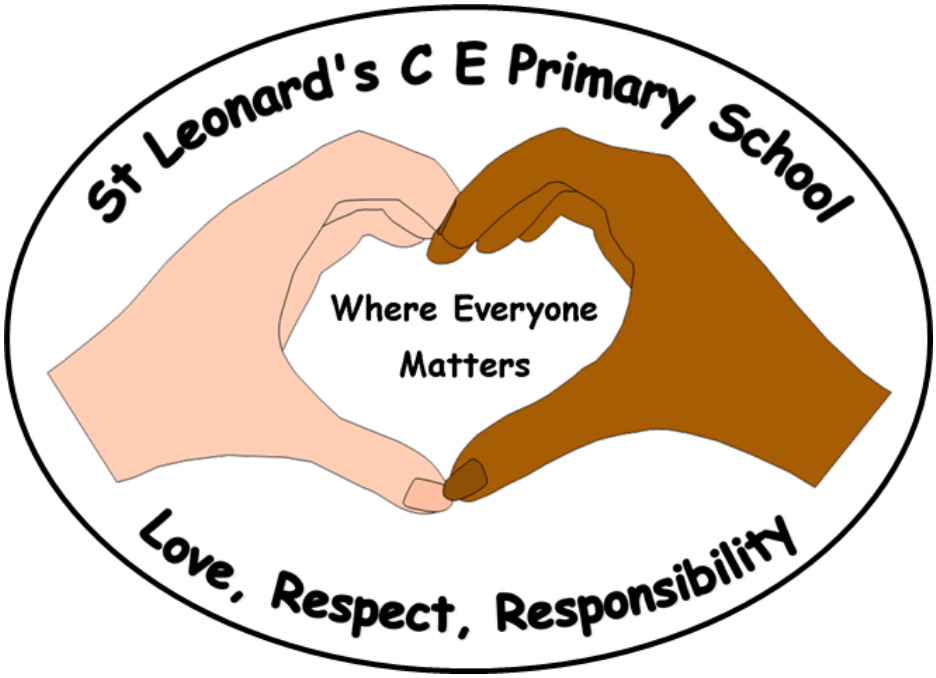
AI Policy



Approved by:	**Full Governing Body**
Date:	**September 2026**
Next review due by:	**September 2028**

Contents

1. Intent 2
2. Related policies 2
3. Implementation 2
4. Responsibilities..... 3
5. Vulnerable groups 4
6. Reporting 4
7. Responding to an incident or disclosure 4
8. Risk assessment ……...5
9. Education ……5
10. Training ……6
11. Appendices ……...7

Intent

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

Related policies

This policy should be read in conjunction with other school policies:

- Data Protection Policy
- Staff codes of conduct
- Behaviour policy
- Anti-bullying policy
- Online safety policy
- Acceptable Use Agreements
- Computing and PSHE Policies

Implementation

- The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.

- We will ensure that, within our education programmes, learners understand the ethics and use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.
- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognize and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks. (Risk assessment matrices are attached as an appendix)
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in our 'Staff Code of Conduct' and 'Allegation Management Policy'.

Responsibilities

Headteacher, Senior Leaders and Computing Lead

Are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

Designated Safeguarding Leads (DSL) and Deputy Designated Safeguarding Leads (DDSLs), PSHE and Computing Leaders

Our Designated Safeguarding Lead, Deputy Safeguarding Lead, PSHE and Computing Leaders has responsibility for online safety in the school. They are expected to have knowledge of AI and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Data Protection Officer

The DPO will be responsible for providing advice and guidance about data protection obligations in relation to the use of AI, including related Data Protection Impact Assessments (DPIAs).

Technical Staff

ICT 123 Technical staff, DSLs and DDSLs and the Computing Lead will be responsible for technical support and guidance, with particular regard to cyber-security and the effectiveness of filtering and monitoring systems. At St Leonard's CE Primary School, we work with ICT 123 and have made them aware of the contents of this policy.

Staff

It is the responsibility of all staff to have read and understood this policy and associated Acceptable Use Agreements. All staff must report any incidents or suspected incidents concerning the use of AI in line with school policy. All staff will challenge any inappropriate behaviour. Staff have a duty to ensure that:

- the school environment is safe
- sensitive and confidential data / information is secure
- that their actions do not put the reputation of the school at risk and that
- learners understand their responsibilities

Governors

We ensure that our governing body has a good understanding of how AI is used in a school context and potential benefits and risks of its use. They receive regular training and updates, enabling them to support the school and challenge where necessary. This may include evaluation of the use of AI in the curriculum, administration and communications, ensuring that risks relating to these issues are identified, that reporting routes are available, and that risks are effectively mitigated. The Curriculum Committee will take lead responsibility for overseeing the use of AI at St Leonard's CE Primary School.

Parents/carers

We work hard to engage parents and carers by:

- regular items in the fortnightly school newsletters
- sharing information online e.g., school website, social media
- providing termly curriculum information via Class Dojo

Our parents and carers are made aware of how AI is used in school and receive guidance on both good practice in its use and the risks of misuse that may affect their childrens' learning or safety. They are encouraged to report any concerns to the school and are made aware that all incidents will be handled with care and sensitivity.

Vulnerable groups

We recognise that vulnerable learners are more likely to be at risk from the misuse of AI (both in their own use or through the actions of others). We ensure that vulnerable learners are offered appropriate support to allow them to gain full benefit of the use of AI, while being aware of the potential risks.

Children are considered to be vulnerable data subjects and therefore any process involving their personal data is likely to be "high risk". If an AI/ automated process is used to make significant decisions about people, this is likely to trigger the need for a Data Protection Impact Assessment (DPIA).

