Ladygrove Primary School and Nursery
Artificial Intelligence (AI) Policy

Written by Max Trusler (Computing Coordinator)

Created: 21.11.25

To be reviewed by: 21.11.26

About this Policy

Ladygrove Primary School is committed to the responsible, ethical, and secure use of Artificial Intelligence (AI) technologies. This policy outlines our approach to implementing AI in alignment with our vision, values, and legal obligations. It provides clear guidance on governance, security, data protection, transparency, and training to ensure AI is used safely and effectively within our school community

Max Trusler
A2168@taw.org.uk

Contents

1. Introduction 2
2. Use of AI 2
3. Governance Requirements for Using AI 3
4. Supplier/Vendor Engagement 3
5. Copyright Considerations 4
6. Accuracy of AI Output 4
7. Confidentiality 4
8. Disclosure and Transparency 4
9. Integration with Other Tools 4
10. AI Risks 5
10.3 Golden Rule for AI Usage 5
11. Compliance with Legal and Regulatory Requirements 6
12. Bias and Discrimination 6
13. Security 6
11. Compliance with Legal and Regulatory Requirements 6
12. Bias and Discrimination 7
13. Security 7
14. Data Sovereignty and Protection 7
15. Training and Awareness 7
16. Compliance 8
17. Review 8

1. Introduction

At **Ladygrove Primary School**, we recognize the growing role of Artificial Intelligence (AI)—the capability of digital systems to perform tasks traditionally associated with human intelligence.

1.1 We understand that using AI technologies, including those that process data such as voice recordings, brings both significant benefits and potential risks.

1.2 To ensure safe and responsible use, **Ladygrove Primary School takes a proactive, risk-based approach to implementing AI. This includes:**

- Carefully assessing any risks to individuals' rights and freedoms when AI is used.
- Applying appropriate technical and organizational measures to reduce and manage these risks effectively.

1.3 Our policy ensures that all AI use within the school complies with relevant laws, regulations, and internal policies. We are committed to promoting ethical and responsible AI practices under the school's guidance.

1.4 This framework applies to everyone involved in school activities—staff (temporary or permanent), Governors, contractors, agents, vendors, and any other parties processing information on behalf of the school.

1.5 As AI technology evolves rapidly, **Ladygrove Primary School will regularly review and update this policy to reflect current legislation, regulatory requirements, and best practices.**

2. Use of AI

2.1 At **Ladygrove Primary School**, any use of AI technologies will always align with our school's vision, priorities, and core values. AI will be implemented only where it enhances teaching, learning, and operational excellence in a way that reflects our commitment to pupils and the wider community.

2.2 Before introducing any AI solution, **Ladygrove Primary School actively engages with key internal stakeholders** to ensure thorough due diligence. At a minimum, we consult with our **Data Protection Officer** and **ICT Support team** for all AI-related projects to guarantee compliance and security.

2.3 During the feasibility stage of any AI initiative, we carefully review:

- Governance requirements and school policies
- Provider practices for any 'off-the-shelf' applications or technologies
- Copyright, confidentiality, and disclosure considerations
- Accuracy of outputs and potential integration with existing tools

2.4 All AI solutions used by **Ladygrove Primary School** will include **robust logging and auditing mechanisms** to track and record activities related to AI usage, ensuring transparency and accountability.

3. Governance Requirements for Using AI

3.1 At **Ladygrove Primary School**, anyone seeking to use or implement AI technology must be fully familiar with our policies and procedures relating to data protection and information management. As a minimum, stakeholders are expected to understand the requirements outlined in the following documents:

- **Data Protection Policy**
- **Information Security Policy**
- **Records Management Policy**
- **Information Sharing Policy**
- **Information Retention Schedule**

3.2 We take a proactive approach to managing risks associated with AI. Before any AI solution is introduced, **Ladygrove Primary School requires a thorough assessment of potential risks and impacts**. To support this process, the following must be completed:

- **AI Risk Assessment**
- **AI Data Protection Impact Assessment**

Templates for these assessments are available from our **Data Protection Officer**.

Both assessments must be reviewed and approved by the **Senior Leadership Team (SLT)**, **ICT team**, **Data Protection Officer**, and the **Governing Board** before any AI solution is permitted for use within the school.

4. Supplier/Vendor Engagement

4.1 When **Ladygrove Primary School** considers procuring AI solutions or technologies, we ensure early engagement with the relevant **Information Asset Owner**, senior leadership, and the developers or vendors involved. This collaborative approach helps us maintain compliance, security, and alignment with our school's objectives.

4.2 To safeguard data and uphold enterprise-level security standards, **Ladygrove Primary School recommends the use of Microsoft Copilot for staff requiring AI tools**.

