ST. LUKE'S CHURCH OF ENGLAND PRIMARY SCHOOL

Church Lane
Lowton **☎ 01942 201140**
Warrington **Fax 01942 205048**
WA3 2PW **web www.saintlukes.wigan.sch.uk**
Headteacher: Mr S Hardaker e-mail enquiries@admin.saintlukes.wigan.sch.uk

E-Safety Policy

Date of Policy: 2024
Review date: Annually

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 previous Internet Policy has been revised and renamed as the Schools' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children.

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

End to End e-Safety
E-Safety depends on effective practice at a number of levels:
Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
Safe and secure broadband from BT.
National Education Network standards and specifications
Monitoring of network activity through the use of Senso Capture MDN software.

Further Information

E-safety Materials and links: http://www.thinkuknow.co.uk
http://www.ceop.gov.uk
http://www.childnet-int.org/kia/

1.1 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 for ICT, Acceptable Use, bullying and for child protection.

- The school has appointed an E-Safety leader (Computing Leader) who is a senior member of staff.
- Our E-Safety Policy has been written by the school, building on government guidance. It has been agreed by senior leadership and approved by governors.
- The E-Safety Policy and its implementation will be reviewed annually.

1.2 Teaching and learning

1.2.1 Why Internet use is important

- Internet use is part of the statutory curriculum and is 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 safety and security.
- 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.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

1.2.2 How will E-Safety be taught?

- E-Safety skills, appropriate to each year group, have been embedded primarily (but not exclusively) into the schools Computing curriculum. Staff plan for and teach the skills within their year group across the curriculum.
- The school uses the 'Digital Literacy' resources to aid the teaching of E-Safety lessons.

1.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

1.3 Managing Internet Access

1.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- All users will have their own designated username and password which will be kept secure by themselves (Reception children will use a single 'Reception' user account)
- Users will not leave themselves logged on at unattended workstations.
- Virus protection will be updated regularly.
- Security strategies will be reviewed in line with best practice regularly.

1.3.2 E-mail

- The school uses Microsoft Exchange on its own server to provide its own e-mail system which is the only permitted e-mail system to be used by all users of the curriculum network.
- 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.
- E-mail sent to an external organisation should be written carefully in the same way as a letter written on school headed paper.
- The forwarding of chain letters/spam e-mails is not permitted.

1.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and where a name is used, only the Christian name will be included.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents.

1.3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites. (Twitter is allowed under the direct supervision of the class teacher where a class twitter account is used to support educational activities)
- 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.
- Pupils will be taught and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

1.3.6 Managing filtering

- The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- The school has the facility to manage its own filtering. Users may request filtered sites to be allowed through the school filter. Requests are to be made to the Computing Leader and approved by the Headteacher (or Deputy Headteacher in their absence) before the site is added to the allowed list.
- It has been agreed that 'Youtube' will be allowed through the filter to be used by teachers to enhance teaching and learning. Pupil access to 'Youtube' will be restricted via the domain controller on the curriculum server.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Coordinator and/or Computing Leader.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- The children will be restricted from using 'Google' within school. Children will use 'Kidrex' as a child friendly search engine.

1.3.7 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.
- Calls should only be made or answered in the presence of a supervising adult.
- Videoconferencing will be appropriately supervised for the pupils' age.

1.3.8 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.
- Pupils are not allowed to have mobile phones in school except for Year 6 pupils. Year 6 pupils are permitted to bring mobile phones to school. Year 6 pupils are responsible for placing their phones in the designated box on arrival at school. Mobile phones are kept in a secure place during the school day. Mobile phones must NOT be kept in pupils school bags. Mobile phones are returned to Year 6 pupils at the end of the school day.

- Staff disable their mobile phones during the school day. They are able to check their mobile at both break and lunchtime. Mobile phones are only to be used in the following areas: staffroom, offices and outside the main entrance. Staff are not to use phones in the classroom.

- **Protecting personal data**
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

1.4 Policy Decisions

1.4.1 Authorising Internet access

- All staff must read and sign the 'IT Acceptablu Usage Policy' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

1.4.2 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 Wigan LA can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit computing provision to establish if the E-safety policy is adequate and that its implementation is effective.

1.4.3 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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- An E-Safety flowchart to respond to incidents is followed by all staff and all 'Computing Incident Violations Reports' iare recorded by Benchmark and reported to school.

1.4.4 Community use of the Internet

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

2.1 Communications Policy

2.1.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be informed that e-mail accounts provided by the school may be monitored and accessed by the administrator.

2.1.2 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.
- Staff will be informed that e-mail accounts provided by the school may be monitored and accessed by the administrator.

2.1.3 Enlisting parents' support

- Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school Web site.

- From time to time Parents and Carers will be invited into school for E-safety awareness sessions to help ensure parents are aware of the most current risks and issues.