Stebbing Primary

Generative Artificial Intelligence Policy

Document Control

Version:	2025
Date approved:	NOVEMBER 2025
Approved by:	FULL GOVERNING BODY
Next review:	2026

When using generative Artificial Intelligence (AI) it is important that our school ensures we are able to maximise the benefits of AI while minimising any risks or concerns.

This policy sets out the rules all employees, governors, voluntary workers, agency staff, contractors, and other third parties working on behalf of the school **must** follow when using generative AI on our Trust or school devices or networks.

Policy rules

1. You must only use AI applications authorised by our school.

2. You must select the opt-out option before first use of authorised AI applications. This will prevent the data you enter into the prompt being used by the Large Language Model (LLM) to train itself. If the opt out selection is unclear or is not available on the authorised AI application, please contact the school Data Protection Lead for further clarification.

3. When using any of the authorised AI applications, you must use your work email address for log-in purposes.

4. Before using an AI application you must have authorisation from the schools Data Protection Lead.

5. When using AI applications you must ensure that confidential, sensitive, or proprietary employee, student, parent/carer or third-party supplier, including personal data or sensitive data, is **not** entered into the application as a prompt in breach of data protection legislation.

6. If your use of AI applications will involve any personally identifiable data you **must** complete a Data Protection Impact Assessment (DPIA) and where necessary an Equalities Comprehensive Impact Assessment (ECIA), both approved by the school prior to any use.

7. If your use of AI applications will involve any personally identifiable data you must ensure that your privacy notices explain your use of AI and explain how AI decisions are made

8. You must be aware of, and comply with, any intellectual property rights (IPR) or licencing conditions and include referencing of your sources when using AI tools.

9. You must not input offensive, discriminatory or inappropriate content as a prompt.

10. You must comply with our Information Security and Data Protection Policies when using AI applications or any other technologies.

11. You must carefully review any AI outputs to guard against bias, inappropriate or offensive data.

12. You must not generate content to impersonate, bully, or harass another person, or to generate explicit or offensive content.

Why must I comply with these policy rules?

These policy rules will help us to comply with the law and regulatory guidance when using artificial intelligence. The use of generative artificial intelligence (generative AI) is transforming the way individuals are working. Informed and responsible use of generative AI has the potential to increase efficiency in the workplace, improve decision making and foster innovation. With these benefits come potential risks, including data protection breaches, copyright issues, the protection of confidential information, ethical considerations and compliance with wider legal obligations. AI systems learn based on the information you enter. Just as you would not share work documents on social media sites, do not input such material into generative AI tools.

Common Generative AI types

Rule-based AI - The AI follows specific rules and guidelines to make decisions or generate language. Very specific AI tools are used in healthcare, finance, customer services, and other industries. These are used in disease detection, drug development, fraud detection and investment monitoring.

Machine learning AI - This type of AI can write reports, summarise documents and help you create policies. Over time, this AI gets better at predicting or making decisions based on the data it has seen. It's more flexible than rule-based AI but still has limitations and what it creates must be checked.

Deep learning AI - Deep learning AI can recognise patterns and make decisions with less explicit programming compared to traditional machine learning.

Natural Language Processing (NLP) AI - This AI specializes in understanding and generating human language. NLP AI can read text, understand it, generate responses, and sometimes even understand sentiment and context.

Reinforcement learning AI - This AI learns by trial and error, receiving rewards for good decisions and penalties for bad ones.

Image generating AI - This is AI can create images from text inputs for use in marketing and communications material.

Minute taking AI – There are AI tools which can be used to take minutes of meetings. These tools can become incredibly intrusive and hard to get rid of as they often invite themselves to meetings and take minutes of meetings which are not intended to be minuted.

Vision processing AI – Recognises faces and makes decisions based on who they see. Used in facial recognition solutions for access and safety.

Robotics AI – AI is integrated into physical machines and industrial robots, drones and autonomous vehicles.

Recommendation systems AI - It bases the recommendations on your activity and that of other people whom it sees as similar to you, e.g., chatbots.

The tools above are large language models (LLMs) and most can generate human like text in response to a prompt. They use deep learning techniques and massive data volumes to generate a response. LLMs can produce outputs which may initially appear to be believable but are in fact highly inaccurate or fabricated. This is known as a hallucination. AI needs personal data for training the LLM so it can mimic human behaviour, and lots of it to improve accuracy. Currently there are no reliable techniques for steering the behaviour of LLMs which are very complex to understand. This increases data protection risks as well as the risk of unconscious bias. AI applications must be used ethically and responsibly to avoid harm, reputational damage, unlawful processing and regulatory censure.

Governance

It is essential that we complete due diligence checks on any AI application the business are considering using to ensure it meets ethical and legal conditions, reducing risks for the business and individuals. AI platforms can involve collaboration between multiple parties or use third-party tools and services. This increases the risk of unauthorised access or misuse of personal data, especially when data is shared across jurisdictions with different privacy regulations.

