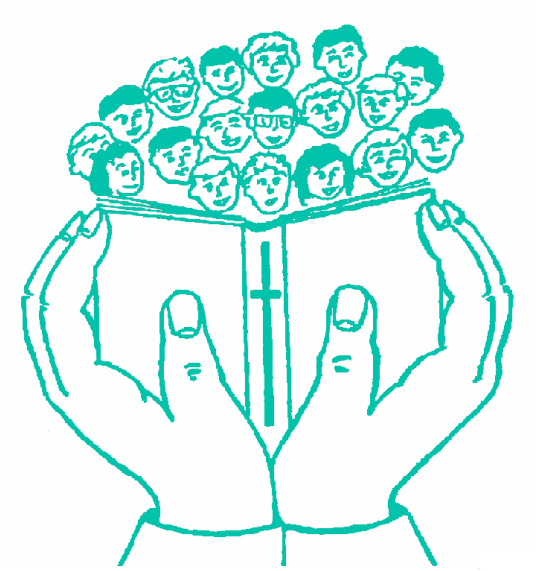
St Luke's Halsall CE Primary School



E-Safety Policy

“Inspiring lives, building futures together with Jesus.”

At St. Luke’s Halsall we recognize that everyone is made in the image of God and that we are privileged to be part of the lives of the children we educate and nurture.

We also recognize that a strong partnership between pupils, staff, parents and governors will enable us to realize our mission statement, “Inspiring lives, building futures together with Jesus”, striving to ensure that our values and decisions are made based on the values Jesus taught us.

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones, tablets and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.
The school’s e-safety policy will operate in conjunction with other policies including those for Pupil Behaviour, Anti-Bullying, Child Protection, Teaching & Learning, Tackling Extremism and Radicalisation.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 the provider including the effective management of content filtering.

Dangers to consider

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual’s consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the child.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils’ resilience to the risks to which they may be exposed, so that they have the necessary confidence and skills to deal with these risks. The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.
The e-safety policy that follows explains how we intend to do this.

E-Safety Audit –
This quick self-audit will help the senior management team (SMT) assess whether the e-safety basics are in place.

Has the school an e-Safety Policy that complies with LSCB guidance? Date of latest update: October 2015 The Policy was agreed by governors on:	
The Policy is available on the school website for parents.	Yes
The Policy is available for staff in policy folder	Yes
The e-Safety Coordinator is:	Richard Miller
Has e-safety training been provided for both pupils and staff?	Yes
Do all staff sign an ICT Code of Conduct on appointment?	Yes
Do parents sign and return an agreement that their child will comply with the School e-Safety Rules?	Yes
Have school e-Safety Rules been set for pupils?	Yes
Are these Rules displayed in all rooms with computers?	Yes
Internet access is provided by an approved educational Internet service provider and complies with DFE requirements for safe and secure access.	Yes
Has the school filtering policy been approved by the SMT with Sefton?	Yes
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Yes

The school will monitor the impact of the policy using:
• Logs of reported incidents
• broadband monitoring logs of internet activity (including sites visited)
• Internal monitoring data for network activity
• Surveys / questionnaires of pupils, parents / carers, staff

School e-Safety Policy

The school will appoint an e-Safety coordinator. This is currently the Computing Subject leader, Mr Richard Miller.
Our e-Safety Policy has been written by the school, building on the Sefton guidance. It has been agreed by the senior management team and approved by governors.
The e-Safety Policy will be reviewed annually. This policy will next be reviewed Oct 2016

Why is Internet Use Important?
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 information and administration systems.
Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.
Many pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?
Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- 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 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 the Local Authority and DCSF; access to learning wherever and whenever convenient

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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
- Internet access will be planned to enrich and extend learning activities
- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised 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.
- Parents will be asked to sign and return the 'Acceptable ICT Use Agreement' which will also be signed by pupils each year

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported tothe e-safety coordinator or network manager who will investigate and take appropriate action,liaising with broadband provider if necessary
- School will ensure that the use of Internet derived materials by pupils and staff complies withcopyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how tovalidate information before accepting its accuracy.

Social Networking

- Schools should block/filter access to social networking sites and newsgroups 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 should be advised not to place personal photos on any social network space

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others
- Pupils and parents should be made aware that some social networks are not appropriate for children of primary school age

Filtering

The school will work in partnership with the internet Service Provider 'Schools Broadband' to ensure filtering systems are as effective as possible.

