding Policy

The school is aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:
- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse/exploitation material
- Harmful content
- Harmful advertisements and promotions
- Bullying

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately.

Any such incident will be dealt with according to the procedures set out in the school's child protection and safeguarding policy and child protection referral process.

11. Breach of this Policy

11.1 By Staff
Breach of this policy by staff will be dealt with in line with our staff code of conduct.
Where disciplinary action is appropriate, it may be taken whether the breach occurs:
- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:
- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

You must report any breach of this policy, either by you or by another member of staff, to the headteacher immediately.

11.2 By Trustees

Breach of this policy by a trustee will be dealt with by the Board of Trustees in line with our Trustee Code of Conduct or complaints policy. This process will also involve the school's Data Protection Officer (DPO) if personal data was compromised, as they provide critical expertise on legal compliance and reporting requirements. The Headteacher will assess the operational impact of the breach on the school community.

11.3 By Pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour policy and we may involve other external agencies, e.g. police or social care, if we believe a breach of this policy may involve material of a criminal nature.

12. Monitoring & Transparency

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, this policy is a live document that must be kept updated by the AI lead whenever there is a significant change to either AI use by the school or the associated risks of AI usage.
This policy will also be regularly reviewed and updated to align with emerging best practices, technological advancements and changes in regulations.
The policy will be shared with the full governing board at least annually.
All teaching and support staff are expected to read and follow this policy.
The AI Lead will monitor the effectiveness of AI usage across the school.
We will ensure we keep members of the school community up to date on the use of AI technologies for educational purposes through the updates to this policy. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use in school.

13. Links with Other Policies

This AI policy is linked to our:
● Data protection policy
● Safeguarding/child protection policy
● Exams and assessment policies
● Behaviour policy
● Staff code of conduct
● Acceptable use policy
● Online safety policy
● Equality policy

Appendix 1: Approved Uses of AI Tools

Note that open-source AI tools / open AI tools, meaning tools that anyone can access and modify, should only be used for tasks that don't require personal information to be input.

Approved AI tools	approved for	Approved uses
KeyGPT	● Teachers ● Trustees ● Support Staff	● Letter to parents/carers ● Job descriptions and adverts ● Interview questions
Chat GPT PLEASE NOTE- We suggest that you alter the setting to not allow information to be used to train the AI software, thus improving the security of this software	Teachers Trustees Support Staff	Letter writing Checking and improving written content (providing there is no identifiable information included) Creating lesson plans Creating adaptive teaching resources Creating images Drafting policies Creating lesson resources
Gemini Google AI Overview	Teachers Trustees Support Staff	Letter writing Checking and improving written content (providing there is no identifiable information included) Creating lesson plans Creating adaptive teaching resources Creating images Drafting policies Creating lesson resources
Arbor	Teachers Support Staff Students	Suggested student overviews Suggested SMS/ Email messages Suggested formulas Generating reports
Canva	Teachers Support Staff Students	Creating documents/ posters Creating images Creating lesson resources
Adobe	Teachers Support Staff Students	Creating images Graphic design
Turn it in	Teachers Students	Checking plagiarism of students work

Approved AI tools	approved for	Approved uses
Seneca	Teachers Students	Revision content Exam practice questions
UniFrog	Teachers Students Support Staff	

Appendix 2: DPIA Template

This template is an example from the ICO and can be used to record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the [Criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject	
Name of controller contact	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm *Remote, possible or probable*	Severity of harm *Minimal, significant or severe*	Overall risk *Low, medium or high*
1.			
2.			
3.			
4.			
5.			

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk *Eliminated / reduced / accepted*	Residual risk *Low medium high*	Measure approved *Yes / No*
1.				
2.				
3.				
4.				
5.				

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		*Integrate actions back into project plan, with date and responsibility for completion*
Residual risks approved by:		*If accepting any residual high risk, consult the ICO before going ahead*
DPO advice provided:		*DPO should advise on compliance, step 6 measures and whether processing can proceed*
Summary of DPO advice:		
DPO advice accepted or overruled by:		*If overruled, you must explain your reasons*
Comments:		
Consultation responses reviewed by:		*If your decision departs from individuals' views, you must explain your reasons*
Comments:		
This DPIA will kept under review by:		