ST. LUKE'S CHURCH OF ENGLAND PRIMARY SCHOOL

Church Lane
Lowton ☎ **01942 201140**
Warrington
WA3 2PW **web** **www.saintlukes.wigan.sch.uk**
Headteacher: Mr S Hardaker e-mail **enquiries@admin.saintlukes.wigan.sch.uk**

ONLINE SAFETY POLICY

Policy Date: October 2026
Review Date: October 2027

OUR CHRISTIAN VISION

St Luke's is built on a core set of Christian values, where children feel happy and cared for. Here they find love, joy, hope and peace.
John 13:34-35 reminds us:
"Love one another. As I have loved you. By this everyone will know that you are my disciples."
At St Luke's we seek to:

- Follow in God's way
- Learn day by day
- Work with one another
- Care for each other

These principles extend to the digital world. We aim to ensure that all members of our school community use technology safely, responsibly and respectfully.

1. POLICY STATEMENT

Online safety is a safeguarding issue.
The Internet, social media, gaming platforms, messaging services and Artificial Intelligence (AI) technologies present significant educational opportunities but also potential risks.
St Luke's recognises that children increasingly access online content through:

- Tablets
- Mobile phones
- Gaming devices
- Smart TVs
- Smart watches
- AI-powered tools and chatbots
- Social media platforms
- Streaming services

The school is committed to providing an environment in which pupils, staff and families can use digital technologies safely.
This policy operates alongside:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Remote Learning Policy

2. LEGISLATIVE FRAMEWORK

This policy has been written with due regard to:

- Keeping Children Safe in Education (KCSIE) 2026
- Children Act 1989 and 2004
- Education Act 2002
- Education Act 2011

- Data Protection Act 2018
- UK GDPR
- Online Safety Act 2023
- Prevent Duty Guidance
- Working Together to Safeguard Children
- DfE Filtering and Monitoring Standards
- UK Council for Internet Safety (UKCIS) Guidance
- DfE Guidance on Generative Artificial Intelligence in Education

These documents place clear responsibilities on schools to maintain effective filtering, monitoring and safeguarding systems and to address emerging risks including AI-generated content, misinformation and online exploitation.

3. AIMS

This policy aims to:

- Safeguard pupils and staff online.
- Establish clear expectations for digital behaviour.
- Promote digital resilience.
- Educate pupils to use technology safely and responsibly.
- Protect personal information.
- Ensure compliance with safeguarding and data protection legislation.
- Address emerging online risks including generative artificial intelligence and deepfake technology.

4. DEFINITIONS OF ONLINE RISK

The school recognises the UK's "4Cs" model of online risk:

Content

Exposure to harmful, misleading or inappropriate material.

Examples:

- Extremist content
- Pornographic material
- Self-harm content
- Misinformation and disinformation
- Deepfakes
- AI-generated harmful content

Contact

Harm arising from interaction with others.

Examples:

- Grooming
- Radicalisation
- Sexual exploitation
- Online coercion
- Scams and fraud

Conduct

Behaviour risks relating to a child's own actions online.

Examples:

- Cyberbullying
- Sharing images without consent
- Harassment
- Creating or distributing inappropriate content

Commerce

Risks linked to financial exploitation.

Examples:

- In-app purchases
- Online gambling
- Loot boxes
- Fraudulent subscriptions
- Digital scams

KCSIE now explicitly highlights misinformation, disinformation and conspiracy theories as safeguarding concerns which schools should address through education and monitoring.

5. ARTIFICIAL INTELLIGENCE (AI)

Principles

The school recognises that AI technologies are becoming increasingly common in education and wider society.
AI may support:

- Learning
- Administrative workload reduction
- Curriculum planning
- Accessibility

However AI creates specific safeguarding risks including:

- Deepfake images and videos
- Misinformation
- Bias and discrimination
- Inaccurate information ("hallucinations")
- Exposure to inappropriate content
- Manipulation and grooming
- Data privacy breaches

The school will:

For Staff

- Use only approved AI tools.
- Never input confidential pupil information into public AI platforms.
- Verify all AI-generated content before use.
- Follow school data protection procedures.
- Maintain professional judgement at all times.

