St Luke's C of E Primary School
Policy for E-Safety

Policy: Internet & E-safety
SLT
Reviewed: Autumn 2015
For review: Autumn 2018

1.1 Definition

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum, Data Protection and Security.

1.2 Introduction

The resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature, will provide access to information, which has sometimes not been selected by the teacher. Whilst pupils will often be directed to sites which provide reviewed and evaluated sources, at times they will be able to move beyond these to sites unfamiliar to the teacher.

There is therefore the possibility that a pupil may access unsuitable material either accidentally or deliberately.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the Internet.
- Describe how these fit into the wider context of our behaviour.
- Demonstrate the methods used to protect the children from sites containing unsuitable material.

The school believes that the benefits to pupils from access to the resources of the Internet far exceed the disadvantages. Ultimately the responsibility for setting and conveying the standards that children are expected to follow, when using media and information resources, is one the school shares with parents.

At St Luke's, success lies in a combination of site-filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

1.3 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those listed in section 1.1.

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by the senior leadership team.
- The e-Safety Policy and its implementation will be reviewed every 3 years.

2.1 Teaching and Learning

2.1.1 Why Internet use is important

- We use the internet for a number of reasons:
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- The Internet is a part of everyday life for education, business and social interaction.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own personal safety and security whilst online.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

2.1.2 The benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Local Authority and DfE;
- access to learning wherever and whenever convenient.

2.1.3 Internet use will enhance learning

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

2.1.4 Pupils will be taught how to evaluate Internet content

- Because the quality of information received via radio, newspaper and telephone is variable and information received via the Internet, email or text message requires even better information handling and digital literacy skills.
- In particular it may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. Pupils should be made aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject.

2.2 Managing Information Systems

2.2.1 Information system security

- School IT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted.
- Portable media may not used without specific permission.

2.2.2 E-mail

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- The forwarding of chain messages is not permitted.

2.2.3 Published content and the school website

- We use the website to celebrate pupils work, promote the school and publish resources for projects.
- The contact details on the website should be the school address, email and telephone number. Personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate and editorial guidance will help reflect the school's requirements for accuracy and good presentation.
- The website will comply with current guidelines for publications including respect for intellectual property rights and copyright.

2.2.4 Publishing pupil's images and work

- Still and moving images and sounds add liveliness and interest to a website, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount.
- Photographs that include pupils will be selected carefully to ensure only those pupils with permission are published.
- Each class is issued with a school digital camera, video camera and laptop. Images of pupils will not be stored on staff's personal cameras, phones or hardware. Only school equipment must be used and images downloaded onto the school network.
- The permission form must be completed by parents or carers before photographs of pupils are published on the school website.
- Pupils' full names will not be used anywhere on the website in association with a photograph.

2.2.5 Social networking and social media

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be taught never to give out personal details of any kind which may identify them or their location unless a teacher has given permission.
- Pupils and parents will be advised that the use of social network spaces outside school could be inappropriate for primary aged pupils.

- Pupils will have the opportunity to learn about social networking and personal publishing (blogs) within the closed environment of the school's IT systems.
- No member of staff should use social networking sites or personal publishing sites to communicate with students.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Staff cannot under any circumstances mention any negative or inappropriate references to their working lives on any social media.

2.2.6 Managing filtering

- The school has a secure filtering system in place, which ensures that children are safe from unsuitable material when accessing the internet in school, for example terrorist and extremist materials.
- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Co-ordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.2.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call. Videoconferencing should be supervised by a member of staff.

2.2.8 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.
- Mobile phones will not be used in school unless part of an organised curriculum lesson. The sending of abusive or inappropriate text messages is forbidden.

2.2.9 Protecting personal data

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

2.3 Policy Decisions

2.3.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

- Parents will be asked to sign and return a consent form.

2.3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Kingston LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- School computers will be monitored using a desktop monitoring system (Securus) and evidence collated if misuse is suspected.

2.3.3 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. If the complaint is about the Head of School this should be reported to the Chair of Governors.
- Complaints of a child protection nature must 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 Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

2.3.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.3.5 How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents of cyberbullying reported to the school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of bullying.
- Sanctions for those involved in Cyberbullying will follow the school's behaviour and anti-bullying policies.

2.4 Communications Policy

2.4.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

2.4.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

2.4.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- Parents' safety awareness meetings will be run on a regular basis to inform parents of e-safety outside of the school.
- All parents and carers will receive written information advice on e-safety measures.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	BBC National Archives Natural History Museum Imperial War Museum London Grid for Learning
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. ▪ Ask ▪ CBBC Search ▪ Kidsclick ▪ Everyclick (raises money for school)
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.	LGfL
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School Website Platform Learning London Grid for Learning
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. Photographs of pupils should not be stored on staff's personal cameras or computers The school reserves the right to stop photographs being taken on school premises due to child protection issues or if permission is withheld by parents of pupils.	School Website Platform Learning
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	Platform Learning
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum Imperial War Museum

Attachments

- Policy for use of digital and video images
- Policy for acceptable use by staff
- Policy for managing equipment
- Parent's e-safety agreement form
- 12 rules for responsible ICT use
- Pupil's E-safety agreement form
- Policy for handling infringements
- Parent's Fact Sheet