



DANE ROYD J&I SCHOOL

Artificial Intelligence Policy

Review frequency: Annually

**Approval by: Governing
Body**

**Date approved: 21st October
2026**

Policy date: October 2026

Review date: October 2027

Lead personnel: Mr Lee

Aims which guide our policies and practice at Dane Royd School



PERSEVERANCE

As a school, we aim to nurture an environment where children and staff achieve and thrive. We want to build strong foundations and a love of learning where every member of our school community feels they belong, can be, and become the very best version of themselves. We want our children to understand the rich heritage of the world; to be a positive member of their community and to become skilled citizens who have self-belief, passion and empathy for the world in which they live.

Our Agreed Strong Foundations are:



RESPECTFUL

- To create a school environment which nurtures and encourages a life-long love of learning.
- All members of the school community will live the school values. Through these values, we will equip our young people with the skills for life, to make them reflective, empathetic and open-minded members of the community.
- To provide vital enrichment activities to provide opportunities for our children to experience and thrive in.
- To teach the knowledge and skills to enable our young people to make informed decisions about their well-being, health and relationships to build their self-efficacy.
- To celebrate differences and diversity, and promote equity of opportunity so all can thrive together.
- To have high aspirations for all our young people. We want every child to succeed in their own way. Successful learning means enabling every individual – regardless of background, race, gender, disability, sexuality or socioeconomic status – to flourish in our school.
- To support pupils to become responsible, active citizens who can play their part in public life as young people and adults in modern Britain.
- We want our children and staff to be proud of their school. By following our school values, we will build a respectful, dynamic and inclusive school community where everyone's achievements are celebrated.



OPEN-MINDED



UNDERSTANDING



DETERMINED

We ensure that all of our policies and practices are guided by these aims and we seek to ensure that they are at the forefront of all that we do.

1. Policy Statement

Artificial Intelligence (AI) is increasingly being used across education to support teaching, learning, and administration. Dane Royd recognises the opportunities AI presents for enhancing efficiency and innovation. However, AI must be used in a safe, ethical, and responsible manner, ensuring compliance with safeguarding, data protection, and academic integrity principles. This policy sets out how Dane Royd uses artificial intelligence (AI): by whom, for what and within what limits, so its benefits are realised without compromising the safety of children and adults, data security and privacy, fairness, or professional and academic integrity. It forms part of the organisation's wider digital strategy and is reviewed annually and whenever law, guidance or the organisation's use of AI materially changes.

This policy sits within, and does not cut across, the wider framework that applies to the organisation. It should be read alongside:

This policy ensures compliance with:

- **Keeping Children Safe in Education 2026**, the statutory safeguarding baseline from 1 September 2026, which addresses AI within its four areas of online risk (section 9);
- the **UK GDPR** and the **Data Protection Act 2018**, each as amended by the Data (Use and Access) Act 2025, with ICO guidance on AI, the ICO AI and data protection risk toolkit and, wherever children's data is involved, the ICO Children's Code;
- the **Equality Act 2010** and, for public bodies, the **public sector equality duty**, which apply to AI-assisted activity as to everything else;
- the **DfE position on generative AI in education** and the **DfE generative AI product safety standards** (January 2026);
- the DfE **filtering and monitoring, cyber security** and **digital leadership and governance** standards;
- the **Online Safety Act 2023** and the **Ofcom Protection of Children code of practice**;
- the **Prevent duty guidance** for England and Wales (2023) and **Working Together to Safeguard Children 2026**;
- the financial governance framework that applies the local authority's **scheme for financing schools** and the **Schools Financial Value Standard** for maintained schools; and
- Dane Royd's **Acceptable Use Policy (AUP)**, **Online Safety Policy**, and **Data Protection Policy**

2. Who and what this policy covers

In this policy, AI means generative AI tools and any software feature that creates content, or that makes or informs decisions or predictions about people, whether standalone, built into approved software, or reached through a browser. In practice that means chatbots, image and content generators, and AI features inside everyday software. Long-established automation such as spellcheck or predictive text is out of scope unless it does either of those things.

AI on a personal or wearable device is still in scope. AI reached through a personal device, including wearables such as smart glasses and other recording-capable devices, is covered by this policy whenever it is used in connection with the work of the organisation. Whether such devices may be brought onto the site at all, and the rules on recording, sit in Dane Royd's Mobile Devices Policy; capturing images, audio or video of others without their

knowledge engages data protection law and, where children are involved, safeguarding (section 9).

Pupils are not within the scope of this policy. In no circumstances may AI be used in a way that undermines the safety or wellbeing of children or adults, the privacy of their data, fairness, the Prevent duty, or the integrity of assessment.