For Pupils

Pupils may only use AI systems approved by school staff.
Children will be taught:

- AI can make mistakes.
- AI-generated information should be checked.
- Not everything online is real.
- Images and videos can be manipulated.
- Personal information must never be shared with AI systems.

Schools are expected to consider AI within filtering, monitoring and safeguarding arrangements.

6. CURRICULUM

Online safety is taught through:

Computing

Children learn:

- Safe searching
- Password security
- Data protection
- Digital citizenship
- Evaluating online information
- AI awareness

PSHE and RSHE

Children learn:

- Healthy online relationships
- Consent
- Peer pressure
- Cyberbullying
- Managing online reputation
- Respectful communication

Collective Worship and Christian Values

Children consider:

- Kindness
- Respect
- Responsibility
- Truthfulness
- Compassion online

Online safety education is embedded throughout the curriculum and is not limited to Computing lessons.

7. FILTERING AND MONITORING
The Governing Body and Headteacher ensure effective filtering and monitoring systems are in place.
The school will:
- Filter inappropriate content.
- Monitor digital activity.
- Review systems annually.
- Work with IT providers to identify emerging risks.
- Ensure systems are proportionate and age appropriate.

The DSL will understand:
- Filtering arrangements
- Monitoring arrangements
- Escalation procedures
- Reporting systems

KCSIE and DfE Standards require schools to maintain effective filtering and monitoring and regularly review their effectiveness.

8. CYBERBULLYING
Cyberbullying includes:
- Offensive messages
- Harassment
- Threats
- Excluding others online
- Sharing images without consent
- Anonymous abuse

All incidents will be investigated promptly.
Sanctions will be applied in line with:
- Behaviour Policy
- Anti-Bullying Policy
- Safeguarding Procedures

Where criminal activity is suspected, the Police may be involved.

9. CHILD-ON-CHILD ABUSE ONLINE
The school adopts a zero-tolerance approach to:
- Sexual harassment
- Sexual violence
- Sharing indecent images
- Online abuse
- Peer-on-peer exploitation

Any concerns will be managed in accordance with safeguarding procedures and statutory guidance.

10. SOCIAL MEDIA
Pupils
Most social media platforms have minimum age restrictions.
The school actively discourages under-age use of social media.
Staff
Staff must:
- Maintain professional boundaries.
- Not accept pupils as friends or followers.
- Not communicate with pupils via personal accounts.
- Protect the reputation of the school.

Parents
Parents are encouraged to:
- Raise concerns directly with school.
- Use social media responsibly.
- Avoid posting content which identifies pupils without consent.

11. DATA PROTECTION
The school will:
- Process information lawfully.
- Protect personal data.
- Ensure secure storage.

- Control access to sensitive information.
- Follow UK GDPR and Data Protection Act requirements.

Special care will be taken when using cloud and AI-based systems to ensure personal information remains secure.

12. PHOTOGRAPHY, VIDEO AND IMAGES

The school will:

- Obtain parental consent.
- Store images securely.
- Use images appropriately.
- Respect privacy rights.

Children will be taught that:

- Images can be altered.
- Deepfakes can be created using AI.
- Not all online images are genuine.

13. MOBILE PHONES AND DEVICES

Pupils in Years 5 and 6 who walk home independently may bring mobile phones.

Phones must:

- Be switched off.
- Be handed to the school office.
- Remain securely stored during the day.

Staff personal devices must not be used in the presence of pupils except in exceptional circumstances.

