

Liscard Primary School
Artificial Intelligence (AI) Policy

Comprehensive Operational & Safeguarding Framework for Ethical AI Integration in Primary Education



Document Owner / Role	Daniel Roberts (Computing Lead)) in consultation with Jane Fagan (Headteacher & DSL)
Statutory Alignment	Keeping Children Safe in Education (KCSIE 2026), Working Together 2026, Children's Wellbeing & Schools Act 2026, Crime & Policing Act 2026
Date of Last Review	22 September 2026
Date Approved by Governors	22 September 2026
Frequency of Review	Annual (Live Document reviewed continuously in response to AI risk updates)
Date of Next Scheduled Review	September 2027

1. Rationale and Policy Aims

At Liscard Primary School, we are committed to the ethical, purposeful, and safe integration of Artificial Intelligence (AI) technologies across all aspects of teaching, learning, and educational administration. We recognise that generative AI tools offer transformative potential to streamline administrative workflows, reduce teacher workload, assist with differentiated resource design, and provide personalised learning opportunities for our pupils.

However, technological innovation must never compromise pupil safety, personal privacy, digital wellbeing, or the core human relationships that underpin effective primary education. Underpinning this policy is the firm principle that AI tools can supplement, but never replace, human expertise, teacher judgment, professional oversight, or the safeguarding vigilance required to protect children.

The primary aims of this policy are to:

- **Framework & Governance:** Establish a clear operational and legal framework for the ethical use of AI tools by staff, governors, and pupils.
- **Statutory Safeguarding:** Ensure absolute alignment with Keeping Children Safe in Education (KCSIE 2026), Working Together to Safeguard Children (2026), and the school's Child Protection - Safeguarding Policy (September 2026).
- **Data Security:** Maintain robust data privacy boundaries in compliance with UK GDPR and the Data Protection Act 2018, strictly prohibiting the input of Personally Identifiable Information (PII) or sensitive safeguarding records into AI systems.
- **Digital Harm Prevention:** Protect primary pupils from online harms, technology-assisted harmful sexual behaviour (TA-HSB), deepfakes, image-based sexual abuse (IBSA), and exposure to inappropriate content.
- **Workload Efficiency:** Empower staff to utilise approved AI applications to reduce administrative burdens while retaining full professional ownership and accountability for all educational outputs.
- **Pupil Digital Literacy:** Equip pupils with essential digital literacy, critical thinking, and source verification skills within an age-appropriate primary curriculum.

2. Definitions

For the purposes of this policy, Artificial Intelligence (AI) encompasses computer systems capable of performing tasks that traditionally require human intelligence, including visual perception, natural language processing, decision-making, and pattern recognition.

Generative AI refers to algorithms (such as Large Language Models and multimodal synthetic media generators) capable of producing new text, images, computer code, audio, or video based on massive datasets and user prompts. Generative AI tools within primary education are categorised into two structural models:

- **Open Generative AI Tools:** AI tools that are publicly accessible and utilise input data (prompts, uploaded documents, and files) to continuously train and refine their underlying models. These tools pose significant data protection risks as inputs may be stored, analysed, or surfaced to external third parties. Examples include public free tiers of commercial web-based chatbots.
- **Closed Generative AI Tools:** Enterprise-level or restricted AI environments where vendor agreements and privacy architectures strictly prevent user inputs from being retained, shared, or utilised for LLM training. While closed models offer higher technical security, staff must remain vigilant as third-party metadata sharing may still occur.

3. Legislation and Statutory Framework

This policy is constructed directly upon current UK statutory guidance, statutory duties, and educational regulations. It complies strictly with:

- **DfE Safeguarding Guidance:** Keeping Children Safe in Education (KCSIE 2026) and Working Together to Safeguard Children (2026) (Department for Education).
- **DfE AI Support Framework:** Generative artificial intelligence (AI) in education and Using AI in education settings: support materials (DfE).
- **Children's Wellbeing Act:** Children's Wellbeing and Schools Act 2026, reinforcing digital safety, pupil wellbeing, and multi-agency safeguarding duty.
- **Crime & Policing Act:** Crime and Policing Act 2026, regarding safer recruitment, violence prevention, and tackling technology-assisted abuse.
- **Online Safety & Cyber Legislation:** Online Safety Act and Computer Misuse Act 1990 (including Cyber Choices awareness and cybercrime prevention).
- **Data Protection Law:** UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA 2018).
- **Assessment Regulations:** JCQ AI Use in Assessments and Ofqual guidance on regulating AI in qualifications.
- **National AI Principles:** AI Regulation White Paper (Department for Science, Innovation and Technology) principles.

