Article 13 *Every child must be free to say what they think and to seek and receive information of any kind as long as it is within the law.*
Article 16 *Every child has the right to privacy. The law should protect the child's private, family and home life.*
Article 17 *Every child has he right to reliable information from the mass media, television, radio, newspaper and other media should provide information that children can understand. Governments must help protect children from materials that could harm them.*
Article 19 *Governments must do all they can to ensure that children are protected from all forms of violence, abuse, neglect and mistreatment by their parents or anyone else who looks after them.*

St. Leonard's Primary School
E-Safety Policy

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

1. E-Safety Policy
Our E-Safety Policy has been written by the school, following government guidance. It has been agreed by senior management and approved by governors. The policy applies to all members of the St. Leonard's community (including staff, pupils, volunteers, parents/carers, visitors and governors) who have access to and are users of the school computing systems.

The school's E-Safety Co-ordinator is: Miss L Rack

The E-Safety Governor is: Mrs L Howell

The E-Safety Policy and its implementation shall be reviewed annually.

Roles and Responsibilities
The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

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 reports. The role of the E-Safety Governor will include:

- Regular meetings with the E-Safety Co-ordinator.
- Regular monitoring of e-safety incident logs.
- Regular monitoring of filtering/control logs.
- Reporting to relevant Governors committee.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator 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 will receive regular monitoring reports from the E-Safety Co-ordinator.

The E-Safety Co-ordinator:

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety policy / documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff
- Liaises with the Local Authority/relevant body.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering/control logs.
- Attends relevant committee meeting of Governors.
-

Technician:

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 E-Safety 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 e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- That monitoring software are implemented and updated.

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understand and signed the Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Headteacher / E-Safety Co-ordinator 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 e-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 workshops, 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.

2. E-safety Tool - Policy Central Enterprise (PCE)

On the school network of computers we have installed the PCE tool. Policy Central Enterprise detects potentially inappropriate content and conduct as soon as it appears on the screen, is typed in by the user or received by the user. A screen capture is taken of every incident detailing the time and date of capture, machine name, username and reason for capture. A weekly headline summary is produced from the system detailing captures of particular interest to alert the person monitoring the system, (Head teacher and E-safety Co-ordinator). These particular violations will be investigated and dealt with in accordance to the Acceptable Use Policy (AUP), behaviour policy and other relevant school policies.

3. 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 AUP on a regular basis.
- 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 new 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 Computing 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. We also measure and assess the impact regularly through meetings with our SEN Co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

4. Authorised Internet Access

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

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access and asked to sign and return a consent form for pupil access.
- Only authorised equipment, software and Internet access can be used within the school.

5. World Wide Web

The Internet opens up new opportunities and is becoming 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 in an E-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The E-Safety Log will be reviewed termly.
- 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.

6. E-mail and Communications

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

- Pupils may only use approved e-mail accounts on the school system.
- Pupils 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.
- Whole class or group e-mail addresses should be used in school rather than individual addresses.
- Access in school to external personal e-mail accounts is not allowed.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Chain letters, 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.

The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff and Adults				**Pupils**			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be bought to school	**X**				**X**			
Use of mobile phones in lesson				**X**				**X**
Use of mobile phones in social time		**X**						**X**
Taking photos on mobile phones				**X**				**X**
Use of other mobile devices e.g. tablets, gaming devices		**X**						**X**
Use of personal email addresses				**X**				**X**

in school or on school network								
Use of school email for personal emails				**X**				**X**
Use of social media				**X**				**X**

7. Social Networking

Social networking Internet sites (such as, MySpace, Facebook) 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 twitter account which is suspended at present. It is the intention of the school governors to reactivate the account when there are enough safeguards in place as this is an excellent means to communicate with parents.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- 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 guidelines laid down in the school's full social media policy.

8. Video Conferencing

Video conferencing will not be used without further consideration.

9. Mobile Phones

Many new 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 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 the school office at 8:45 and collected at the end of the day.
- The sending of abusive or inappropriate text messages is forbidden.
- All digital communications with pupils/parents or carers should be on a professional level and only carried out using official school systems.
- Staff including students and visitors are not permitted to access or use their mobile phones within the classroom. All staff, visitors and volunteers within the Foundation Stage place their phones in a locked cabinet in Nursery and Reception for the duration of hours worked by each member of staff. The remainder of staff ensure that their phones are turned off and stored safely away during the teaching day.
- Staff may use their mobile phones in the staffroom during the lunch period.
- Parents cannot use mobile phones on school trips to take pictures of the children.