14. REPORTING CONCERNS

Any online safety concern must be reported immediately to:

Designated Safeguarding Lead

Mr Steve Hardaker

Deputy DSLs

(Insert current Deputy DSL names)

Concerns may include:

- Grooming
- Online exploitation
- Cyberbullying
- Harmful content
- Sextortion
- Radicalisation
- AI-generated abuse
- Deepfake images
- Sharing of indecent images

The school will work with:

- Children's Social Care
- Police
- LADO
- Multi-agency safeguarding partners
- Internet providers where appropriate

15. WORKING WITH PARENTS

Parents play a crucial role in safeguarding children online.

The school will support families through:

- Parent workshops
- Newsletters
- Website resources
- Safer Internet Day activities
- Information on emerging technologies

Advice will include:

- Age restrictions
- Screen time
- Privacy settings
- AI awareness
- Cyberbullying prevention

- Online gaming safety

16. MONITORING AND REVIEW

This policy will be:

- Reviewed annually.
- Reviewed following safeguarding incidents.
- Updated following legislative changes.
- Approved by Governors.

The Headteacher and Governing Body will ensure the policy remains effective in meeting current safeguarding requirements

Appendix A: Artificial Intelligence (AI) Acceptable Use Guidance for Staff and Pupils
St Luke's CE Primary School

Purpose

Artificial Intelligence (AI) is becoming an increasingly common part of education and everyday life. AI tools can support learning, creativity, communication and productivity; however, they can also present safeguarding, privacy and misinformation risks. The school is committed to ensuring that AI is used safely, responsibly and ethically. The Department for Education expects schools to consider AI within their safeguarding, filtering, monitoring and data protection arrangements.

Guidance for Staff

Staff may use approved AI tools to support professional practice where authorised by the school.
Staff must:

- Use AI to support, not replace, professional judgement.
- Check and verify all AI-generated content before using it with pupils, parents or colleagues.
- Ensure all resources remain accurate, age-appropriate and inclusive.
- Use only school-approved AI platforms and applications.
- Follow all school safeguarding, data protection and confidentiality procedures.
- Consider risks of bias, inaccuracy and misinformation in AI-generated content.

Staff must not:

- Enter confidential, sensitive or personally identifiable information about pupils, staff or families into public AI tools.
- Use AI to make safeguarding, SEND, disciplinary or welfare decisions without appropriate professional oversight.
- Present AI-generated content as fact without checking its accuracy.
- Upload photographs, videos or recordings of pupils to AI systems unless authorised and compliant with data protection requirements.

Guidance for Pupils

Pupils may only use AI tools that have been approved by the school and supervised by a member of staff.
Pupils will be taught to:

- Use AI respectfully and responsibly.
- Check information from AI using trusted sources.
- Understand that AI can make mistakes.
- Ask an adult if they are unsure about something AI has produced.
- Use AI to support their learning rather than complete work dishonestly.
- Report anything online that makes them feel worried, unsafe or uncomfortable.

Pupils must never:

- Share personal information with AI systems.
- Use AI to create unkind, harmful, bullying or inappropriate content.
- Attempt to bypass school filtering or monitoring systems.
- Use AI to create fake images, videos or recordings of others.
- Use AI to cheat, plagiarise or misrepresent their own work.

Deepfakes, Misinformation and Online Safety

Staff and pupils should be aware that AI can create highly realistic text, images, audio and videos known as "deepfakes".
Everyone in the school community should:

- Think critically about online content.
- Question whether information is genuine and accurate.
- Be cautious of manipulated images, videos and voice recordings.
- Report concerning or harmful content to a trusted adult immediately.

The school recognises misinformation, disinformation and manipulated content as emerging online safety risks and teaches pupils how to recognise and respond appropriately.

Safeguarding and Reporting Concerns

Any concerns regarding AI misuse, inappropriate content, privacy breaches, cyberbullying, deepfake images, online exploitation or safeguarding risks must be reported immediately to the Designated Safeguarding Lead (DSL).
The school will investigate concerns and respond in line with its:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Online Safety Policy
- Data Protection Policy