4. Regulatory Principles

Liscard Primary School enforces the five core regulatory principles set out in national AI governance frameworks:

- **1. Safety, Security & Robustness:** AI systems deployed must be secure, technically robust, and subject to technical filtering to prevent user harm, data leakage, hacking, or deepfake generation.
- **2. Appropriate Transparency & Explainability:** Staff and governors must maintain full transparency regarding where and how AI tools are used. AI-generated elements in official communications, lesson resources, or policy drafts must be clearly attributed.
- **3. Fairness & Equality:** AI tools must be evaluated to ensure they are equitable and free from algorithmic bias or prejudice, particularly concerning protected characteristics under the Equality Act 2010.
- **4. Accountability & Governance:** Clear lines of governance are established across the Senior Leadership Team, Governing Body, and staff. The school remains fully accountable for all decisions made using AI support.
- **5. Contestability & Human Intervention:** Staff retain absolute authority to overrule, reject, or modify any AI-generated decision or output. Decisions affecting pupils are made solely by qualified human professionals.

5. Roles and Responsibilities

Safeguarding and effective digital governance are collective responsibilities across Liscard Primary School. Specific key leadership responsibilities are defined below:

Operational AI Lead/ Computing Lead — Daniel Roberts

Daniel Roberts serves as the school's operational AI Lead. In this role, he is responsible for:

- Leading the day-to-day strategic management and educational oversight of AI integration across the curriculum.
- Conducting initial technical, pedagogical, and age-appropriateness reviews of proposed AI applications.
- Coordinating with the Data Protection Officer (DPO) and IT Network Manager- Hi Impact- to perform rigorous Data Protection Impact Assessments (DPIAs) prior to tool approval.
- Overseeing staff Continuous Professional Development (CPD) to ensure safe, effective, and workload-reducing AI practices.
- Monitoring AI usage across year groups and maintaining the live registry of approved AI applications.

Headteacher & Designated Safeguarding Lead (DSL) — Jane Fagan

Jane Fagan holds dual statutory responsibility as Headteacher and Designated Safeguarding Lead (DSL). Supported by Deputy DSLs Marie Caton (Senior Family Support Worker) and Leanne Quarry-Ellis, Mrs Fagan is responsible for:

- Exercising overall executive authority and signing off on all approved AI applications following DPIA completion.
- Maintaining comprehensive safeguarding oversight over all AI activities, ensuring complete alignment between AI practices and the Child Protection - Safeguarding Policy (September 2026).
- Monitoring automated filtering and monitoring software alerts relating to AI usage, prompt inputs, or unauthorised system access.
- Evaluating emerging AI-driven safeguarding threats, including technology-assisted harmful sexual behaviour (TA-HSB), image-based sexual abuse (IBSA), deepfakes, voice cloning, and cybercrime.
- Logging and managing AI-related safeguarding incidents on CPOMS, coordinating with Wirral Integrated Front Door (0151 606 2008), Merseyside Police, or the LADO (Kevin Dykes) where thresholds are met.

The Governing Body

The Governing Body (chaired by George Lucking, with Sarah Brear serving as Link Governor for Safeguarding) will:

- Hold the Headteacher and AI Lead to account for the ethical, legal, and safe implementation of this policy.
- Conduct an annual review of the school's AI Policy, Online Safety Policy, and IT filtering/monitoring provisions in accordance with KCSIE 2026.
- Ensure that staff receive appropriate resources, time, and training to navigate AI risks effectively.

Data Protection Officer (DPO)

The DPO advises the school on UK GDPR compliance, reviews draft DPIAs for new AI software, monitors data processing agreements, and investigates any suspected personal data breaches resulting from AI prompt inputs.