10. Digital/Video Cameras

Pictures, videos and sound are not directly connected to the Internet but images are easily transferred to the schools network.

- Pupils will not use digital cameras or video equipment at school unless specifically authorised by staff.
- Publishing of images, video and sound will follow the policy set out in this document under 'Publishing Content'.
- Parents will not use digital cameras, mobile phones or video equipment at school unless specifically authorised by staff.
- The Headteacher or nominee will inform parent(s)/guardian(s) and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner
- All images are stored on the secure school network.
- Digital images are disposed of in accordance with the Data Protection Act.
- Digital images will not be stored on portable devices.

11. Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

12. Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- 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 will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school Web site.
- Work can only be published with the permission of the pupil and parents.
- Parents may upload pictures of their own child only onto social networking sites. If the picture includes another child / children then it is their responsibility to gain permission from that child's parents.
- The Governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

13. Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-Safety will be discussed with our ICT support and those arrangements incorporated in to our agreement with them.

14. Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

15. 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 audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

16. Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

17. Actions and Sanctions

Any actions that are deemed as inappropriate in the school setting will be referred to the Headteacher. The necessary child protection steps will be followed if it is deemed a child protection matter. For all other incidents of misuse of the school ICT systems the schools behaviour sanctions will be referred to and parents/carers contacted if necessary. Below is a guide to the possible actions and sanctions for both staff and pupils. These are a guide, as each individual case will be considered so appropriate action in relation to the incident is given.

Pupil Incidents	**Actions / Sanctions**							
	Refer to class teacher	Refer to Headteacher	Refer to police	Refer to technical support staff for action	Inform parents/ Carers	Removal of network/ Internet access rights	Warning	Further sanction e.g. isolation/ exclusion
Deliberately accessing or trying to access material that could be considered illegal		**X**	**X**		**X**			
Unauthorised use on non-educational sites during lessons	**X**						**X**	
Unauthorised/ Inappropriate use of mobile phone digital camera/other mobile device		**X**			**X**			
Unauthorised/ Inappropriate use of social media/ messaging apps/personal email		**X**			**X**			
Allowing others to accessing the school network, using another pupil's account		**X**					**X**	
Attempting to access or accessing the school network, using another pupils account		**X**					**X**	
Attempting to access or accessing the school network, using the account of a member of staff		**X**					**X**	
Corrupting or destroying the data of other users		**X**				**X**		
Continued infringements of the above, following previous warnings or sanctions		**X**			**X**	**X**		**X**
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		**X**						**X**
Using proxy sites or other means to subvert the school's filtering system		**X**				**X**		**X**
Accidently accessing offensive or pornographic material and failing to report the incident		**X**			**X**			

Deliberately accessing or trying to access offensive or pornographic material		X	X		X			

Staff Incidents	**Actions / Sanctions**						
	Refer to Headteacher	Refer to LA/HR	Refer to Police	Refer to Technical support	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal	X	X	X		X	X	X
Inappropriate personal use of the internet/social media/personal email	X				X		X
Unauthorised downloading or uploading files	X			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X						
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X		
Deliberate actions to breach data protection or network security rules	X				X		
Corrupting or destroying the data of others or causing deliberate damage to hardware or software	X				X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X	X	
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students/pupils	X	X	X				X
Actions which could compromise the staff member's professional standing	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X			X	X	X
Using proxy sites or other means to subvert the school's filtering system	X			X			

Accidently accessing offensive pornographic material and failing to report the incident	X	X		X	X		

18. Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that all ICT use is monitored and recorded.
- Pupils will be informed when they are in Y3 of the importance of being safe on social networking sites. This will be strongly reinforced across all year groups during ICT lessons and all year groups look at different areas of safety through the digital literacy lessons.

Staff:

- All staff will be given the School E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic (including emails) can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents:

- Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website. They will receive annual updates on E-Safety at our Meet the Teacher sessions during the summer term. Training for parents has been delivered by an LA advisor and parents have been provided with an e –safety related website links.

19. Further Resources

We have found these web sites useful for E-Safety advice and information.

www.st-leonards-stafford.staffs.sch.uk
Our school's web site for this and other policies and school information

http://www.staffsscb.org.uk/
Staffordshire Safeguarding Children Board's site with locally provide information on all aspects of protecting children.

http://www.thinkuknow.co.uk/
Set up by the Police with lots of information for parents and staff including a place to report abuse.

http://www.childnet-int.org/
Non-profit organisation working with others to "help make the Internet a great and safe place for children