Walverden Primary School

AI Policy

Approved by:	Governors	**Date:** March 2026	
Next review due by:	March 2027		

Walverden Primary School — Artificial Intelligence (AI) Policy

Pupil / staff contact for AI queries: Humma Ahmed/Charlotte Wildman/Zishan Ashraf / IT Lead

1. Purpose

This policy sets out Walverden Primary School's approach to the safe, responsible and effective use of Artificial Intelligence (AI) technologies by staff, pupils, governors, parents and third-party providers. It explains responsibilities, acceptable use, safeguarding and data-protection requirements, procurement checks, training and monitoring arrangements to ensure the benefits of AI are realised while risks are managed.

2. Scope

This policy applies to:

- All staff (teaching, support, leadership), supply staff and volunteers
- All pupils in the school (in-school and during school-led remote learning)
- Governors and trustees
- Parents/carers when engaging with school-provided AI services or supporting pupil use
- Third-party providers and contractors supplying AI-enabled products or services to the school
- All devices using school accounts, networks and resources, and personal devices used for school business or learning where school accounts are used

3. Definitions

- AI: Technologies that perform tasks requiring human-like cognitive processes, including generative AI (text, image, audio), predictive analytics and automated decision-making systems.
- Personal Data: Any information relating to an identified or identifiable individual (GDPR definition).
- AI Tool / Service Provider: Any application, platform or dataset employing AI that the school or users may access.

4. Principles

Walverden Primary School will:

- Prioritise pupil safety, privacy and wellbeing at all times.
- Use AI to enhance teaching, learning, efficiency and inclusion where educational benefit is clear.
- Maintain human oversight over decisions affecting pupils.
- Avoid use of AI that would undermine professional judgement or pupil safeguarding.
- Ensure transparency, accountability and proportionate risk assessment before procurement or deployment.

5. Roles and responsibilities

- Governing Body: Approve policy, ensure accountability, monitor impact and provide scrutiny for AI procurement and high-risk deployments.
- Headteacher: Overall responsibility for implementation and culture; sign-off for procurement and high-risk use.
- Data Protection Officer (DPO): Advise on GDPR/Data Protection Impact Assessments (DPIAs); review data-sharing and contracts.
- Designated Safeguarding Lead (DSL): Advise on safeguarding implications of AI use and handle disclosures or concerns linked to AI.
- IT Lead / Network Manager: Technical assessment, cybersecurity checks, account management and restrictions.
- Pupil / Pastoral Leads and SENCO: Ensure AI provision is accessible and appropriate for pupils with SEND and additional needs.
- Staff: Follow this policy, undertake training and exercise professional judgment and supervision when using AI with pupils.
- Parents/Carers: Support safe use at home and follow guidance when consenting to school-provided AI services.

6. Risk assessment and procurement (third-party AI services)

Before procuring or using an AI product or service, the school will:

- Complete a written risk assessment and DPIA for any processing of personal data (DPO to advise).
- Verify vendor compliance with UK GDPR and data-protection standards, including data storage location, retention policy and deletion arrangements.
- Require a data-processing agreement (DPA) or contract with clear responsibilities, security standards and breach notification timescales.
- Check transparency and provenance: how the model was trained, known limitations, bias audits and accuracy levels for relevant tasks.
- Confirm there is a reliable support/maintenance route and escalation process.
- Avoid vendors requiring the upload of pupil-sensitive data unless legally necessary and approved by DPO and Headteacher.
- Trial in a controlled environment and monitor impact before wider rollout.
- Where a vendor offers a cloud-hosted AI service, ensure appropriate cybersecurity measures (encryption, strong authentication, logging).

7. Acceptable use — staff

- **Staff may use school-approved AI tools to support planning, differentiation, assessment and professional development, subject to the following:**
    - Do not upload any pupil sensitive personal data, safeguarding records, medical information or SEND plans to public or unauthorised AI tools.
    - Redact personal identifiers when using examples for model prompts unless explicitly authorised by the DPO and parental consent obtained where required.
    - Use AI outputs as a draft or support — always check accuracy, bias and appropriateness; apply professional judgement before sharing with pupils, parents or including in official records.
    - Cite AI-generated content where used in teaching materials and do not represent AI-produced work as entirely human-created if that would mislead pupils or parents.
    - Avoid using AI to make high-stakes decisions about pupils (e.g. exclusion risk, safeguarding decisions) without human review and oversight by senior staff.
    - Keep any logs of AI use where relevant (e.g. for assessment marking support).
    - Inform IT Lead and DPO if an AI tool behaves unexpectedly or produces inappropriate content.

