



AI Policy (Artificial Intelligence)

Review Responsibility: AI Lead

Frequency of Review: 1 year

Date Approved: Sep 26

Approved By: Board of Trustees – Curriculum & Learning Committee

Next Review Due By: Sep 27

Contents

1. Aims & Scope	3
1.1 Definitions	3
2. Legislation	3
3. Regulatory Principles	4
4. Roles & Responsibilities	5
4.0 AI Lead	5
4.1 Trust Board	5
4.2 Headteacher	5
4.3 Data Protection Officer (DPO)	5
4.4 Designated Safeguarding Lead (DSL)	5
4.5 All Staff	6
4.6 Pupils	6
4.7 Parents/ Carers	6
5. Staff and Trustees' Use of AI	6
5.1 Approved Use of AI	6
5.2 Process for Approval	7
5.3 Data Protection and Privacy	7
5.4 Intellectual Property	7
5.5 Bias	7
5.6 Raising Concerns	7
5.7 Ethical and Responsible Use	7
6. Educating Pupils About AI	8
7. Use of AI by Pupils	8
8. Formal Assessments	9
9. Staff Training	9
10. Referral to our Child Protection and Safeguarding Policy	9
11. Breach of this Policy	9
11.1 By Staff	10
11.2 By Trustees	10
11.3 By Pupils	10
12. Monitoring & Transparency	10
13. Links with Other Policies	10
Appendix 1: Approved Uses of AI Tools	12
Appendix 2: DPIA Template	14

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 also applies where AI functionality is embedded within another platform, application, browser, search tool or school system, whether or not the user is directly interacting with a chatbot.

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

For the purposes of this policy, AI tools are distinguished by how they are approved, managed and how they process school data, rather than by the terms “open” and “closed”.

- Public/consumer AI tools are services accessed through a public or personal account where the school does not have a contract or other controls governing how school data is processed. Personal, special category, confidential or otherwise identifiable school information must not be entered into these tools.
- School-approved managed AI tools are tools or specific account/tenant configurations approved for defined uses following appropriate data protection, safeguarding and IT/security review. Approval of a tool does not automatically approve every feature or every use of that tool.
- Automated decision-making means a decision made using automated processing. The school will not use AI as the sole basis for decisions that have a legal or similarly significant effect on a pupil, parent/carers, member of staff or applicant.
- Learner-facing AI means any AI feature that pupils can access directly or that generates personalised content or recommendations about a pupil.

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](#)
- DfE Generative artificial intelligence (AI) in education guidance
- DfE Generative AI: product safety standards (updated January 2026)
- DfE Using AI in education settings: support materials (updated for 2026 to 2027)

- DfE Data protection in schools guidance, including Generative AI and data protection and Procuring educational technology (EdTech)
- DfE Meeting digital and technology standards in schools and colleges: Filtering and monitoring core standard
- Joint Council for Qualifications (JCQ) guidance on AI use in assessments and the current coursework/non-examination assessment instructions

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](#)
- Equality Act 2010, including the Public Sector Equality Duty
- [Keep Children Safe in Education 2026](#)

3. Regulatory Principles

Our governance of AI is informed by the five cross-sector principles set out in the UK AI regulation white paper. These principles are applied alongside the school's statutory duties and current DfE, ICO, Ofqual and JCQ guidance.

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

REGULATORY PRINCIPLE	WE WILL ...
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. The Headteacher is responsible for approving new AI tools and uses, taking advice from the AI Lead. DPO/DP Coordinator, DSL and IT/security lead as appropriate. The AI Lead will maintain an AI Register recording approved tools, approved use cases, users, relevant risk/DPIA status, safeguards, owner and review date.

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 the tool and the specific intended use are approved and whether it is a public/consumer tool or a school-approved managed tool
 - Ensure there is no personal, special category, confidential or otherwise identifiable school information entered into public/consumer AI tools
 - Acknowledge or reference the use of generative AI in their work
 - Fact-check results to make sure the information is accurate
- Ensure a named trustee receives assurance about the school's filtering and monitoring provision in line with DfE standards. The named trustee as delegated by the Board of Trustees will be the trustee linked with Safeguarding.
- Receive assurance that filtering and monitoring arrangements take account of generative AI and that learner-facing AI tools have been assessed against relevant DfE product safety standards.

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 approved uses of AI and new AI tools, taking into account advice from the AI Lead, DPO/DP Coordinator, DSL and IT/security lead, together with the outcome of any DPIA screening, DPIA or other risk assessment required.

4.3 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law in relation to AI, including lawful basis, transparency, DPIAs, processor/controller roles, international transfers, retention, data subject rights and any profiling or automated decision-making.

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 and reviewing the filtering and monitoring systems and processes in place, including whether they adequately address dynamic, personalised and AI generated content and any learner-facing AI products.

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
- Use only the tools, account types, features and use cases approved by the school and recorded in Appendix 1 and/or the AI Register.
- Never enter personal, special category, confidential or otherwise identifiable school information into a public/consumer AI tool. Personal data may only be processed in a school-approved managed tool where that specific use has been authorised and the required data protection safeguards are in place.
- Fact-check results to make sure the information is accurate
- Check AI generated communications, reports, feedback and resources before they are shared or acted upon. AI must not independently send communications or make decisions on behalf of a member of staff.