All Teaching and Support Staff

All staff members must:

- Use only AI tools explicitly listed on the School Approved AI Tools Registry (Section 6).
- Strictly adhere to the mandatory prohibition against entering personal, sensitive, or identifiable pupil/staff data into any AI except for first names
- Fact-check, sense-check, and critically evaluate all AI outputs before relying upon them for lesson delivery, assessment, or administration.
- Report any software vulnerabilities, policy breaches, or emerging safeguarding concerns immediately to the Headteacher/DSL or AI Lead.

MANDATORY REQUIREMENT: ABSOLUTE DATA PRIVACY BOUNDARY

- No pupil full name, date of birth, UPN, address, SEN status, medical details, or vulnerable flag may EVER be entered into an AI prompt, and any name must be added in to a closed AI app such as Gemini.
- CPOMS disclosures, safeguarding notes, case files, Family Help records, and disciplinary logs are strictly prohibited from all AI processing.
- Staff breaches involving personal data inputs will trigger immediate data breach reporting under UK GDPR and potential disciplinary review under the Staff Code of Conduct.

6. Approved Use of AI Tools

To ensure safety, data protection, and workload efficiency, staff and governors may only utilize AI applications that have undergone full due diligence and received formal Headteacher sign-off.

The table below details the current Approved AI Tools Registry for Liscard Primary School:

Approved AI Tool	Permitted Educational & Workload Uses	Mandatory Safeguarding & Data Constraints
Canva (AI Functionalities)	Designing visual worksheets, classroom displays, presentation slides, certificates, newsletter graphics, and branded materials.	No pupil photos or identifiable student graphics to be processed using AI magic edit tools without explicit parental consent. Zero PII inputs.
Claude AI (Anthropic)	Lesson planning, curriculum sequencing, differentiated rubric creation, drafting administrative correspondence, and policy synthesis.	Strictly prohibited from receiving real pupil names, CPOMS notes, or sensitive staff files. All outputs must be expert-reviewed before use.

Google Gemini (Workspace Integrated)	Data trend analysis, summarising educational research, drafting multilingual communication templates, intervention planning.	Must be accessed solely via managed school accounts with enterprise data protections enabled. No entry of SEN/safeguarding logs.
Adobe Express (AI Suite)	Generating educational graphics, visual aids, classroom presentation media, design templates for school displays.	All generated media must adhere to age-appropriate standards. No creation of synthetic media depicting real individuals.

7. Process for Approving New AI Tools

Staff seeking to introduce a new AI application, web extension, or software feature must submit a formal request to Daniel Roberts. Before any tool is added to the Approved Registry, the following rigorous due diligence process must be completed:

- **1. Data Protection Impact Assessment (DPIA):** Verification of data storage locations, vendor privacy policy, model training permissions, and compliance with UK GDPR. A formal DPIA must be completed and signed off by the DPO.
- **2. Technical & Safeguarding Audit:** Evaluation of technical filtering, content moderation safeguards, susceptibility to prompt injection, and protection against generating inappropriate or harmful material.
- **3. Pedagogical & Age Review:** Assessment of tool accessibility, user interface clarity, age appropriateness, and suitability for primary school pupils or staff workflows.
- **4. Technical Integration:** Verification that the tool integrates securely with existing school infrastructure (e.g., Google Workspace for Education, MIS) without creating cyber vulnerabilities.
- **5. Executive Sign-Off:** Final written authorisation from Headteacher Jane Fagan prior to software deployment or account creation.

8. Data Protection, Privacy, and Strict PII Boundaries

Data privacy is a non-negotiable statutory requirement. Liscard Primary School strictly enforces a zero-PII policy regarding open and closed generative AI platforms:

- **Absolute Prohibition of PII:** Staff, governors, and pupils must NEVER enter Personally Identifiable Information into an AI prompt. PII includes pupil full names, dates of birth, home addresses, parent contact details, Unique Pupil Numbers (UPNs), photographs, or voice recordings.
- **Safeguarding Data Ban:** Under no circumstances may confidential safeguarding notes, CPOMS logs, Family Help assessments, SEN EHCP documents, medical files, or disciplinary records be uploaded or pasted into an AI system.
- **Anonymisation Protocol:** When using AI to assist with lesson differentiation or report commentary, staff must use fully generic or anonymised descriptors (e.g., 'a Year 3 pupil working at age-related expectations who requires support with fractions').
- **Data Breach Reporting:** If sensitive personal data is accidentally entered into an unauthorised or open AI platform, this must be reported immediately to Headteacher Jane Fagan and the DPO. The incident will be investigated as a potential personal data breach in accordance with our Data Protection Policy.