3. Roles, responsibilities and oversight

Role	What this role owns	Named owner
Trustees / governing board	Strategic oversight and assurance; ensures AI appears on the organisation's risk register; receives termly reporting covering adoption, incidents, breaches and changes to the approved list.	School Governors
Headteacher	Accountable for AI use in their setting; ensure staff are trained; model human-led use.	Miss C Kelly
Senior leadership	Approves this policy and material changes; approves tool additions where named as approver under section 4.2; commissions the periodic AI risk review.	Miss C Kelly, Mr J Davison, Mrs G Kendall
AI / digital lead	Owns the approved list and approval gate; keeps this policy and staff guidance current; first contact for queries.	Mr M Lee
Data protection officer / lead	Coordinates impact assessments; advises on lawful basis and processing agreements; receives reports of data entered in error.	Mrs E Wake
Designated safeguarding leads	Receive safeguarding and Prevent concerns involving AI; advises on safeguarding implications of proposed uses	Miss C Kelly, Mrs G Kendall, Miss B Ellam, Mr M Lee, Mrs C Ward

Filtering and monitoring leads	Senior named owner of filtering and monitoring arrangements (section 12).	Eduthing
IT / network lead	Operates access, security, filtering and monitoring controls; blocks unapproved services; includes AI in cyber reviews.	Eduthing
All staff	Use only approved tools through organisation accounts; follow sections 5 to 8; report concerns promptly.	Everyone in scope

4. Approved AI tools and how tools are approved

Staff may use AI for work only through tools the organisation has approved, and only through organisation-provided accounts. Personal accounts must not be used for work, whatever the tool.

4.1 The approved list

- **Microsoft 365 Copilot**
- **TeachMate AI**
- **Canva**
- **Google Gemini**

Any AI tool or service not named above, in section 4a, or excluded under section 2 is not approved and must not be used for work. This includes public consumer chatbots and anything reached through a personal login. A new AI feature appearing inside an already-approved product is not approved by default.

5. What staff may use AI for

Working within this policy, through approved tools and organisation accounts, staff are encouraged to let AI take some of the load on suitable tasks, for example:

- producing a first draft of a plan, resource or message that the member of staff then reviews, shapes and takes responsibility for;
- pulling out key points and actions from documents or notes containing nothing that could identify a real person;
- exploring a topic or organising thinking, with facts checked against reliable sources before they are relied on;
- generating teaching resources, slides or visual materials, checked line by line for subject accuracy, reading level, curriculum fit and accessibility before any pupil or audience sees them;
- supporting accessibility and inclusion: as assistive technology for staff, and to produce accessible or adapted materials for pupils, including those with SEND. Pupils' own use of assistive AI sits under the pupil module.

Every use is subject to the oversight duties in section 8.

6. What staff must not do

6.1 Entering personal or special category data

Do not put information about real, identifiable people into an AI tool. That means no names or anything that could identify a pupil, colleague, parent or carer, and nothing about anyone's needs, health, behaviour, home life, safeguarding, employment, pay or legal matters, even with names removed if the person could still be worked out. If data is entered by mistake, inform Mrs E Wake straight away; it is treated as a possible data breach.

6.2 Reaching for tools that are not approved

Staff must not use AI tools other than those approved under section 4, and must not try to get round filtering or monitoring to reach a blocked service.

6.3 Passing off AI work or breaching assessment rules

Staff must not pass off AI-generated material as their own unaided work where that would mislead, and must not use AI in any way that falls foul of JCQ rules on AI in assessments, which also bar relying on AI as the sole marker of student work. Disclosure of substantial AI drafting is governed by section 8.4.

6.4 High-risk uses and decision about people

AI never takes a decision about a person. AI must not be used to:

- screen, sift or score job applicants, or decide or recommend the ending of anyone's employment or engagement;
- reach, or stand behind, decisions to admit, refuse, suspend or exclude a pupil; where use is authorised, at most it may surface background information for a person to weigh;
- run or inform grievance, disciplinary, complaint or similar processes affecting pupils, parents or staff;
- identify people biometrically, that is, recognising who someone is from their face, voice or body, from images, video or other recordings; if such use were ever authorised through the gate, the Protection of Freedoms Act 2012 requires written parental consent for anyone under 18, and an alternative for those who refuse;
- infer or judge the emotional state, mood or character of a pupil, parent or member of staff;
- treat the output of an AI cheating or plagiarism detector as proof; even where such a tool is approved, its output is unreliable and only ever one input to a judgement a person makes and owns;
- act autonomously on the organisation's behalf, for example sending communications or executing actions without a person approving each output.

6.5 Intellectual property

Staff must not upload third-party copyrighted or licensed material, such as published schemes of work, textbooks or exam papers, into an AI tool without the rights to do so; doing so can breach licences and copyright.

7. Data protection and information security

Everything done with AI complies with the UK GDPR and the Data Protection Act 2018, each as amended by the Data (Use and Access) Act 2025, and with Dane Royd's Data Protection Policy, the main reference for lawful bases, minimisation and individuals' rights.

8. Accuracy, bias, accountability and human oversight

8.1 Getting things wrong

AI can state untruths, invent sources, carry the biases of its training data, or be out of date. Anything factual is checked against a reliable source before use, and outputs are read critically for bias, especially where they touch teaching, assessment, messages to parents or anything going to an external body.

