



St Leonard's C of E (A) Primary School

Online Safety Policy

Date written: **February 2026**

Date for review: **February 2027**

Reviewed by: Louise Lowe

Headteacher: Kirsty Cullen

Contents

Statement of Intent

1. Legal Framework
2. Policy Aims
3. Policy Scope
 - 3.1 Links to other Policies and Practices
4. Monitoring and Review
 - 4.1 Filtering, Monitoring and Technical Safeguards
5. Roles and Responsibilities
6. Teaching and Learning
7. Pupil email
8. Social Media/Networking
9. Use of Artificial Intelligence
10. Mobile phones and devices
11. Educational Use of Video conferencing and Webcams
12. The School Website and Published Content
13. E-safety beyond the school gates
14. Reporting Incidents

Statement of Intent

As a Church school, we, at St Leonard's, are committed to providing a caring, inclusive, and safe environment where every child is valued as an individual and encouraged to flourish academically, socially, and spiritually. Safeguarding the wellbeing of our pupils is central to our Christian ethos, and this includes ensuring that children learn to use digital technologies safely, responsibly, and with integrity.

Digital technologies play an important role in learning, communication, and everyday life. While they provide many valuable educational opportunities, they also present potential risks that must be carefully managed. This Online Safety Policy sets out how the school works to protect pupils, staff, and the wider school community from online harm, while supporting pupils to develop the knowledge, skills, and values needed to become thoughtful and responsible digital citizens.

In partnership with parents, carers, governors, and the wider community, the school is committed to promoting safe online behaviour, encouraging respect and kindness in all forms of communication, and ensuring that technology is used in ways that reflect our shared Christian values of responsibility, honesty, and care for others.

This policy supports statutory safeguarding duties, aligns with safeguarding guidance.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images,

and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.

- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE 'Filtering and monitoring standards for schools and colleges'
- DfE 'Harmful online challenges and online hoaxes'
- DfE 'Keeping children safe in education 2025'
- DfE 'Teaching online safety in school'
- DfE 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement
- Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Relationship and Behaviour Policy
- GDPR Data Protection Policy

2. Policy Aims

This online safety policy has been written by St Leonard's Primary School. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2023, the updated Early Years and Foundation Stage 2024 and 'Working Together to Safeguard Children' 2023.

The school aims to:

- Provide a secure digital environment for pupils, staff, and visitors
- Educate pupils in safe, responsible, and respectful online behaviour
- Prevent exposure to harmful or inappropriate content
- Protect personal and sensitive data
- Ensure all adults understand their safeguarding responsibilities in relation to technology
- Promote digital resilience, critical thinking, and responsible use of emerging technologies

3. Policy Scope

This policy applies to:

- All pupils enrolled at the school
- Teaching and non-teaching staff
- Governors, volunteers, contractors, and visitors
- All school ICT systems, networks, and platforms
- All school-owned and personal devices used on school premises or during school activities, including trips and remote learning

3.1 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Staff Handbook
- Relationship and Behaviour policy
- Safeguarding policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Relationships and Sex Education (RSE)
- GDPR policy

4. Monitoring and Review

- Technology in this area evolves and changes rapidly. St Leonard's Primary School will review this policy annually if:
 - New safeguarding guidance is issued
 - Significant technological developments occur
 - Incidents indicate the need for procedural change
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Head Teacher will be informed of online safety concerns, as appropriate.
- The Headteacher will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action plan.

4.1 Filtering, Monitoring, and Technical Safeguards

The school will:

- Use approved internet filtering systems appropriate to the age of pupils
- Monitor network activity proportionately to identify safeguarding risks
- Restrict installation of unauthorised software or applications
- Maintain secure user authentication systems
- Ensure systems are regularly updated and patched
- Ensure remote learning platforms meet safeguarding standards

Any concerns identified through monitoring systems will be reviewed promptly by designated staff.

5. Roles and Responsibilities

5.1 Governing Body

The leadership and management committee will take overall responsibility for e-safety and report to the full governing body when appropriate.