8. Acceptable use — pupils

- Pupils may use school-approved AI tools under teacher supervision and with age-appropriate guidance. Expectations:
    - Use AI tools only as directed by staff.
    - Do not attempt to upload personal data (own or others), images of pupils or staff, or seek to reveal personal information.
    - Use AI outputs as a starting point for learning — pupils must show how they have edited, improved or critically evaluated any AI-generated text or media.
    - Plagiarism rules apply: pupils must acknowledge assistance from AI where required by staff and learning tasks will require evidence of pupil thinking.
    - Report any concerning outputs, misinformation or content that makes the pupil uncomfortable to a member of staff immediately.

9. Age-appropriate guidance and teaching

- AI literacy will be taught through the curriculum, with pupils learning:
    - What AI is and its limitations
    - How to evaluate AI outputs critically
    - Safe and ethical use online, including privacy and digital citizenship
    - How to cite and attribute AI assistance where appropriate

10. Safeguarding and child protection

- Any disclosure, grooming attempt, inappropriate content or safeguarding concern emerging from AI use must be reported to the DSL immediately in line with the school's Safeguarding Policy.
- The school will not rely on automated AI for safeguarding decision-making without human oversight.
- If an AI system flags safeguarding concerns (e.g. automated monitoring), DSL must review before action; any automated alerts do not replace statutory safeguarding procedures.

11. Data protection and privacy

- The school will adhere to UK GDPR and Data Protection Act requirements:
    - Process personal data lawfully, fairly and transparently.
    - Ensure a lawful basis for processing and obtain parental consent where required (for special categories of data or where contractual requirements demand).
    - Use the minimum data necessary for the purpose. Avoid feeding pupil personal data into third-party AI without DPO approval.
    - Maintain data security — encryption, access control and retention schedules.
    - Conduct DPIAs for new or changed AI processing activities involving personal data.
    - Respect data subject rights (access, rectification, erasure) and include AI processing descriptions in the school's privacy notices.

12. SEND and reasonable adjustments

- The SENCO will advise on AI adaptations for pupils with SEND to ensure accessibility and avoid disadvantaging pupils.
- Where AI is used to support learning for pupils with additional needs, decisions will be overseen by staff with appropriate expertise and parental involvement.

13. Training and professional development

- Staff will receive regular CPD on:
    - Safe and effective classroom use of AI
    - Data protection and redaction practices
    - Evaluating AI outputs, bias and misinformation
    - Safeguarding implications
- Governors will receive briefing on AI risks and oversight responsibilities.

14. Monitoring, evaluation and compliance

- The school will maintain an inventory of approved AI tools, their purpose, data processed and review dates.
- The Pupil / IT Lead and DPO will review AI deployments termly and report to governors.
- Random audits of AI use, logs and outcomes will be undertaken to ensure compliance.
- Non-compliance with this policy by staff may result in disciplinary action in line with staff conduct procedures.

15. Incident reporting

- Any AI-related incident (data breach, harmful content, safeguarding concern, inappropriate outputs) must be reported immediately using the Incident Report Template (Appendix C) and to the DPO and DSL as appropriate.
- The school will follow its Data Breach Response and Safeguarding procedures and inform parents/carers where pupil data or wellbeing is affected.

16. Examples of acceptable and restricted uses

Acceptable examples (with human oversight):

- Using AI to generate differentiated lesson starters which staff check and adapt.
- Automated transcription of lessons for accessibility where pupils' consent and data controls are met.
- Curriculum resources produced with AI that are reviewed for accuracy and bias.

Restricted / not permitted:

- Uploading pupil names, images, assessment records, behaviour logs or safeguarding files into public AI chatbots or services without DPO approval.
- Relying on AI for safeguarding decisions, awarding qualifications, or formal assessments without human verification.
- Use of unverified third-party AI tools that store data insecurely or outside permitted jurisdictions.

