

ARTIFICIAL INTELLIGENCE (AI) IN PRIMARY EDUCATION POLICY

Start children off on the way they should go, and even when they are old they will not turn from it.”

Proverbs 22:6



Adopted:	September 2026
Committee:	Full Governors
Review Date:	September 2028
The scope of this policy is Forsbrook CE Primary School and Nursery	

We are a Christian school where quality and opportunities make a difference. We value all children as unique ‘Children of God’ and nurture each other to show **LOVE** in our relationships and a **RESPECT** for all. We foster **HOPE** within our community and encourage children to find **PEACE** by creating times and places for stillness and reflection. We strive for excellence, inspiring dreams both now and in the future. We promote **POSITIVITY**, celebrate **COURAGE**, demonstrate **RESPONSIBILITY** and share **JOY** through...

‘Learning, loving, laughing in the light of Jesus’.

Contents

1. INTRODUCTION	3
2. STATEMENT OF INTENT	3
3. SCOPE AND DEFINITIONS	3
4. RELATED POLICIES	3
5. APPROVED AI TOOLS AND ACCESS	3
6. POLICY STATEMENTS	4
7. ROLES AND RESPONSIBILITIES.....	4
HEADTEACHER AND SENIOR LEADERSHIP TEAM (SLT).....	4
DESIGNATED SAFEGUARDING LEAD (DSL) / ONLINE SAFETY LEAD	4
DATA PROTECTION OFFICER (DPO)	4
IT LEAD / TECHNICAL STAFF.....	4
STAFF	4
GOVERNORS/TRUSTEES	4
PARENTS/CARERS	4
8. REPORTING	5
9. RESPONDING TO INCIDENTS	5
10. RISK ASSESSMENT	5
11. EDUCATION (PRIMARY) AND CURRICULUM INTEGRATION	6
12. STAFF TRAINING	6
13. REVIEW	6
APPENDIX A: STAFF AI ACCEPTABLE USE AGREEMENT (AUA)	6
APPENDIX B: CHILD-FRIENDLY SUMMARY (FOR KS1/KS2)	6
APPENDIX C: AI INVENTORY TEMPLATE	7

1. Introduction

This policy sets out how Forsbrook CE Primary School will use artificial intelligence (AI) safely, ethically, and effectively to support teaching, learning, administration and pupil welfare. It aligns with UK safeguarding and data protection expectations and complements existing school policies.

2. Statement of Intent

- We will harness AI to improve outcomes, reduce workload and promote inclusion while prioritising pupil safety and wellbeing.
- We will comply with UK GDPR and relevant statutory safeguarding guidance, including Keeping Children Safe in Education (KCSIE).
- We will train staff and governors on effective, responsible use of AI and equip pupils with age-appropriate AI literacy.
- We will ensure human oversight of AI-assisted processes and decisions—AI assists; humans decide.
- We will protect sensitive information and will not input personal or confidential data into AI tools unless they are approved and privacy-assured.

3. Scope and Definitions

This policy applies to all staff, governors, volunteers, contractors and pupils using AI in school or on school-managed accounts/devices. “AI” includes generative and non-generative systems (e.g., Microsoft 365 Copilot, educational tools with AI features, analytics and recommendation systems).

4. Related Policies

- Data Protection Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Behaviour and Anti-bullying Policies
- Staff/Volunteer Acceptable Use Agreement (AUA)
- Curriculum: Computing and PSHE

5. Approved AI Tools and Access

- Only school-approved AI tools may be used for school purposes.
- Staff must use school-provided accounts (e.g., Microsoft 365 tenancy) for any AI-supported work.
- A school-wide AI inventory will be maintained by the Computing Lead, listing tools, purposes, data flows and risk assessments.

6. Policy Statements

- Responsible use: AI tools may be used to support planning, differentiation, accessibility, feedback and administrative tasks when pedagogically sound and risk-assessed.
- Human oversight: All AI-generated content must be fact-checked and reviewed prior to use or publication, especially external communications.
- Data protection: Do not input personal data (pupil, staff, parent) into generative AI unless the tool is vetted, configured, and a DPIA confirms lawful, secure processing.
- Sensitive content: Do not upload confidential documents or strategic plans to third-party AI tools unless explicitly approved.
- Bias and fairness: Staff should critically evaluate outputs for bias or discriminatory content and escalate concerns.
- Copyright/IP: Respect intellectual property and ensure pupils' work is not used to train AI models without appropriate consent.
- Procurement: New AI systems must undergo due diligence, security review and (where needed) a Data Protection Impact Assessment (DPIA).

7. Roles and Responsibilities

Headteacher and Senior Leadership Team (SLT)

- Set the strategic approach, approve tools and ensure resourcing.
- Oversee training, monitoring and evaluation of AI use.

Designated Safeguarding Lead (DSL) / Online Safety Lead

- Advise on AI-related safeguarding risks and responses.
- Ensure pupil-facing guidance is age-appropriate and integrated into Online Safety education.