9. Intellectual Property and Pupil Work

Under UK copyright law, pupils retain intellectual property rights over their original creative works, artwork, and writing. Staff must ensure that:

- Pupil work (including stories, poems, artwork, or audio recordings) is never uploaded into open AI tools that utilise user inputs to train public language models, unless explicit written consent has been obtained from parents/carers.
- AI-generated content used in school policies, curriculum materials, or public communications is properly acknowledged and transparently documented.

10. Algorithmic Bias and Discrimination

Generative AI models are trained on vast web datasets that frequently contain historical, societal, and cultural biases, particularly concerning protected characteristics under the Equality Act 2010 (such as sex, race, ethnicity, disability, and religion).

Staff must apply critical professional evaluation to all AI-generated resources, checking for biased assumptions, stereotypical representations, or inaccuracies. Biased or discriminatory AI outputs must be discarded immediately, and staff CPD will explicitly include training on detecting algorithmic bias.

11. Raising Concerns and Whistleblowing

Staff, governors, or parents who harbor concerns regarding the improper, unethical, or unsafe use of AI within the school are encouraged to raise these directly with Headteacher Jane Fagan or Daniel Roberts.

Where concerns relate to potential leadership misconduct or systemic safeguarding failures involving technology, staff may utilize the school's Whistleblowing Policy or contact the NSPCC Whistleblowing Helpline directly on 0800 028 0285.

12. Ethical and Responsible Use Standards

All members of the Liscard Primary School community are expected to maintain the highest ethical standards when interacting with digital technology. Staff, governors, and pupils are strictly prohibited from:

- **Impersonation & Harassment:** Creating, generating, or manipulating synthetic media, images, or audio to impersonate, intimidate, bully, or harass any pupil, staff member, or community member.
- **Deepfakes & Harmful Media:** Utilising AI applications to generate, edit, or view deepfake imagery, synthetic nude or semi-nude images, sexually explicit content, or material linked to Image-Based Sexual Abuse (IBSA) or Technology-Assisted Harmful Sexual Behaviour (TA-HSB).
- **Discriminatory Prompts:** Inputting discriminatory, misogynistic, racist, extremist, or offensive prompts into any AI platform.
- **System Bypassing:** Attempting to bypass school web filtering, security firewalls, or monitoring tools to access unauthorised AI applications.

13. Educating Students About AI & Digital Safety

To prepare pupils for a digital society while protecting them from online harms, Liscard Primary School embeds age-appropriate AI literacy and online safety throughout the ICT/Computing curriculum, PSHE lessons, and assemblies.

Key educational components include:

- **Critical Thinking & Verification:** Teaching pupils that AI outputs can be inaccurate, incomplete, or biased, and training them to check facts using trusted books and verified online resources.
- **Digital Harms & Synthetic Media:** Educating pupils on the dangers of deepfakes, voice cloning, synthetic media, and online mis/disinformation.
- **Privacy & Personal Boundaries:** Helping pupils understand why personal information (names, photos, school details) must never be shared with online chatbots or apps.
- **Safeguarding Disclosures:** Guiding pupils on how to report uncomfortable online encounters, cyberbullying, or inappropriate content to a trusted adult immediately.

14. Use of AI by Primary School Students

Recognising the developmental vulnerabilities and screen-time considerations of primary-aged children, pupil interaction with AI technology at Liscard Primary School is governed by strict operational safeguards:

- **Mandatory Staff Supervision:** Primary pupils may only interact with AI applications under direct, continuous, adult staff supervision in structured learning contexts.
- **Account Restrictions:** Pupils are strictly prohibited from independently creating accounts or accessing unmonitored open AI chatbots.
- **Structured Prompting:** When AI tools are utilised for learning (e.g., evaluating AI-generated image variations in Art, or exploring text summaries in Computing), all prompt inputs must be managed or pre-approved by the classroom teacher.
- **AUP Alignment:** Pupil access to AI must align fully with the school's Online Safety Policy and IT Acceptable Use Policy (AUP).