Reporting

Our reporting systems are well promoted, easily understood and easily accessible for staff, learners and parents/carers to confidently report issues and concerns, knowing these will be treated seriously. All

reports will be dealt with swiftly and sensitively and outcomes shared where appropriate. We also respond to anonymous reports, or reports made by third parties. This can be done via:

- nominated member of staff - DSLs and Deputy DSLs
- established school reporting mechanisms - CPOMS, Dealing with Allegations against staff and volunteers, Complaints procedures
- Headteacher, Chair of Governors and OCC DPO

Responding to an incident or disclosure

Our response is always based on sound safeguarding principles and follows school safeguarding and disciplinary processes. It is calm, considered and appropriate and puts the learner at the centre of all decisions made.

- All AI incidents (including data breaches and/or inappropriate outputs) must be reported promptly to the relevant internal teams. Effective reporting helps mitigate risks and facilitates a prompt response.
- Where relevant / required incidents will be reported to external agencies e.g., Police, LADO, DPO, ICO.
- All AI related incidents will be recorded through the school's normal recording systems

In the case of misuse of AI by staff, the normal staff disciplinary processes will be followed.

Risk assessment

It is key that our approach to managing risk aligns with, and complements, our broader safeguarding approach.

The school understands that despite many positive benefits in the use of AI, there are some risks that will need to be identified and managed, including:

- Legal, commercial, security and ethical risks
- Data Protection
- Cyber Security
- Fraud
- Safeguarding and well-being
- Duty of care

Education

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include:

- Computing lessons (utilising NCCE Teach Computing and Project Evolve)
- PSHE
- School collective worship (assemblies)
- Participation in Safer Internet Day
- SCIB and SCARF workshops
- External visits from organisations such as the Police
- Junior Citizen Trip (Year Six)

Our approach is given the time it deserves and is authentic i.e., based on current issues nationally, locally and within our school's risk profile. It is shaped and evaluated by learners and other members of the school community to ensure that it is dynamic, evolving and based on need. We do this through:

- Learner assessment
- Critical evaluation of emerging trends and research findings
- Parental engagement
- Staff consultation
- Engaging with learners
- Staff training

The following resources may be used for guidance:

- UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (including updated AI reference)
- ProjectEVOLVE - https://projectevolve.co.uk
- UKCIS DSIT "Education for a Connected World"
- Welsh Government - Generative AI – Hwb guidance - Resources, guidance and information for education practitioners, learners, and families on generative AI.

Training

As AI becomes an integral part of modern education, it is essential for staff to be trained in its effective use. Training equips educators with the knowledge and skills to integrate AI tools responsibly into teaching, learning, and administrative processes. It ensures that AI is used to enhance educational outcomes, streamline workloads, and promote equity while safeguarding ethical practices and data privacy. By fostering AI literacy, staff can confidently prepare pupils for a future where AI is a key driver of innovation and opportunity.

- We will provide comprehensive training to all staff on the effective, responsible, and ethical use of AI technologies in education, ensuring these tools enhance teaching, learning, and administrative processes.
- We will integrate AI-related risks and safeguards into annual safeguarding training, aligning with statutory guidance, including "Keeping Learners Safe."
- We will ensure all staff are equipped with the knowledge and skills to confidently integrate AI into their professional practice and to prepare pupils for a future shaped by AI-driven innovation and opportunities.
- We will train staff to identify, assess, and mitigate risks associated with AI technologies, including issues such as biased algorithms, privacy breaches, and harmful content.
- We will train staff on robust data protection practices, ensuring compliance with UK GDPR and other relevant regulations while using AI systems.
- We will promote ethical practices in the use of AI, ensuring that these technologies contribute to equity, fairness, and inclusivity in education.

- We will empower educators to teach learners about the safe and ethical use of AI, cultivating a culture of awareness, resilience, and informed decision-making in the digital age.
- We will train staff to use AI responsibly as a tool to monitor and address online risks, reinforcing our commitment to a safe learning environment.

Appendix C6a - Risk Assessment Matrix for Schools Implementing AI

Introduction

The following risk assessment matrix is intended to help schools identify, evaluate, and mitigate risks associated with implementing Artificial Intelligence (AI) in educational processes.

Risk Mitigation Matrix

Risk Area	Risk Description	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.	Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.	Monitor AI communication tools, implement clear reporting mechanisms, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.	Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulation	AI systems unintentionally affecting student mental health through curated content.	Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing learners to harmful or unsuitable materials / behaviour	Conduct rigorous testing of AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.	Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or inclusion. AI models producing discriminatory or biased outcomes.	Regularly audit AI algorithms for bias and provide inclusive media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).	Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.	Educate staff and learners to verify AI outputs and establish clear policies for verifying content authenticity.
Digital Divide	Inequitable access to AI tools among learners from diverse demographic groups.	Provide equitable access to AI resources and ensure alternative solutions are available.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.	Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.	Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and learner data.	Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.	Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Appendix C6b – Staff Use of AI Acceptable Use Agreement

Artificial Intelligence (AI) and Emerging Technologies Staff (and Volunteer) Acceptable Use Agreement

School Policy

Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalized learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

1. Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
2. School systems and users are protected from misuse or harm resulting from the use of AI.
3. Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

1. I understand that the school may monitor my use of AI tools and technologies.
2. I will only use AI tools and technologies for purposes authorized by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
3. I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
4. I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

1. I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.
2. I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
3. I will communicate professionally and responsibly when using AI systems.
4. I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

1. I will support learners on the safe, ethical, appropriate and effective use of AI.
2. I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

1. I will use AI systems in compliance with established security measures and access protocols.
2. I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.
3. I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

1. I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.
2. I will ensure I have explicit authorisation when uploading sensitive school-related information into generative AI systems.

Responsibility and Accountability:

1. I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
2. I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
3. I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.