Data Protection Officer (DPO)

- Advise on lawful bases, DPIAs, data minimisation and vendor compliance.
- Maintain the AI inventory and records of processing (where applicable).

IT Lead / Technical Staff

- Ensure effective filtering/monitoring, cyber security controls and account governance.
- Support staff with safe configuration and updates.

Staff

- Follow this policy and AUA; model safe, ethical AI use.
- Report incidents or concerning outputs promptly.

Governors/Trustees

- Receive training; scrutinise and support AI implementation and risk management.

Parents/Carers

- Engage with school guidance on AI; raise concerns via published routes.

8. Reporting

Concerns, incidents or suspected breaches should be reported via: admin@forsbrook.staffs.sch.uk and to the DSL/DPO (SDawson) as appropriate. Anonymous reports are accepted.

9. Responding to Incidents

1. Record: Log the incident in school systems (e.g., safeguarding record / data incident log).
2. Assess: DSL/DPO/IT Lead assess severity (safeguarding, data, cyber, reputational).
3. Act: Contain risk, disable accounts/tools if necessary; support affected individuals.
4. Notify: Where required, notify external agencies (Police, LADO, ICO) and trustees.
5. Review: Conduct post-incident review; update training, controls and policy.

10. Risk Assessment

Leaders will review AI risks alongside broader safeguarding and data protection. Use the matrix below to complete likelihood, impact and risk level for your context.

Risk Area	Risk Description	Likelihood	Impact	Risk Level	Mitigation Measures
Data Protection and Privacy	Unauthorised access or inappropriate data sharing.	Medium	High	High	Use vetted tools; encryption; access controls; DPIA; audits.
Cyberbullying / Inappropriate Content	Exposure to harmful content or AI-mediated bullying.	Low	High	Medium	Filtering/monitoring; reporting routes; staff/parent education; pastoral support.
Over-reliance on AI	Reduced teacher autonomy or pupil critical thinking.	Low	Medium	Low	Balance AI with human interaction; clear pedagogical rationale; review impact.
Bias and Discrimination	Biased outputs affecting inclusion or fairness.	Low	Medium	Low	Audit outputs; staff training; escalate issues to SLT/DPO.
Misinformation	Inaccurate or misleading AI content used in school.	Medium	Medium	Medium	Fact-check; trusted sources; staff/pupil media literacy.
Mental Health Impacts	Stress or dependency due to AI use.	Low	Medium	Low	Set usage expectations; monitor wellbeing; adjust practice.
Legal Compliance	Non-compliance	Low	High	Medium	Stay current with guidance; consult DPO; update policies.

	with relevant laws/guidance.				
Cyber Security	AI tools used in attacks or increase attack surface.	Medium	High	High	Patching; MFA; least privilege; network monitoring; vendor due diligence.

11. Education (Primary) and Curriculum Integration

AI literacy will be delivered where relevant across the curriculum, with a focus on Computing and PSHE, assemblies and cross-curricular projects. Emphasis will be placed on safe, responsible use, critical thinking, fairness and creativity.

- Computing: prompts, evaluation, safe searching, understanding AI features in tools.
- PSHE: online safety, media literacy, wellbeing and responsible digital behaviour.
- Assemblies/Parent Communication: awareness, benefits, boundaries and reporting.

12. Staff Training

- Annual safeguarding training includes AI-related risks and reporting.
- Role-specific training for DSL/DPO/IT Lead on data protection, DPIA and vendor management.
- Practical CPD on classroom use (planning, differentiation, accessibility) and risk mitigation.

13. Review

This policy will be reviewed annually or when new guidance/technologies arise. Next scheduled review: September 2026

Appendix A: Staff AI Acceptable Use Agreement (AUA)

- Use only approved, school-managed AI tools and accounts.
- Do not input personal or sensitive data unless the tool is vetted and a lawful basis is confirmed.
- Evaluate outputs for accuracy; maintain human oversight.
- Respect copyright and intellectual property.
- Report incidents immediately to DSL/DPO/IT Lead.
- Breaches may lead to disciplinary action.

Appendix B: Child-friendly Summary (for KS1/KS2)

- We sometimes use smart computer helpers (AI) at school to help us learn.
- We check that what AI says is true and kind. If something seems wrong, tell an adult.
- We never share private information with AI.
- If AI shows something upsetting, tell a trusted adult straight away.

Appendix C: AI Inventory Template

Tool	Purpose	Owner	Personal Data (Y/N)	DPIA (Y/N)	Notes
Microsoft 365 Copilot	Staff planning & admin tasks	SLT	Y	Y	Approved; only staff accounts; GDPR safe
GivEducation	Staff planning, resource creation	SLT	N	N	Staff use only; no pupil data
EdShed (Spelling Shed)	Literacy practice & gamification	English Lead	Y	Y	Adaptive tasks; GDPR-compliant