



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

E-Safety Policy

Date written: **February 2026**

Reviewed : February 2027

Reviewed by: Louise Lowe

Headteacher: Kirsty Cullen

Introduction

This policy outlines the processes and guidance in place at St Leonard's CE (A) Primary School to safeguard and promote the well-being of our staff and the pupils in our care during their use of ICT and the Internet.

1. Roles and Responsibilities

Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The leadership and management committee will take overall responsibility for e-safety and report to the full governing body when appropriate. Part of their role will include regular monitoring of the filtering and monitoring log.

The **Headteacher** and **Senior Leadership Team** are responsible for ensuring the safety (including e-safety) of members of the school community on a day to day basis. They will ensure that staff receive suitable CPD and are aware of the procedure in the event of an e-safety incident. The headteacher and senior leadership team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. They are also responsible for keeping a log of e-safety incidents.

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

- liaising with the school technician;
- reporting regularly to the senior leadership team;
- promoting and developing an e-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 e-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 e-safety technical information in order to effectively carry out her e-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.

Teaching and support staff are responsible for:

- ensuring they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices;
- reading and signing the school Staff Acceptable Use Policy to show that they understand the contents;
- reporting any suspected misuse or problem to the computing coordinator/headteacher as appropriate for investigation / action / sanction
- ensuring that e-safety issues are embedded in all aspects of the curriculum and other school activities;
- ensuring that pupils understand and follow the school e-safety and Acceptable Use Policy;
- ensuring that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- monitoring ICT activity in lessons, extra-curricular and extended school activities;
- ensuring that they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices;
- guiding pupils to sites checked as suitable for their use in lessons where internet use is pre-planned. Processes should be in place for dealing with any unsuitable material that is found in internet searches.

The **designated safeguarding lead** (headteacher) 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

Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which their parents will be expected to sign before pupils are given access to school systems;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;

- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying;
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be responsible for:

- promoting and modelling safe and appropriate use of ICT at home.

2. 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 for pupil use including appropriate content filtering. The filter for a particular site may be temporarily removed by StaffsTech 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.

3. Pupil use of e-mail

- 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 e-mails from unknown sources should be deleted immediately without opening or forwarding.

Social 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.

4. Mobile phones

- Children in years 5 and 6 may bring a mobile phone to school with the permission of the headteacher where it is agreed by the school/parents that this is for safety reasons (eg for use to contact parents when walking home.) Mobile phones must be handed to the class teacher at 8:50am to be locked away and collected at the end of the school day;
- Staff should never use personal mobile phones to contact parents;
- Staff (including students and visitors) are not allowed to access their mobile phone whilst children are in the classroom (unless for a reason previously agreed by the headteacher.)

5. Recording equipment

- Pupils must have permission from a member of staff before taking any photographs or video;
- Publishing of images/video/sound will follow section 8 of this policy;
- Parents will be informed at school events that photographs/video may be taken on the basis that they are for private use;

- Governors have the right to ban photographic/recording equipment at school events if the school policy is not followed.

6. The school website and published content

- Contact details on the website will be phone number, office e-mail and school e-mail addresses of teaching staff;
- Personal information about staff/pupils will not be published;
- The headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate;
- The full names of pupils will not be used with photographs on the website;
- Consent from parents/carers will be gained before photographs are published on the school website;
- Work can only be published with the permission of parents/carers and pupils;
- Parents/carers may upload photographs of their own child only onto social networking sites. If the picture includes another child/children, it is their responsibility to gain permission from that child's parents/carers;

7. E-safety beyond the school gates

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

- a) results in offsite bullying including through the use of mobile devices
- b) results in repercussions for the orderly running of the school
- c) poses a threat to another pupil or member of the public
- d) adversely affects the reputation of the school

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.

8. 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 recorded) 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.

Pupil acceptable use of ICT/E-safety rules

ICT including the Internet, email, computers, mobile phones, digital cameras, ipads etc has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT

Please discuss these e-safety rules with your child.

- I will only use school computer equipment for learning as directed by my teacher;
- If I have a school email address, this will be the only address I use on the school computer equipment;
- I will make sure that all ICT contacts with other children and adults are responsible;
- I will not deliberately look for, save or send anything that could be unpleasant. If I find anything like this, I will tell my teacher immediately;
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe;
- I know that my use of ICT can be checked and that my parent/carer can be contacted if a member of school staff is concerned about my e-safety.

E-safety beyond the school gates

As stated in our school policy, we take e-safety beyond the school gate very seriously, particularly when behaviour:

- a) results in offsite bullying including through the use of mobile devices
- b) results in repercussions for the orderly running of the school
- c) poses a threat to another pupil or member of the public
- d) adversely affects the reputation of the school

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.

Staff acceptable use of ICT/Code of Conduct

- I will only use the school's email/Internet/network and any related technologies for professional purposes or for uses deemed 'reasonable' by the headteacher or governing body;
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities;
- I will ensure that all electronic communications with pupils, staff and parents are compatible with my professional role;
- I will only use the approved, secure email system for any school business;
- I will ensure that personal data is kept secure and is used appropriately, whether in school or off the premises;
- I will not browse, download or upload material that could be considered offensive or illegal;
- I will not send to pupils, staff or parents anything that could be considered offensive or illegal;
- Images of pupils will only be taken and used for professional purposes and will not be distributed outside the school network without consent of the parent/carer;
- I will respect copyright and intellectual property rights;
- I will support and promote the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

9. Online Home Learning Guidelines for Parents and Carers

Guidelines for All Teams Video Calls and Teams Video lessons

The parent or carer must make sure their child and other members of the household are aware the video call is happening,

Staff, children and other members of the household must wear suitable clothing

Devices used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background.

Language must be professional and appropriate, including any family members in the background.

The same expectations apply for remote teaching and conversations as normal school conduct.

Staff will only ever video call a pupil with prior agreement with parents and the head teacher. This will always be at a pre-arranged time.

Wherever possible, Video calls will be recorded and stored on Teams for 21 days so that if any issues were to arise, the video can be reviewed. Parents and children will be asked to confirm they are aware of this and give consent at the start of each session

1:1 Video Conversations:

Staff will only ever video call a pupil with prior agreement with parents.

This will be at a pre-arranged time and day.

The parent or carer must stay in the room.

Guidelines for Pupils for Home Learning