15. Plagiarism, Misuse, and Academic Integrity

At Liscard Primary School, we value authentic learning, creative effort, and original thought. AI tools must not be used by pupils to complete classwork or homework where the work is presented as their own unassisted effort.

Where pupils use AI tools under teacher guidance to support research or brainstorming, proper attribution must be included (e.g., 'Image generated using Adobe Express under teacher guidance on [Date]'). Unattributed copy-pasting of AI text constitutes academic plagiarism and will be managed in accordance with our Behaviour Policy.

16. Formal Assessments

The use of AI applications during formal standardised assessments (such as Key Stage 2 SATs, baseline assessments, or internal summative examinations) is strictly prohibited and constitutes assessment malpractice. Liscard Primary School adheres fully to JCQ and Ofqual regulations regarding assessment integrity.

17. Staff Training & Continuous Professional Development

To maintain high standards of digital safety and pedagogical effectiveness, the AI Lead Daniel Roberts and Headteacher/DSL (Jane Fagan) will ensure that:

- All teaching and support staff receive baseline annual training on ethical AI usage, prompt security, PII prohibitions, and emerging AI safeguarding threats.
- Safeguarding CPD explicitly addresses AI-driven risks, including deepfakes, TA-HSB, cybercrime indicators, and monitoring software alerts.
- Good practice and workload-reducing strategies are shared regularly through staff briefings and Professional Growth Development time.

18. Breach of Policy & Allegation Management

Compliance with this policy is mandatory for all staff, governors, contractors, and pupils.

Staff and Governor Breaches

Any breach of this policy by a staff member will be investigated under the Staff Code of Conduct and Disciplinary Policy. Depending on severity, breaches may result in formal disciplinary action, revocation of IT privileges, or summary dismissal.

Where a staff breach involves low-level concerns (e.g., inadvertent slip in prompt design without harm), it will be managed under the Low-Level Concerns Framework. Where a breach involves potential harm to a child, data breach, or illegal activity (e.g., generating deepfakes or uploading confidential records), Headteacher Jane Fagan will immediately refer the matter to the Local Authority Designated Officer (LADO), Kevin Dykes (0151 666 4442 / kevin.dykes@wirral.gov.uk), in accordance with Appendix 3 of our Safeguarding Policy.

Pupil Misuse

Pupil breaches (such as unauthorised system access, cyberbullying, or attempting to generate offensive media) will be managed proportionately under the school's Behaviour Policy and Child Protection - Safeguarding Policy.

19. Monitoring, Filtering, and Policy Transparency

AI technology and associated societal risks evolve rapidly. Consequently, this policy is maintained as a live operational document:

- **Filtering & Monitoring Alerts:** Automated monitoring and filtering software actively scans the school network for unauthorised AI access, inappropriate prompts, or safety violations. Automated alerts are routed directly to DSL Jane Fagan and the IT Network Team.
- **Annual Review Cycle:** The Senior Leadership Team and Governing Body will review this policy annually, or immediately upon the release of updated statutory guidance from the DfE or WSCP.
- **Community Transparency:** This policy is published on the Liscard Primary School website and is readily accessible to parents, staff, and the wider community.

20. Links With Other School Policies

This AI Policy must be read and operated directly alongside the following statutory school policies:

- **Safeguarding Core:** Child Protection - Safeguarding Policy and Procedures (September 2026 - September 2027)
- **Digital Safety:** Online Safety Policy & IT Acceptable Use Policy (AUP)
- **Data Governance:** Data Protection Policy & Privacy Notices (UK GDPR / DPA 2018)
- **Staff Governance:** Staff Code of Conduct & Low-Level Concerns Framework
- **Pupil Behaviour:** Pupil Behaviour Policy & Anti-Bullying Policy
- **Operational Standards:** Whistleblowing Policy & Safer Recruitment Policy