Microsoft Copilot provides significant benefits from both a **data protection** and **enterprise compliance** perspective, including:

- **Enterprise-grade data protection**: All prompts and responses are protected under the same contractual terms trusted for Microsoft services like Exchange and SharePoint.
- **Encryption at rest and in transit**, rigorous physical security controls, and tenant-level data isolation.
- Respect for identity models and permissions, inheritance of sensitivity labels, application of retention policies, and full audit support for interactions.
- Strict adherence to administrative settings, ensuring data privacy and security.
- A clear commitment that Microsoft will not use school data except as instructed, and **Copilot does not use your data to train foundation models**, keeping proprietary information confidential.

These features make Microsoft Copilot a **secure and reliable choice for AI integration**, supporting our commitment to data protection and compliance.

For more details, see: Enterprise data protection in Microsoft 365 Copilot and Microsoft Copilot (https://learn.microsoft.com/en-us/copilot/microsoft-365/enterprise-data-protection).

5. Copyright Considerations

5.1 At **Ladygrove Primary School**, we ensure full compliance with copyright law when using AI technologies.

5.2 AI must never be used to create content that infringes on the intellectual property rights of others, including copyrighted materials. If there is any uncertainty about whether an intended use of AI could breach copyright, the school will seek advice from its legal support team before proceeding.

6. Accuracy of AI Output

6.1 All information generated by AI solutions must be carefully reviewed by **Ladygrove Primary School** for accuracy before it is shared or used in any capacity.

6.2 If there is any doubt about the accuracy or reliability of AI-generated output, the school will not use that information.

7. Confidentiality

7.1 Personal and confidential information must never be processed using public AI platforms (such as ChatGPT), as this could result in data entering the public domain.

7.2 If the school plans to use a secure, non-public AI solution that involves processing personal data, an **AI Data Protection Impact Assessment** must be completed as a minimum requirement.

7.3 Any processing of personal data through AI solutions must comply fully with the principles of the **UK Data Protection Act 2018**.

8. Disclosure and Transparency

8.1 At **Ladygrove Primary School**, we are committed to transparency when using AI-generated content. If AI is used to create or assist in producing content, this must be clearly disclosed. Any documents or publications containing AI-generated material should include a statement such as:

"Note: This document contains content generated by Artificial Intelligence (AI). AI-generated content has been reviewed by the author for accuracy and edited/revised where necessary. The author takes responsibility for this content."

9. Integration with Other Tools

9.1 When integrating AI with other tools through APIs or plugins, **Ladygrove Primary School follows best practices to ensure safety and reliability**, including:

- **Adversarial testing** – testing AI with typical scenarios and attempts to 'break' the system
- **Human-in-the-loop (HITL)** – ensuring a person reviews AI output before wider use
- **Prompt engineering** – reducing the chance of undesired content
- **Know Your Customer (KYC)** – requiring user registration and unique IDs for AI access
- **Constrain user input and limit output tokens** – minimizing misuse and errors
- **Issue reporting mechanism** – enabling users to log concerns about AI performance
- **Communicating limitations** – identifying and sharing any risks of offensive or discriminatory content
- **End-user IDs** – using unique IDs to detect improper use

9.2 All relevant API and plugin tools must undergo rigorous testing for:

- **Moderation** – ensuring AI can handle inappropriate input (e.g., hate speech, discriminatory or threatening content)
- **Factual accuracy** – establishing a ground truth and reviewing AI responses against it

10. AI Risks

10.1 At **Ladygrove Primary School**, we recognize that the use of AI carries inherent risks. Before any AI solution or technology is implemented, a **thorough risk assessment** must be completed. (See Section 3.2 for required assessments.)

10.2 Each AI project is unique, with its own context, data flows, and output requirements. Therefore, every project will be assessed individually against the core requirements of this policy. Completing both the **AI Risk Assessment** and the **AI Data Protection Impact Assessment** ensures that risks are identified, mitigated, and managed effectively.

10.3 Golden Rule for AI Usage

When using AI solutions, **Ladygrove Primary School strictly adheres to the golden rule**: **Do not input any identifiable, personal, confidential, or sensitive information into any AI platform.**

This includes, but is not limited to:

- Personal identification numbers (e.g., passport numbers)
- Financial information (e.g., credit card or bank details)
- Health information (e.g., medical records)
- Confidential business information (e.g., trade secrets, proprietary data)
- Any information that could identify an individual or compromise their privacy
- Identifiable student information (e.g., names, student IDs, academic records)

By following this rule, we protect individual privacy and maintain the confidentiality and integrity of sensitive data. **Always consult with the Data Protection Officer and ICT Support before using AI solutions to process any data that may fall into these categories.**

11. Compliance with Legal and Regulatory Requirements

11.1 At **Ladygrove Primary School**, we understand that data processed by public-facing AI solutions may enter the public domain, creating risks such as personal data breaches, breaches of confidentiality, and compromise of intellectual property.