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. The school will be transparent about material uses of AI, including how personal data is processed where relevant. Staff may use approved AI to support appropriate administrative and educational tasks, but staff remain responsible for the final content and decisions.

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.

AI must not be used as the sole basis for a significant decision about a pupil, parent/carers, member of staff or applicant. Meaningful human review and professional judgement must be retained.

Approval is use-case and configuration specific. A tool appearing in Appendix 1 does not mean that all of its current or future AI features are approved.

Given how rapidly AI is evolving, staff must contact the AI Lead before using a new AI tool or a materially new AI feature for school purposes. The AI Lead will coordinate proportionate screening with the DPO/DP Coordinator, DSL and IT/security lead. A full Data Protection Impact Assessment (DPIA) will be completed where required or judged proportionate. Approved tools and use cases are listed in Appendix 1 and maintained in the AI Register.

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 approved AI tools and use cases. Before approval, the school will consider the intended users and educational purpose; age restrictions; safeguarding and filtering/monitoring; data flows and lawful basis; model training/product improvement; supplier and sub-processors; retention and deletion; international transfers; security and access controls; intellectual property; bias/equality; automated decision-making/profiling; and whether a DPIA is required. Approval and review dates will be recorded in the AI Register.

5.3 Data Protection and Privacy

Personal, special category, confidential or otherwise identifiable information must not be entered into public/consumer generative AI tools. Personal data may only be processed using a school-approved managed

AI tool where the specific use is authorised, a lawful basis and appropriate contractual/security safeguards are in place, and a DPIA has been completed where required.

Any unauthorised disclosure or processing of personal data through an AI tool will be assessed under the school's personal data breach procedure and reported promptly to the DPO/DP Coordinator. Where the incident also raises a safeguarding concern, it must be reported immediately to the DSL. Please also refer to section 10 of this policy.

Where AI is used to support profiling or recommendations about individuals, the DPO must be consulted and meaningful human oversight must be maintained.

The school's privacy information will reflect relevant AI processing. Data minimisation must be applied and personal data must not be used to train or improve an AI model unless the school has explicitly assessed and authorised that processing.

Photographs, video, audio recordings, pupil work and free-text case information can contain personal or special category data and must be treated in the same way as other personal information.

5.4 Intellectual Property

Some generative AI tools use user inputs to train, fine-tune or improve models or products; others provide settings or contractual terms that restrict this. Staff must not assume that inputs are private or excluded from training and must follow the conditions recorded for the approved tool.

Pupils may own copyright in the original work they create, subject to the normal requirements of copyright law. Staff-created materials may also be protected by copyright, with ownership depending on the circumstances in which they were created.

Pupil or staff work must not be uploaded or used for model training, fine-tuning or product improvement unless the copyright position and any required permission have been established and the data protection implications have also been approved.

AI generated output must be checked for possible copyright infringement and should not be assumed to be original, accurate or safe to publish simply because it was generated by an approved tool.

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 or amplify bias, including in relation to protected characteristics, SEND, language and other factors. The school will have due regard to the Equality Act 2010 and Public Sector Equality Duty. Critical thought and human review must be applied to AI outputs, particularly where they could affect access, support, behaviour, assessment, recruitment or other opportunities.

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.

Data protection concerns or complaints about how personal data has been processed through AI should be raised with the DPO/DP Coordinator in line with the school's data protection complaints procedure.

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
- Be transparent where AI has materially contributed to content or a process and acknowledgement is required by this policy, an assessment rule or another school policy.
- Maintain meaningful human oversight and be able to explain and justify any decision or professional judgement informed by AI.

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
- Upload school passwords, authentication codes, confidential security information or other credentials to an AI tool.
- Use AI to fabricate evidence, records, references, safeguarding information or the identity/voice/image of a real person in a misleading way.

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
- How AI can create convincing false information, synthetic media and deepfakes, and how to question provenance and verify sources
- How personal information, photographs, voice recordings and other data may be collected or reused by AI services, and how to protect privacy
- Intellectual property, authorship, acknowledgement and the difference between using AI as a source or support and presenting AI output as their own work
- Age restrictions, safety controls and why pupils must only use school-approved AI tools in the ways authorised by staff

7. Use of AI by Pupils

We recognise that AI has many uses to help pupils learn.

Pupils may use school-approved AI tools when the teacher has made clear that AI use is permitted for the task and the pupil follows the stated conditions:

- 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

Any pupil-facing AI use must comply with the tool's age restrictions and the school's safeguarding, filtering and monitoring arrangements. Pupils must not enter personal, special category, confidential or otherwise identifiable information into public/consumer AI tools.

AI can support learning but can also undermine independent thinking and the authenticity of pupils' work. Teachers will make clear whether AI is prohibited, permitted with conditions or encouraged for a particular task. Pupils must follow that instruction.