17. Contracts with third-party providers

- Contracts must include clauses covering:
    - Data processing terms, lawful basis and DPA
    - Security standards and audit rights
    - Breach notifications and liability
    - Clear deletion and retention schedules for pupil data
    - Right to service termination and data return

18. Review

- This policy will be reviewed annually or sooner if there are material changes in technology, regulation or school practice.

If at any time you are unsure whether a specific AI use is permitted, seek advice from the DPO and Headteacher before proceeding.

Appendices

Appendix A — Staff Acceptable Use Agreement (AI)
Please read, sign and return to the Headteacher / IT Lead.
Walverden Primary School — Staff AI Acceptable Use Agreement

I have read and will follow the Walverden Primary School AI Policy.

I will:
- Use only school-approved AI tools for work purposes unless authorised.
- Not upload or share personal data, safeguarding information or SEND plans to unauthorised AI services.
- Redact personal identifiers before creating prompts unless explicitly authorised in writing.
- Critically evaluate and verify AI outputs before using them with pupils or in official documents.
- Report any AI-related safeguarding concerns or data incidents immediately to the DSL and DPO.

Name: _____
Role: _____
Signature: _____ Date: _____

Appendix B — Pupil Acceptable Use Agreement (AI) — age-appropriate
To be displayed in classrooms and copied to parents.
Walverden Primary School — Pupil AI Agreement (short)

- I will only use AI tools when my teacher says it is OK.
- I will not put my name, other pupils' names, photos or private information into AI tools.
- I will treat AI outputs like a help, not as the final answer — I will check and talk about them with my teacher.
- If I see anything from AI that worries me, I will tell my teacher straight away.

Pupil name: _____ Class: _____
Signed (pupil): _____ Date: _____

Appendix C — AI Incident Report Template
Use this for any AI-related incident (data breach, harmful output, safeguarding issue).

AI INCIDENT REPORT

1. Report details
- Date and time reported:
- Reported by (name and role):

2. Incident summary
- Date/time of incident:
- Location (platform / tool / device):
- Brief description of incident:

3. People affected
- Pupil(s) / staff (initials only) affected:
- Any obvious harm or risk to welfare? Yes / No. Details:

4. Data involved
- Type of data involved (e.g. name, image, assessment data, safeguarding note):
- Was personal or special-category data uploaded to an external AI service? Yes / No

5. Immediate actions taken
- Steps to contain/mitigate (e.g. revoked access, deleted uploads, informed provider):
- Staff/pupil support provided:

6. Notifications
- DSL informed: Yes / No (time/date)
- DPO informed: Yes / No (time/date)
- Parents/carers informed: Yes / No (time/date)
- External agencies informed: (e.g. ICO, police, LA) — details:

7. Follow-up actions / review
- Further actions required:
- Root cause and recommended changes to practice or controls:

Completed by: Name / Role / Date

Appendix D — Suggested parental information (letter / web text)

Short text to publish on website or send to parents.

Walverden Primary School — Information about our use of AI

We use carefully selected AI tools to support teaching and learning and to make administrative tasks more efficient. The safety and privacy of pupils are our highest priorities.

Key points:
- We only use school-approved AI tools and assess these for data protection, safety and educational benefit.
- Pupils will use AI only under staff supervision and with age-appropriate guidance.
- We do not upload sensitive pupil information into public AI chatbots. If any pupil data is used in an AI system, we will have explicit safeguards and parental information/consent where necessary.
- If you have questions about a specific AI tool or want to discuss consent, please contact Humma Ahmed/Charlotte Wildman/Zishan Ashraf

Signed: Headteacher — H Ahmed
Date: March 2026

Appendix E — Implementation checklist (for leadership)

- Inventory existing AI tools and services.
- Ensure DPIAs are in place for any data processing by AI.
- Confirm contracts / DPAs with vendors.
- Identify training needs and schedule CPD sessions.
- Publish policy on website and distribute staff/pupil agreements.
- Set monitoring timetable and governor reporting dates.