Online Safety Policy

Last reviewed	**January 2026**
Reviewed by	**Catherine Phillips and Ellie Lovatt**
Approved by	**Governing Body**
Date of approval	**Fbruary 2026**

St. Leonard's Primary School

Online Safety Policy

E-Safety involves pupils, staff, governors, visitors and parents making best use of technology, information, training and this policy to create and maintain a safe online and computing environment for St. Leonard's Primary School.

1. Policy Statement

The policy applies to all members of the school community who have access to or use school computing systems.

The Online Safety Co-Ordinator: Ellie Lovatt

This policy will be reviewed annually.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE)
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring.

The safeguarding governor will support the oversight of online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

Headteacher and Senior leaders – including DSLs:

The Headteacher is responsible for overall online safety and safeguarding within the school.

- The Headteacher is responsible for ensuring the safety (including online-safety) of members of the school community, though the day-to-day responsibility for online-safety will be delegated to the Computing Subject Leader.
- The Headteacher / Senior Leaders are responsible for ensuring that the Computing Subject Leader and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher and Deputy Head should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders will receive regular monitoring reports of online-safety breaches via the school's monitoring software.

The Computing Subject Leader:

1. Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school Online-Safety policy / documents along with the Headteacher.
2. Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

3. Provides support for staff.
4. Liaises with the Local Authority/relevant body and other professionals as required.
5. Liaises with school computing technical staff.
6. Reviews the curriculum under the direction of the Headteacher / Senior Leaders following any trends in computing related concerns.

ICT Technician(s):

The Technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements and any Local Authority/other relevant body Online Policy/Guidance that may apply.
- That the users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep up to date with online-safety technical information in order to effectively carry out their online-safety role and to inform and update others as relevant.
- That monitoring software is implemented and updated.

School staff and Volunteers:

Teaching and support staff (including volunteers) are responsible for ensuring that:

- They follow the Online-Safety Policy and Acceptable Use Agreement (Appendix) and report concerns via agreed safeguarding systems.
- They have an up to date awareness of e-safety matters and of the current school online-safety policy and practices.
- They have read, understand and signed the Staff Acceptable Use Policy (Appendix)
- They report any suspected misuse or problem to the Headteacher / Computing Subject Leader for investigation/action/sanction.
- All digital communications with pupils/parents or carers should be on a professional level and only carried out using official school systems.
- E-safety issues are embedded in all aspects of the curriculum.
- Pupils understand and follow the online-safety and acceptable use policies.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do this.

Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parent engagement, newsletters, letters, and website information about national/local e-safety campaigns/literature. Parents/Carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

4. E-safety tool – filtering and monitoring

On the school network we have installed 'Securus'. This system detects potentially inappropriate content and conduct as soon as it appears on the screen – this may be typed, received or viewed by the user. A screen capture is taken of each incident detailing the time and date of the capture, username and reason for the capture. DSLs can review captures and are alerted to captures meeting an agreed threshold. Content is reviewed and investigated where there is cause for concern. This is recorded using the school's safeguarding procedures.

5. Teaching and Learning

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 expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what is acceptable and what is not with reference being made to the Pupil Acceptable Use Agreement (Appendix)
- 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 Computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe on line. These units include topics from how to use a search engine, our digital footprint and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning.

Through the Computing curriculum we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

6. Acceptable Use of Technology

By explicitly authorising use of the school's Internet access pupils, staff, governors and parents are provided with information relating to Online-Safety and agree to its use:

- The school will maintain records of anyone who is not permitted to access the internet and reasons for access not being permitted.
- All staff must read and sign the 'Acceptable Use Agreement' (Appendix) before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access as part of the curriculum.
- Only authorised equipment, software and Internet access can be used within the school. See table below:

	Staff, Volunteers and Adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with permission	Not allowed
Mobile phones	X					X		
Use of mobile phones in lesson				X				X
Use of mobile phones in free time		X						X
Taking photos on mobile phones		X						X
Use of other mobile devices		X					X	
Use of personal accounts on school networks				X				X
Social media (own)				X				X
Social media (school)	X							X
Online shopping		X						X
File sharing	X					X		
Messaging/chat		X						X
Entertainment streaming		X						X
Video broadcasting		X						X

7. Managing Online Content

The Internet opens up new opportunities and is an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident according to the school's safeguarding procedures.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

8. Email and Digital Communication

E-mail is a quick and easy method of communication, ensuring beneficial and appropriate usage is an important part of Online-Safety:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils and staff must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully before sending, in the same way as a letter written on school headed paper.
- Phishing, spam, advertising and all other emails from unknown sources will be deleted without opening or forwarding.
- Any digital communication between staff and pupils or parents / carers (email, social media, chat, blogs, etc) must be professional in tone and content.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will review ICT use to

establish if the Online-Safety policy is adequate and that the implementation of the Online-Safety policy is appropriate.