The governing body will:

- Provide oversight and challenge regarding the school's online safety arrangements
- Review policy implementation and effectiveness
- Ensure statutory safeguarding expectations relating to online safety are met
- Ensure appropriate online safety policies and procedures are in place
- Monitor the effectiveness of safeguarding arrangements
- Support leadership in allocating resources for filtering, monitoring, and staff training

5.2 Senior Leadership Team

5.2.1 The Headteacher will:

- Provide strategic leadership for online safety across the school
- Ensure online safety is fully integrated into safeguarding procedures and school policies
- Allocate appropriate resources for filtering, monitoring, staff training, and technical infrastructure
- Ensure that online safety incidents are managed effectively and escalated where necessary
- Report significant safeguarding concerns, including online risks, to governors and relevant authorities where required

5.2.2 Members of the leadership team will:

Support the consistent implementation of online safety expectations across the school

- Monitor staff compliance with acceptable use and safeguarding procedures
- Ensure online safety is reflected within curriculum planning, behaviour systems, and pastoral support
- Lead parental engagement initiatives relating to digital safety and wellbeing
- Ensure that risk assessments for trips, remote learning, and new technologies consider online safety implications
- Ensure that staff receive suitable CPD

5.3 Designated Safeguarding Lead (DSL)

The designated safeguarding lead should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming cyber-bullying

The DSL will:

- Take operational lead responsibility for safeguarding issues involving online activity
- Ensure all online safety concerns are recorded, monitored, and followed up appropriately
- Liaise with external safeguarding partners, local authorities, and the police where necessary
- Provide guidance to staff on responding to online safety incidents
- Monitor patterns of incidents to identify emerging risks and required interventions

5.4 Computing/Online Safety Lead

The **computing lead** (Mrs Lowe) is responsible for:

- Liaising with the school ICT technician (Staffs Tech)
- reporting regularly to the senior leadership team
- promoting and developing an online safety conscious community
- ensuring that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensuring that the school meets the online safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant LA e-safety policy and guidance
- ensuring that users may only access the school's network through a properly enforced password protection policy
- ensuring that the school's filtering policy is applied and updated on a regular basis
- ensuring that she keeps up to date with online safety technical information in order to effectively carry out her online safety role and to inform and update others as relevant
- ensuring that the use of the network/email is regularly monitored in order that any misuse/ attempted misuse can be reported

5.5 Teaching and support staff

To maintain a safe digital environment and promoting responsible technology use.

All staff will:

- Read, understand, and comply with the school's Online Safety Policy, Safeguarding Policy, and Acceptable Use Agreement
- Model safe, respectful, and professional online behaviour at all times
- Supervise pupils appropriately when using digital devices, the internet, or online learning platforms

- Report any online safety concern, safeguarding risk, or inappropriate content immediately in line with school safeguarding procedures
- Ensure that digital resources used in teaching are age-appropriate, lawful, and suitable for pupils
- Protect personal data by following school data protection procedures and using only authorised systems for storing or sharing pupil information
- Ensure secure password practices and prevent unauthorised access to school systems
- Reinforce online safety messages through everyday teaching and classroom discussions where appropriate

5.5.1 Teaching Staff

Teaching staff will:

- Deliver age-appropriate online safety education as part of the curriculum
- Remind pupils regularly of acceptable use expectations before digital activities
- Monitor pupil activity during online learning sessions and intervene where necessary
- Ensure pupils understand how to report anything online that makes them feel uncomfortable or unsafe
- Plan learning activities that promote responsible, respectful, and critical use of digital technologies

5.5.2 Teaching Assistants and Support Staff

Support staff will:

- Assist in supervising pupils during the use of digital technologies
- Reinforce online safety expectations when supporting individuals or groups
- Report any safeguarding or online safety concerns observed during lessons or unstructured times
- Follow school procedures when supporting pupils using assistive or specialist digital technologies

5.5.3 Administrative and Technical Support Staff

Administrative and technical staff will:

- Follow secure information-handling procedures when processing personal data
- Report any suspected misuse of school systems, data breaches, or technical safeguarding risks
- Support the implementation of filtering, monitoring, and access control procedures as directed by leadership

5.6 Pupils

Pupils play an important role in helping to keep themselves and others safe online. The school will support pupils in understanding these responsibilities in an age-appropriate way. To maintain personal safety pupils and staff at St Leonard's, will work to the SMART rules.

S – Safe

M – Meeting

A – Accepting

R – Reliable

T – Tell

Pupils are expected to:

Follow School Rules for Technology Use

- Use school devices, platforms, and the internet for learning purposes only unless given permission otherwise.
- Follow the school's Acceptable Use Agreement at all times.
- Only access websites, apps, or online services approved by staff.
- Log on using their own username and password and keep login details private.

Keep Themselves Safe Online

- Keep personal information private, including full name, address, phone number, passwords, and school details.
- Tell a trusted adult immediately if they see or receive anything online that makes them feel worried, upset, or unsafe.
- Understand that people online may not always be who they say they are.
- Avoid clicking on suspicious links, pop-ups, or downloads.

Treat Others with Respect

- Communicate kindly and respectfully when using digital tools.
- Never send, post, or share unkind, hurtful, or inappropriate messages or images.
- Not take photos, videos, or recordings of others without permission.
- Understand that online bullying is taken seriously and may result in consequences.