8.2 How prompts shape, and skew, responses

Generative AI reflects the patterns in its training data, and the same request often comes back differently depending on the words used. Ask a tool to explain something "to a boy" and then "to a girl", and the responses can differ in tone, assumption and content: training biases surfacing. Setting an audience in a prompt is often sound teaching practice, but staff should know it can pull stereotyped or culturally skewed material into the output, and read what comes back with that in mind.

8.3 Unsuitable or concerning output

Outputs are read in full before use. Anything raising a safeguarding concern goes to a school DSL at once, with the material retained for review.

8.4 Being open about AI use

Staff should be ready to say where they have used AI. Where a document drafted substantially with AI goes to external bodies, that use is disclosed. Responsibility is unchanged: the author owns the content.

8.5 Keeping a person in charge

However persuasive an output looks, it is not used, shared, published or acted on until a suitably qualified member of staff has reviewed it and applied their own judgement.

- Treat it as a draft, not an answer.
- The output is yours; using AI is no excuse for getting it wrong.
- Read it properly, in full, before you use it.
- People, not AI, decide about people.

9. Safeguarding, online safety and Prevent

Keeping Children Safe in Education 2026 names AI within its four areas of online risk: content, including misinformation and disinformation; contact, expressly including harmful interaction with generative AI applications that simulate human contact; conduct, including explicit images generated using AI; and commerce. Online safety, including AI, runs through the whole-organisation approach to safeguarding, and this policy forms part of that approach.

Creating or sharing fabricated media, including deepfakes, intended to mislead, harass, distress or harm anyone in the community is prohibited and dealt with as a serious conduct and, where relevant, safeguarding matter. Where such material is sexual it may be criminal, and AI-generated sexual imagery of a child is a criminal matter in all circumstances: it is reported to a school DSL, handled under the child protection policy and referred to the police.

where required, in line with the Online Safety Act 2023 and the Ofcom Protection of Children code. Multi-agency action follows Working Together to Safeguard Children 2026.

Making, adapting, supplying or offering nudification tools, tools designed to remove clothing from images of real people, is a criminal offence under the Crime and Policing Act 2026. Any encounter with such a tool involving a member of this community is a safeguarding matter and is reported as above. Staff must not use AI to clone or simulate the voice or likeness of any pupil, parent or colleague; and because cloned voices and fabricated messages are increasingly used in fraud, any unusual or urgent request, particularly one involving payments, credentials or personal data, is verified through a known channel before anyone acts on it, in line with the DfE cyber security standards.

Automated tools can harvest photographs of children from public webpages and social media, including the organisation's own, for use in fabricated or abusive material. The organisation keeps its publication of identifiable pupil images, and the consent underpinning it, under review with this risk in mind.

The Prevent duty applies to AI as to everything else. AI can produce, surface or amplify extremist or radicalising content, sometimes from innocuous prompts; any such content or concern is routed through the usual Prevent and safeguarding channels, with section 12 keeping unapproved services out of reach.

The organisation is open with its community about AI: it communicates to parents and carers how AI is used in the organisation, including staff use.

10. Impact assessment and product safety checks

Before any AI tool that could process personal data is deployed, an impact assessment is completed, led by Mrs E Wake. Every new tool is also checked against the DfE generative AI product safety standards (January 2026), which cover stated purpose, educational use cases, filtering, monitoring and reporting, security, privacy and data protection, intellectual property, design and testing, governance, and safeguards for cognitive development, emotional and social development, mental health and manipulation. The check includes considering, under the Prevent duty, whether the tool could generate or expose users to extremist or otherwise inappropriate ideological content, with any concern routed to the designated safeguarding lead (section 9).

11. Training and awareness

Before using approved tools for the first time, staff complete appropriate training, covering what is approved, the data rules in sections 6 and 7, the principle that a person stays in charge, and what to do if something is entered in error.

12. Filtering, monitoring and assurance

Access to AI services sits within the organisation's filtering and monitoring, in line with the DfE filtering and monitoring standards and current UK Safer Internet Centre definitions. Unapproved services are blocked at network level so far as reasonably possible. The named senior lead is the filtering and monitoring lead (section 3). Each year the review considers how generative AI tools are used, whether the solution can handle real-time, dynamic, personalised and AI-generated content, and how access routes that bypass network controls, including personal devices with their own connectivity such as wearables, are managed. No filter reliably catches live AI-generated content.

13. Breaches and serious incidents

Suspected breaches are looked into promptly. Depending on seriousness, the response may include withdrawing access to AI tools, requiring further training before access returns,

formal action under Staff Code of Conduct, referral to the Teaching Regulation Agency for serious professional misconduct, and notification to the ICO for a data protection breach. Where safeguarding is involved, the matter is handled under the child protection policy and may be referred to the police or the local authority designated officer. A serious AI incident, such as a significant data breach, a safeguarding matter or an event carrying reputational risk, is escalated at once to the head teacher without waiting for routine reporting.

Acknowledgment of Source and Licensing

This policy has been developed with reference to and support from the ICT *Evangelist's Use of Artificial Intelligence Policy Template*. The original work is protected by a Creative Commons License: CC BY-NC-SA 4.0. This licence requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for non-commercial purposes only. If others modify or adapt the material, they must license the modified material under identical terms.