10. Social Media

Social networking sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites and newsgroups in the school, is not allowed and will be blocked/filtered.
- The school has a Facebook account. It is managed via a central email address and used for sharing of information. The school uses Class Dojo to communicate with parents/carers. Permission must be granted by the school for new users to access Class Dojo.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends, and family over the Internet and deny access to others.
- Parents and pupils 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.
- Staff must follow the expectations laid down in the school's Staff Code of Conduct.

11. Mobile Devices

Mobile phones have access to the Internet and picture and video messaging. Whilst these are the more advanced features, they present opportunities for unrestricted access to the Internet and sharing of images. There are risks of mobile bullying, or inappropriate contact.

- Pupils in Year 5 and 6, by permission of the Headteacher, can bring mobile phones onto the school site where it is seen by the school and parents as a safety/precautionary use. These are handed into school staff upon arrival and collected at the end of the day.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or areas where children are present. All staff, visitors and volunteers should store mobile phones and devices securely, only bringing them out at times when children are not present e.g. when working in classrooms at the end of teh school day.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Please see our Mobile Phone Policy for more information.

12. Images and Video

- Pupils will not use photo or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will be done in accordance with the permissions granted by staff and parents for use of images. These consents are kept centrally by the school office and distributed accordingly.
- During school events and performances, parents will only use digital cameras, mobile phones or video equipment at school in accordance with the conditions set out by school staff. At times, the conditions may be that use is not permitted.
- All images taken by school staff and on school devices are stored securely.

13. Published content including the school website

The school website and use of Class Dojo are valuable sources of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number. Parents are encouraged to contact the central office@ email address rather than making contact directly with staff via email or Class Dojo.
- Staff and pupils' personal information will not be published.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully, and in accordance with permissions given, and will not enable individual pupils to be clearly identified.
- Parents may upload pictures of their own child only onto social networking sites outside of school. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.

14. Responding to Incidents and Misuse

Serious incidents will be managed in line with safeguarding and behaviour policies.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Please see our Whistleblowing Policy for more information.

Appendix:

Acceptable Use Agreement

Staff, Governors, Volunteers, Visitors

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a

violent, criminal or pornographic nature (or create, share, link to or send such material)

- Use them in any way that could harm the school's reputation

- Access social networking sites or chat rooms

- Use any improper language when communicating online, including in emails or other messaging services

- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network

- Share my password with others or log in to the school's network using someone else's details

- Take photographs of pupils without checking with teachers first

- Share confidential information about the school, its pupils or staff, or other members of the community

- Access, modify or share data I'm not authorised to access, modify or share

- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT lead know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Name: _____ Signed: _____

Date: _____

Acceptable Use Agreement

Pupils – Key Stage One

To stay **SAFE online and on my devices**:	
1. I only **USE** devices or apps, sites or games if an adult I trust says I am allowed to	
2. I **ASK** for help if I'm stuck or not sure	
3. I **TELL** an adult I trust if I'm upset, worried, scared or confused	
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult	
5. I look out for my **FRIENDS** and tell someone if they need help	
6. I **KNOW** people online aren't always who they say they are	
7. Anything I do online can be shared and might stay online **FOREVER**	
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to	
9. I don't change **CLOTHES** or get undressed in front of a camera	
10. I do not share my name, address or school name when I am online	
11. I am **KIND** and polite to everyone	

Acceptable Use Agreement

Pupils – Key Stage Two

These rules can keep me and others safe & happy at school and home

7. ***I can learn safely online*** – I don't behave differently when I'm learning online, so I don't say or do things I wouldn't do in the classroom. If I get asked or told to do anything that I would find strange in school, I will tell another teacher or adult I trust. I read instructions and messages carefully.

1. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to.

2. ***I am a friend online*** – I am kind and polite. I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, including the teacher or I will even do it for them.

8. ***I am a secure online learner*** – I keep my passwords to myself. Friends don't share passwords!
9. I do not tell people my name, address, phone number or school name. I use an appropriate user name on all devices.
10. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or I have asked an adult I trust. Sometimes apps can cost money, so it is important I always check.
11. ***I ask for help if I am scared or worried*** – I will talk to an adult I trust if anything upsets me or worries me on an app, site or game. If I get a funny feeling, I talk to an adult about it.
12. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell an adult I trust. If I make a mistake, I don't try to hide it but ask for help
13. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
14. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with an adult I trust before I video chat with anybody for the first time.
15. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult or skills but very unsuitable.