Use Devices Responsibly

- Follow school rules regarding mobile phones and personal devices.
- Switch off and hand in devices where required.
- Not attempt to bypass school filtering, security systems, or access restrictions.
- Take care of school equipment and report any damage or technical issues

Use Artificial Intelligence (AI) Responsibly

- Only use AI tools when directed or approved by a teacher.
- Not enter personal, private, or sensitive information into AI systems.
- Understand that AI-generated content may not always be accurate and should be checked with a teacher.
- Use AI as a support for learning, not as a substitute for their own thinking and effort.

Report Concerns

Pupils must report:

- Online bullying or unkind behaviour
- Inappropriate content
- Suspicious messages or requests
- Accidental access to unsuitable material

The school will ensure pupils know how and who to report concerns to and will support them appropriately when they do.

By following these responsibilities, pupils help create a safe, respectful, and positive online environment for everyone.

5.7 Parents / Carers

Support Safe Online Behaviour at Home

- Encourage safe, respectful, and responsible use of the internet, games, and digital devices.
- Discuss age-appropriate online risks, including sharing personal information, online friendships, and digital footprints.
- Reinforce the importance of kindness and respect in online communication.

Monitor and Guide Technology Use

- Be aware of the apps, games, and websites their child is using.
- Use appropriate parental controls and privacy settings where available.
- Establish clear expectations around screen time and device use at home.
- Supervise internet use in line with the child's age and level of independence.

Promote Open Communication

- Encourage children to speak openly about their online experiences.
- Reassure children that they can report concerns without fear of blame or punishment.
- Inform the school of any online safety concerns that may impact a pupil's wellbeing or relationships within school.

Support School Policies

- Read and support the school's Online Safety and Acceptable Use policies.
- Ensure that mobile phones or smart devices brought to school comply with school rules.
- Avoid sharing images of other pupils on social media without permission.

Responsible Use of Digital Communication

- Use school communication platforms appropriately and respectfully.
- Avoid discussing individual pupils, staff members, or school matters inappropriately on social media.

6. Teaching and Learning

Online safety education is delivered through the computing curriculum, PSHE education, assemblies, and cross-curricular activities. Teaching is age-appropriate and includes:

- Protecting personal information and privacy
- Safe passwords and account security
- Online friendships and communication risks
- Cyberbullying awareness, prevention, and reporting
- Understanding misinformation, scams, and persuasive design
- Digital footprints and long-term online reputation
- Safe gaming and social platform behaviour
- Healthy screen use, and digital wellbeing
- Understanding artificial intelligence and automated content

Pupils are regularly reminded of school acceptable use expectations.

The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- The school Internet access will be designed for pupil use including appropriate content filtering. The filter for a particular site may be temporarily removed by Staffs Tech if needed
- Pupils will be given clear objectives for Internet use and taught what is acceptable and what is not
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- As part of the school computing curriculum, all pupils are educated in different elements of staying safe online
- The school will ensure that use of Internet derived materials by staff and children complies with copyright law
- If children are directed to a website as part of home learning, this will have been checked for appropriateness by the member of staff setting the task

7. Pupil email

- Pupils may only use approved e-mail accounts on the school system
- Pupils must inform a member of staff immediately if they receive any offensive mail
- Access in school to personal e-mail accounts is not allowed
- Chain letters/spam/advertising and other emails from unknown sources should be deleted immediately without opening or forwarding

8. Social Media/Networking

- Use of social networking sites within school is not allowed and is filtered on our system
- Pupils will be advised never to give out personal details that may identify themselves, other pupils, or the school. This will also include not using personal photographs or videos
- Pupils and parents will be advised that the use of some social networking sites outside of school is not appropriate for primary aged children
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory comments

9. Use of Artificial Intelligence (AI)

St Leonard's recognises the increasing role of artificial intelligence in education and society. The school will ensure safe, ethical, and responsible use.

9.1 Pupil Use

- Pupils may only use AI tools when approved and supervised by staff.
- Pupils must not input personal, identifying, or sensitive information into AI systems.
- Pupils will be taught that AI outputs may contain errors, bias, or misleading information and must be checked carefully.

9.2 Staff Use

- Staff may use approved AI tools to support planning, administration, differentiation, and accessibility.
- Staff must check all AI-generated content for accuracy, safeguarding suitability, copyright considerations, and bias before use.
- Personal or confidential school information must not be entered into public AI systems unless authorised and secure.