11.2 We ensure that all AI use complies fully with applicable laws, regulations, and school policies at all times.

11.3 The unauthorized use of copyrighted material or creation of content that infringes on intellectual property rights is strictly prohibited.

12. Bias and Discrimination

12.1 Some AI solutions may generate biased, discriminatory, or offensive content. **Ladygrove Primary School takes this risk seriously and requires that all AI outputs are reviewed by a human before use**, ensuring that any inappropriate content is identified and removed.

13. Security

13.1 Ladygrove Primary School is committed to protecting the confidentiality, integrity, and availability of its data.

13.2 AI solutions may store personal, sensitive, or confidential information, which could be at risk if the technology is compromised.

13.3 Before implementing any AI solution, we ensure that the technology is secure and that technical controls are proportionate to the level of risk associated with the data being processed.

13.4 Where personal data is processed, we investigate whether this data can be anonymized.

13.5 All data processed by AI solutions must be encrypted both in transit and at rest.

13.6 AI solutions should hold appropriate security accreditations such as **ISO 27001** or **Cyber Essentials+**. If cloud computing is used, compliance with the **NCSC 14 Principles of Cloud Security** is required.

13.7 The level of security for any proposed AI solution must be verified with the **ICT Support team** and **Data Protection Officer** before implementation.

11. Compliance with Legal and Regulatory Requirements

11.1 At **Ladygrove Primary School**, we recognize that data processed by public-facing AI solutions may enter the public domain, creating risks such as personal data breaches, breaches of confidentiality, and compromise of intellectual property.

11.2 We ensure that all AI use complies fully with applicable laws, regulations, and school policies at all times.

11.3 The unauthorized use of copyrighted material or creation of content that infringes on intellectual property rights is strictly prohibited.

12. Bias and Discrimination

12.1 Some AI solutions may generate biased, discriminatory, or offensive content. **Ladygrove Primary School requires that all AI outputs are reviewed by a human before use**, ensuring that any inappropriate content is identified and removed.

13. Security

13.1 Ladygrove Primary School is committed to protecting the confidentiality, integrity, and availability of its data.

13.2 AI solutions may store personal, sensitive, or confidential information, which could be at risk if the technology is compromised.

13.3 Before implementing any AI solution, we ensure that the technology is secure and that technical controls are proportionate to the level of risk associated with the data being processed.

13.4 Where personal data is processed, we investigate whether this data can be anonymized.

13.5 All data processed by AI solutions must be encrypted both in transit and at rest.

13.6 AI solutions should hold appropriate security accreditations such as **ISO 27001** or **Cyber Essentials+**. If cloud computing is used, compliance with the **NCSC 14 Principles of Cloud Security** is required.

13.7 The level of security for any proposed AI solution must be verified with the **ICT Support team** and **Data Protection Officer** before implementation.

14. Data Sovereignty and Protection

14.1 At **Ladygrove Primary School**, we understand that many AI solutions are hosted internationally. However, under data sovereignty rules, any information created or collected in the originating country remains subject to that country's laws.

14.2 Before using any AI solution, we check its data sovereignty practices to ensure compliance. If these practices cannot be determined, the school will seek guidance from the **Data Protection Officer** before proceeding.

15. Training and Awareness

15.1 All users of AI solutions at **Ladygrove Primary School** will receive training on the responsible and secure use of AI. This training will cover:

- Ethical considerations
- Risk management
- Security requirements
- Compliance with legal and regulatory standards

16. Compliance

16.1 This policy applies to all uses of AI solutions and technologies within **Ladygrove Primary School**.

16.2 Any suspected or confirmed security incidents related to AI usage must be reported immediately to the **Data Protection Officer**.

16.3 Failure to comply with this policy may result in disciplinary action.

17. Review

17.1 This policy will be reviewed regularly and updated as needed to ensure continued compliance with relevant legislation, regulations, other school policies, and best practice.

This policy has been written by Max Trusler (Computing Co-ordinator) in consultation with SLT, Staff, Governors and the T&W Data Protection Officer.

Policy- Document Status			
Date of Policy Creation	September 2022 – Reviewed every years.	**Named Responsibility**	Max Trusler
Date of review completion	21.11.25	**Named Responsibility**	Pupils, Staff, Parents and Governors.
Inception of new Policy	21.11.25	**Named Responsibility**	Max Trusler
Date of Policy Adoption by Governing Body		21.11.25	