Throston Primary School

A Flying Start To Success

Artificial Intelligence Policy

Date Policy Agreed by the Full Governing Body:

Monday 6th October 2025

Date of Next Review:

October 2026

CONTENTS

ARTIFICIAL INTELLIGENCE POLICY

Ensuring Safe, Ethical, and Responsible Use of AI in Education

Foreword

This policy has been created in conjunction with out safeguarding advisors, Helen Hogan: Safeguarding Matters to provide clarity to all stakeholders in school on the safe, ethical and responsible use of Artificial Intelligence (AI).

Introduction

This policy sets out the expectations and guidelines for the use of artificial intelligence (AI) within Throston Primary School, ensuring compliance with safeguarding regulations and ethical considerations.

Purpose and aim

The purpose of this policy is to promote the safe and responsible integration of AI in teaching and administration, whilst at the same time safeguarding children and staff from potential risks associated with AI technologies.

This policy also ensures compliance with data protection and child protection laws, including GDPR and statutory safeguarding guidance.

Acceptable Use of AI

AI tools may be used for the benefit and enhancement of learning for children in a variety of positive ways, including through lesson planning and delivery, to support and improve administration functions to improve efficiency and to support children with special educational needs or additional vulnerability to improve and enhance learning opportunities.

Safeguarding Considerations

As with all newly evolving technology there are risks associated with the use of AI in schools. These risks include the impact on Data Privacy. School will ensure that all AI tools that are accessed comply with the GDPR and do not store or process personal student data unlawfully.

Another risk includes the bias and misinformation that is produced by AI, this will be heavily monitored by school to prevent inaccuracies or biased perspectives being taught or shared in the classroom.

Furthermore, school will take all necessary steps to prevent the risk of any AI interactions that expose students to harmful or inappropriate material.

Finally, school will ensure that while AI is accessed it does not replace human judgment in safeguarding decisions.

Safeguarding Measures

The school will ensure that safeguarding measures are in place to reduce and mitigate the risk of harm to children (including misinformation, disinformation (including fake news) and conspiracy theories

(KCSIE, 2025). This means that all AI systems used in the school will be assessed for compliance with safeguarding and data protection laws. Alongside this, school will ensure that all staff receive training on AI-related risks and responsible usage and are confident in accessing any of the AI tools available.

All staff will ensure that AI generated content used in teaching is vetted for accuracy and appropriateness.

AI tools will never be used for decisions making in safeguarding concerns. This will always be a decision made by Designated Safeguarding Leads.

Responding to AI-Related Safeguarding Risks

If a safeguarding concern arises due to AI usage, Throston Primary School will take the following steps:

- Immediate Assessment – Staff will assess the nature and severity of the concern. This could involve AI-generated content that is inappropriate, biased, misleading, or violating data protection laws.
- Reporting Procedures – Any safeguarding concerns will be reported to the Designated Safeguarding Lead (DSL).
- Staff will record the incident, including the AI tool involved, its output, and any potential risks identified.

Risk Mitigation Measures

- School will immediately restrict the AI tool in question while further investigation occurs.
- School will ensure that any affected students or staff receive appropriate support, including intervention from the Designated Safeguarding Lead if necessary.

Investigation & Decision-Making

Following the incident, the DSL, along with senior leadership and IT specialists, will investigate to determine the root cause and whether AI misuse, bias, or data exposure occurred.

If the AI tool was responsible for exposing students to harmful material, it will be permanently removed or adjusted appropriately to ensure it is compliant.

Parent/Carer & Stakeholder Communication

Where relevant, parents and guardians will be informed immediately of any safeguarding risks involving AI.

Designated Safeguarding Leads will seek advice and guidance from external safeguarding agencies if the risk has broader implications, such as online safety threats. This may include contacting statutory agencies including the police and children's service social care.

The Law around Online Safety Incidents

From the 25.07.2025 there is a new law around online age verification on pornography sites. Platforms must use **highly effective methods** to verify users' ages before showing any pornographic material.

Accepted Verification Methods

Sites may use one or more of the following:

- **Facial age estimation** via photo or video
- **Open banking** checks to confirm age via financial data
- **Digital identity wallets** storing verified age credentials
- **Credit card verification**
- **Photo ID matching** (e.g. passport or driving licence)
- **Mobile network age filters**
- **Email-based age estimation** using linked services like banks or utilities.

The Online Safety Act 2023

New Communications Offences

These are designed to replace and modernise older laws under the Malicious Communications

Act 1988 and Communications Act 2003:

- **False Communications (Section 179)**
  Sending a message that the sender knows is false, intending to cause non-trivial psychological or physical harm to a likely audience.
- **Threatening Communications (Section 181)**
  Sending a message that conveys a threat of death or serious harm (including GBH, rape, or serious financial loss), intending or being reckless as to whether someone fears it will be carried out.
- **Flashing Images Offence (Section 183)**
  Sending or showing flashing images electronically with intent to cause harm—particularly targeting individuals with epilepsy (known as *Zach's Law*).
- **Encouraging or Assisting Serious Self-Harm (Section 184)**
  Doing any act (including sending or showing content) intended to encourage or assist serious self-harm, even if no harm occurs.

Sexual Image Offences (Amendments to Sexual Offences Act 2003)

These expand protections against non-consensual image sharing:

- **Cyber-Flashing (Section 66A)**
  Sending unsolicited images of genitals with intent to cause alarm, distress, or for sexual gratification.

- **Sharing or Threatening to Share Intimate Images (Section 66B)**
  Includes revenge porn, deepfakes, and down-blousing. Covers both actual sharing and threats to share, even if the image is fake.

Other Notable Offences

- **False Reporting of Child Sexual Abuse to the NCA (Section 69)**
  Criminalises knowingly making false reports of child sexual exploitation or abuse to the National Crime Agency.

Policy Review & Staff Training

This AI policy will be reviewed and updated to prevent future safeguarding concerns.

All Staff will receive additional training on AI-related risks and responsible usage to reinforce best practices as and when new technology emerges or new systems are integrated into school.

Ongoing Monitoring & Safeguarding Compliance

AI usage in the school will be continually monitored to identify any emerging risks. Throston Primary School will undertake regular safeguarding training to ensure compliance with relevant laws and best practices.

Staff Roles & Responsibilities

It is the role of the School Leadership Team to oversee AI integration and ensure safeguarding compliance. All school staff must use AI responsibly and report safeguarding concerns immediately to the Designated Safeguarding Lead.

The ICT leads in school will ensure technical safety and adherence to cybersecurity best practices and inform the School Leadership Team and the Designated Safeguarding Lead of any incidents in school.

Children and parents will continue to receive regular education and learning on the risks and benefits of AI and safe digital engagement.