9.3 Curriculum Education

The curriculum will include:

- Age-appropriate explanations of what AI is – taught in PSHE, Computing and Safer Internet Day
- Understanding AI-generated images, text, and misinformation
- Encouraging critical thinking and verification of sources

10. Mobile phones and Personal Devices

10.1 Pupils

- Pupils are discouraged from bringing mobile phones or smart devices to school unless essential
- Where permitted, devices must be switched off on arrival and handed to the class teacher who will store them securely as directed
- Phones will be signed in and out by the pupil at the beginning and end of each day, and the teacher will put them in a secure location
- Pupils must not photograph, record audio/video, or access social platforms during school hours without staff permission.
- Any misuse of devices may result in confiscation, parental contact, and behaviour sanctions in line with school policy
- Smart Watches are only to be worn and used as a watch when within the school setting

10.2 Staff

- Staff must follow professional conduct expectations when using personal devices on school premises
- Personal devices must not be used to photograph pupils or store pupil data unless specifically authorised through secure school systems
- Staff should never use personal mobile phones to contact parents

10.3 Visitors

- Visitors must not photograph or record pupils without explicit school permission.
- Visitors using school Wi-Fi must comply with acceptable use expectations.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy
- Members of staff are expected to challenge visitors if they have concerns, and will always inform the Headteacher of any breaches of our policy.

11. Educational Use of Video conferencing and Webcams

St Leonard's Primary recognises that videoconferencing and webcam technologies can enhance learning, enable remote education, and support communication with pupils, families, and external professionals. Their use must always prioritise safeguarding, privacy, and appropriate conduct.

11.1 Approved Platforms

- Only school-approved videoconferencing platforms and communication systems may be used for teaching, meetings, or pupil engagement.
- Staff must not use personal accounts or unapproved applications for educational videoconferencing with pupils.

11.2 Safeguarding and Supervision

- Live sessions involving pupils must be organised, scheduled, and supervised by authorised staff members.
- Wherever possible, sessions should take place through secure school systems that require authenticated access.
- Staff should ensure that session links are shared only with intended participants and are not publicly posted.

11.3 Appropriate Use by Pupils

- Pupils must participate in videoconferencing sessions only when directed by the school or teacher.
- Pupils should use appropriate language, behaviour, and backgrounds during live sessions.
- Recording, screenshots, or sharing of live sessions by pupils or families is not permitted unless explicitly authorised by the school.

11.4 Staff Professional Conduct

- Staff must conduct videoconferencing sessions in a professional environment, using appropriate dress, language, and surroundings.
- Cameras should be positioned to avoid displaying confidential information or inappropriate background content.
- Staff should ensure that communication with pupils occurs only through official school systems and never through personal video or messaging accounts.

11.5 Recording of Sessions

- Sessions may only be recorded where there is a clear educational purpose and approval from school leadership.
- Parents and carers must be informed where recordings are made, and recordings must be stored securely in accordance with data protection procedures.
- Access to recordings will be restricted to authorised staff and pupils as appropriate.

11.6 Privacy and Data Protection

- Personal information must not be shared during live sessions unless necessary for the educational activity.
- All recordings and associated data will be handled in accordance with the school's data protection and safeguarding policies.

11.7 Technical and Safety Measures

- Staff should use available platform controls such as waiting rooms, participant permissions, and moderated chat functions to maintain safe learning environments.
- Any safeguarding concerns arising during videoconferencing sessions must be reported immediately in line with school safeguarding procedures.

12. The School Website and Published Content

- The headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate
- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: GDPR policy, acceptable use policies, codes of conduct, social media policy.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.

- We will post appropriate information about safeguarding, including online safety, on our website for members of the community

13. E-safety beyond the school gates

We take online safety beyond the school gate very seriously, particularly when behaviour:

- Results in offsite bullying including through the use of mobile devices
- Results in repercussions for the orderly running of the school
- Poses a threat to another pupil or member of the public
- Adversely affects the reputation of the school

Online bullying, harassment, or misuse of digital technology will be treated as a serious behaviour issue. Pupils will be supported in reporting incidents safely.

The school will investigate incidents in line with behaviour and safeguarding procedures and involve parents where appropriate.

Serious incidents may be referred to external agencies where required.

In all of these circumstances the headteacher will consider whether it is appropriate to notify the police. If the behaviour is criminal or poses a serious threat to a member of the public, the police will always be informed.

14. Reporting Incidents

Where an e-safety incident occurs, whether in or out of school, it must be reported and recorded. Appropriate action must be taken, and where necessary the designated safeguarding lead informed. Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Responding to Online Safety Incidents:

- All incidents must be reported immediately to a member of staff
- Safeguarding-related incidents will be referred to the DSL without delay
- Incidents will be recorded, investigated, and managed proportionately
- Where necessary, parents, external safeguarding partners, or the police may be involved