LEIGH ST PETER'S CE PRIMARY SCHOOL

Together with God we challenge minds, recognise talents and build dreams

E-SAFETY POLICY

Date of Policy: December 2016

Review Date: Annually

Member of staff responsible: Mr K Robinson

WRITING AND REVIEWING THE E-SAFETY POLICY

- The school's e-Safety Coordinator is Mr K Robinson, who is a member of the Senior Leadership Team.
- Our e-Safety policy has been written by the school, building on the Wigan Safeguarding Children Board (WSCB) e-Safety strategy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety policy and its implementation will be reviewed annually.

1.0 TEACHING AND LEARNING

1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.

1.2 Internet use will enhance and extend learning

- Staff will be made aware of and pupils will be educated in the safe use of the Internet.
- Clear boundaries will be set and discussed with staff and pupils, for the appropriate use of the Internet and digital communications.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3 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.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.0 MANAGING INTERNET ACCESS

2.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

- All pupil users on the system have a designated username and password. ***(Reception children will use a single 'Reception' user account)***
- Security strategies will be discussed with Wigan LA and the IT service provider.

2.2 E-mail

- Pupils and staff should only use approved e-mail accounts on the school system. This is currently Office 365.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils must immediately tell a teacher if they receive offensive or inappropriate e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school website

- 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.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Parents will complete a consent form stating what can and cannot be published in relation to their child. These details will be consulted before any work or photographs are published in any context.
- 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 website.
- Pupil's work can only be published with the permission of the pupil and parents.
- Staff will not keep images of children on personal devices eg. memory sticks, mobile phones or use the images for any other use than in school.
- Staff will not keep images of children on staff iPads which leave school premises.
- Staff must ensure that all equipment in school containing images of children, e.g. school lap tops, iPads and digital cameras, are locked away securely at the end of the school day and must not be taken out of school.

2.5 Social networking and personal publishing

- The school will educate people in the safe use of social networking sites and educate pupils on their safe use.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must be made aware of how they can report abuse and who they should report abuse to.
- Pupils should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.

- Pupils should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

2.6 Managing filtering

- The school will work with Wigan Council 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 Coordinator or Headteacher who will report the site to Abtec and to the (Local Authority).
- Senior Leaders will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable (using Securus).

2.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils will not independently make or answer 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.

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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Pupils are not allowed to have mobile phones in school except for pupils in Key Stage Two. Key Stage Two pupils are permitted to bring mobile phones to school and are responsible for placing their phones in the designated box on arrival at school. Mobile phones must **NOT** be kept in pupils' school bags. Mobile phones will be returned to pupils at the end of the school day. Mobile phones must **NOT** be used at school or on school premises.

2.9 Protecting personal data

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

3.0 POLICY DECISIONS

3.1 Authorising Internet access

- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource, including any laptop issued for professional use.
- 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 directly supervised access to specific, approved on-line materials.
- At Key Stages 1 and 2, access to the internet will be supervised at all times and children will be told which internet site(s) they are allowed to access. Staff will check screens to ensure that the pupils are on the correct website both at the start and during the session.
- Parents will be asked to sign and return a consent form (a copy of which is attached as appendix 3 & 4.)

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 Wigan 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.
- The school will ensure monitoring software and appropriate procedures are in place to highlight when action needs to be taken by the school.

3.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior leader in school.
- Any complaint about staff misuse must be referred to the headteacher. Any misuse that suggests a member of staff is unsuitable to work with children should be reported to the LADO in accordance with Wigan Safeguarding Board policies.
- If the misuse is by the headteacher it must be referred to the chair of governors in line with Wigan Safeguarding Board Child Protection procedures.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils, parents and staff will be informed of the complaints procedure.

3.4 Community use of Internet

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

4.0 COMMUNICATING E-SAFETY

4.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all classrooms where laptops and other electronic devices are used and they will be discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of e-safety training and awareness raising will be put in place in line with the Wigan Safeguarding Children's Board e-safety strategy.

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.
- Staff will be informed that e-mail accounts provided by the school may be monitored and accessed by the administrator/member of the Senior Leadership Team.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff should understand that phone or on-line communications with pupils can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Equipment from school which is used at home, must not be used by other members of your family or friends.
- Email communication cannot be used on personal devices.
- Electronic devices provided by the school cannot be synced with personal equipment from home.

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 Web site.
- From time to time parents and carers may be invited into school for e-Safety awareness sessions to help ensure parents are aware of the most current risks and issues.
- If school is informed of any potential risks for pupils relating to e-Safety, for example any safeguarding issues relating to the use of social networking sites at home, school will ensure parents and carers receive advice and information.
- Parents and carers will be reminded that they must not publish any images or video footage on social network sites before and after each event.

Other useful e-safety materials and links:
http://www.thinkuknow.co.uk
http://www.ceop.gov.uk
http://www.childnet-int.org/kia/

Approved by the Governing Body at their meeting held on:
21st December 2016

Signed:……**(Headteacher)**
Date:……

Signed:……**(Chair of Governors)**
Date:……