You must always comply with our Code of Conduct and our Policies and consider the need to complete an Equalities Comprehensive Impact Assessments (ECIAs).

Security of information

Every employee is responsible for assuring the security of any processing by the school. AI can be misused for malicious purposes, such as automating cyberattacks or creating sophisticated phishing scams. Attackers can leverage AI to launch more targeted and efficient attacks, making it harder for traditional security measures to detect and mitigate them. You must be vigilant and ensure that all technical and organisational controls are complied with to fully protect the data.

Since generative AI models take unstructured prompts from users and generate new, possibly unseen responses, you need to protect personal or sensitive data in-line. Many known prompt-injection attacks have been seen in the wild. The main goal of these attacks is to manipulate the model into sharing unintended information.

Verifying outputs

Generative AI has the potential to produce inaccurate outputs or hallucinations. There is also a risk that the output is biased, inappropriate or otherwise offensive. This means that critical thought must be applied to all outputs of authorised AI applications; they must always be fact and sense checked before being relied upon for business purposes and reviewed to ensure content is appropriate. These tools can produce credible looking output. They can also offer different responses to the same question if it is posed more than once, and they may derive their answers from sources you would not trust in other contexts. Therefore, be aware of the potential for misinformation from these systems.

How must I comply with these policy rules?

You cannot use AI applications without first seeking and gaining written permission from the school Data Protection Lead. You must select the 'opt out' option, and if one is not available, seek advice from the school Data Protection Lead. You must fully comply with policy and guidance to protect data from cyber threats, reducing risks for individuals and the organisation. You must always use your work assigned email address to enable clarity that AI use has been approved by the business.

To assess the data protection risks of proposed uses of AI applications you must complete a DPIA. Any identified risks must be mitigated to an acceptable level before the DPIA can be approved and the use of AI commenced. Where AI involves the use of personal data you must be able to inform individuals of their data protection rights and how to exercise them. Your privacy notices must be clear if AI activities including the use of personal data. In addition, you should provide explanations to data subjects of the process, fairness, outcome and impact to reassure data subjects and enable and inform challenges. The ICO provide guidance on how to ensure you meet data subjects rights when using AI.

You must read and apply the DfE guidance for education sector on the use of generative artificial Intelligence.

Identify and abide by any relevant licensing conditions regarding intellectual property rights in the authorised AI application's terms of use and ensure that third party proprietary data or material is not entered into the application as a prompt without the third party's permission. This includes ensuring, for example, that all or any substantial part of any copyright work owned by a third party is not inputted into the application as a prompt without the third party's consent. Records of checks for copyright, or licencing information, must be evidenced. Whether using the outputs from generative AI either verbatim or with minor alterations, it is important to make clear to those reading that an AI tool has been used. To do this the tools should be cited in a footnote, with its URL and any sources used as inputs.

AI tools, such as a LLM, answer questions by choosing words from a series of options it classifies as plausible. These tools cannot understand context or bias. Always treat with caution the outputs these tools produce and challenge the outputs using your own knowledge and judgement. Outputs must always be fact and sense checked before being relied upon for business purposes and reviewed to ensure content is appropriate. Always apply the high standards of rigour you would to anything you produce, and reference where you have sourced output from in one of these tools.

Remember that under the UK GDPR data subjects have the right to object to automated decision making and profiling. You must make clear in your privacy notice that AI is being used, and that the data subject has the right to object, and how to do so. You must have processes in place to manage any objections

Always use authorised AI applications ethically and responsibly, taking into account our policies and research governance.

We reserve the right to monitor all content (including but not limited to any prompts, or outputs) on any generative AI application used for school purposes. This will only be carried out to the extent permitted by law, in order for us to comply with a legal obligation or for our legitimate business purposes, including but not limited to:

a) prevent misuse of the content and protect our confidential information (and the confidential information of our staff, students, parent/carers and suppliers);

b) ensure compliance with our rules, standards of conduct and policies;

c) monitor performance at work;

d) ensure that our workforce does not use our facilities or systems for any unlawful purposes or activities that may damage our school or reputation;

e) comply with legislation for the protection of intellectual property rights and to support proprietary rights in the output.

What if I need to do something against this policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school Data Protection Lead.

If you believe the policy does not meet your business needs, you may raise this with your school Data Protection Lead who, if they agree with your suggestion, may propose a policy change.

References

- Data Protection Act 2023/ UK GDPR
- The Intellectual Property Act 2014
- Human Rights Act 1998
- Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk)
- Data protection in schools - Generative artificial intelligence (AI) and data protection in schools - Guidance - GOV.UK
- Guidance on AI and data protection | ICO
- Our work on Artificial Intelligence | ICO
- ICO – Explaining Decisions made with AI
- NASUWT | Artificial Intelligence and Digital Technologies
- EU AI Act 2024
- ePrivacy legislation
- Education legislation
- Marketing legislation

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