- In examinations and controlled assessments unless the relevant rules expressly permit it. For coursework, non-examination assessments and other qualification work, pupils must follow the current JCQ/awarding organisation rules and the teacher's instructions. Permitted use of AI as a source must be acknowledged and the submitted work must remain the pupil's own independent work.
- 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 must acknowledge their use in the format required by the teacher, JCQ or awarding organisation. For qualification work this should include the name of the AI tool and the date the content was generated, and a copy of the generated content must be retained/submitted where required for authentication.

Unacknowledged or inappropriate use of AI may constitute plagiarism, academic misconduct or examination malpractice depending on the context. The school will follow its behaviour, plagiarism/malpractice and assessment procedures as applicable.

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, alter or share explicit sexualised or otherwise harmful content, including AI generated or manipulated intimate images/deepfakes of pupils or other people
- 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](#).

For qualification assessments, work accepted for assessment must be the pupil's own. AI misuse can constitute malpractice and may lead to serious sanctions.

Teachers must follow current JCQ and awarding organisation requirements for supervision, authentication, acknowledgement and retention of AI generated content used as a source.

AI must not be used as the sole or primary means of marking candidates' work. Teachers must review the work in its entirety, apply the published marking criteria and remain responsible for the mark awarded.

AI detection or plagiarism indicators may inform professional enquiry but must not, on their own, be treated as conclusive evidence of misconduct.

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.

Core training will include data protection and secure use, safeguarding and emerging AI harms, filtering/monitoring, bias and equality, intellectual property, assessment malpractice, human oversight, age restrictions and the safe use of school-approved tools. Training will be refreshed when significant risks or product changes arise.

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 material (CSAM), including AI generated or AI manipulated material
- Harmful content
- Harmful advertisements and promotions
- Bullying
- Non-consensual intimate imagery, nudification and sexualised deepfakes
- Impersonation, synthetic voice/image/video and deceptive or coercive AI interactions
- AI generated content that promotes self-harm, suicide, eating disorders, extremism, violence or other harmful behaviour
- Inappropriate relationships with or over-reliance on AI chatbots where this creates a safeguarding or wellbeing concern

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.

The school will consider AI generated and dynamic content when reviewing filtering and monitoring provision and will review those arrangements when a new learner-facing AI tool is introduced or materially changed.

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)

- Relevant audit logs, records, school-managed account information or devices where access is lawful and proportionate under school procedures. Staff must never disclose passwords or authentication codes to another person.

You must report any suspected breach of this policy promptly to the appropriate person: the Headteacher/Al Lead for general policy breaches, the DPO/DP Coordinator for data protection incidents, and the DSL immediately for safeguarding concerns.

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 reviewed through the school's agreed governance route at least annually and whenever there is a material change in law, guidance, approved AI use or risk.

All teaching and support staff are expected to read and follow this policy.

The AI Lead will monitor the effectiveness and risk of AI usage across the school, maintain the AI Register and coordinate an annual audit of approved tools, use cases, incidents, training and required actions.

We will keep members of the school community appropriately informed about AI use through this policy, relevant privacy information and guidance for staff, pupils and parents/carers. Feedback, complaints, incidents and equality/safeguarding impacts will be considered in the ongoing evaluation of AI use in school.

13. Links with Other Policies

This AI policy is linked to our:

- Acceptable Use Policy
- Behaviour Policy
- Curriculum Policy
- Equality Objectives & Policy
- Exams & Assessment Policies
- GDPR UK & Data Protection Policy & Privacy Notices
- Online Safety Policy
- Safeguarding & Child Protection Policy
- Staff Code of Conduct

Appendix 1: Approved Uses of AI Tools

Approval applies to the specific tool, account/tenant configuration, feature and use case recorded by the school. Public/consumer AI tools must not be used with personal, special category, confidential or identifiable school information. Learner-facing use must meet age, safeguarding, filtering/monitoring and product-safety requirements.

Approved AI tools	approved for	Approved uses
KeyGPT	• Teachers • Trustees • Support Staff	• Letter to parents/carers • Job descriptions and adverts • Interview questions
ChatGPT Use only in the school-approved configuration and for the approved use cases. Disabling model training/product improvement is an additional safeguard where available, but it does not replace data minimisation, approval or the prohibition on entering unauthorised personal/confidential data.	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 Approval must identify the exact Google/Gemini service and school account/tenant configuration; approval of one Google AI feature does not approve all current or future AI features.	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

Approved AI tools	approved for	Approved uses
Adobe	Teachers Support Staff Students	Creating images Graphic design
WinstonAI	Teachers Students	Checking plagiarism of students work
Seneca	Teachers Students	Revision content Exam practice questions
UniFrog	Teachers Students Support Staff	Refine writing Prepare for interview Structure applications

Any AI enabled feature is subject to the school's specific approval, age restrictions, safeguarding, filtering/monitoring and data-protection controls.

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 <i>Remote, possible or probable</i>	Severity of harm <i>Minimal, significant or severe</i>	Overall risk <i>Low, medium or high</i>
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 <i>Eliminated / reduced / accepted</i>	Residual risk <i>Low medium high</i>	Measure approved <i>Yes / No</i>
1.				
2.				
3.				
4.				
5.				

Step 7: Sign off and record outcomes

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