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 for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden
- Staff will be issued with a school phone where contact with pupils is required

Published Content and the School Web Site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content isaccurate and appropriate

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified on the website
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs
- Written permission from parents or carers 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

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 our technical support team and broadband provider if necessary

Protecting Personal Data

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

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 cannot 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

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff – Headteacher or Deputy Headteacher
- 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
- Pupils and parents will be informed of the complaints procedure
- Discussions will be held with the LADO to establish procedures for handling potentially illegal issues

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms
- Pupils will be informed that Internet use will be monitored

Staff

- 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.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Website

Policy Reviewed: Oct 23rd 2015

Adopted by Governing Body:

Review date: Oct 2016

Appendix A

The following letter will be sent to new pupils and their parents.

Acceptable ICT Use Agreement: pupils and parents

Rules for Responsible Computer and Internet Use

In school we have access to the internet. This is a powerful tool which opens up new opportunities for everyone and promotes effective learning. We at St Luke's Halsall CE Primary School are aware that children should have an entitlement to safe internet access at all times. However, the school and parents have a duty of care to protect children and ensure that internet use is responsible and safe.

The school strongly recommends that children do not use social network sites such as Facebook and Bebo at home, as these sites carry an age-restriction and pose a risk to children. Social networks have no place in our school and so school staff should not be approached online or invited to join.

Please read and sign the 'Rules for Responsible Computer and Internet Use' with your child to show your support of the school in this important aspect of our work.

- I will only access the system with my own login
- I will not access other people's files
- I will ask permission from a member of staff before using the internet and I will only access sites approved by a trusted adult
- I will only email or message people I know or a trusted adult has approved
- The messages I send will be polite and responsible
- I will not give my home address or telephone number in any message
- I will report any unpleasant material, anything that upsets me or anything that seems 'wrong'. Iwill tell a trusted adult if I am contacted by a stranger or receive unpleasant messages. Iunderstand that this would help protect other pupils and myself and that the school would needto take appropriate action.I understand that the school may check my computer files and may monitor my use of the internet

Sanctions

- Deliberate minor incidents in school will lead to a warning
- Serious incidents (or repeated minor incidents) will mean access to the ICT equipment or the internet is removed
- Illegal behaviour by anyone will be dealt with by the police

Parent/Guardian Name _____

Signed _____

Pupil Name _____

Signed (child) _____

Date _____

Appendix B

E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use
- It is a criminal offence to use a computer or network for a purpose not permitted by the school
- Irresponsible use may result in the loss of network or Internet access
- Network access must be made via the user's authorised account and password, which must not be given to any other person
- All network and Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers
- Anonymous messages and chain letters are not permitted
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging
- The school ICT systems may not be used for private purposes, unless the Headteacher has given specific permission
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix C

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Parent's Consent for Web Publication of Work and Photographs
I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access
I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but that the school cannot be held responsible for the content of materials accessed through the Internet.

Signed:

Date:

Please print name:
Please complete, sign and return to the school

Appendix D

Unsuitable / inappropriate activities

The school believes that activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or out of school when using school equipment or systems. The school policy restricts certain internet usage as follows:

User Actions

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **child sexual abuse images promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation**
- **adult material that potentially breaches the Obscene Publications Act in the UK**
- **criminally racist material in UK**
- **pornography**
- **promotion of any kind of discrimination**
- **promotion of racial or religious hatred**
- **threatening behaviour, including promotion of physical violence or mental harm**
- **any other information which maybe offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute**
- **Using school systems to run a private business**
- **Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school**
- **Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions**
- **Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)**
- **Creating or propagating computer viruses or other harmful files**
- **Carrying out sustained or instantaneous high volume network traffic (downloading /uploading files) that causes network congestion and hinders others in their use of the internet**
- **On-line gaming (educational)**
- **On-line gaming (non educational)**
- **On-line gambling**
- **On-line shopping / commerce**
- **File sharing**
- **Use of social networking sites**
- **Use of video broadcasting eg Youtube**

Appendix E

Acceptable Use Agreement: staff

To ensure that all staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

Monitoring

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.
Sefton Local Authority will monitor and audit Internet use to see if users are complying with the policy. Any potential misuse identified by Sefton will be reported to the school.
N.B. Access to any site that might be deemed 'inappropriate' but has an educational use should be recorded in your planning.

Incidents which appear to involve deliberate access to web sites, newsgroups and online groups that contain the following material will be reported to the police:

- images of children, apparently under 16 years old, involved in sexual activity or posed to be sexually provocative,
- material that breaches the Obscene Publications Act in the UK
- criminally racist material.

If inappropriate material is accessed accidentally, users should immediately report this to the Headteacher

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- I understand that comments made in networking sites such as Facebook, twitter or similar sites should make no direct or indirect reference to our school, should not include images of school or children involved in school activities. Parents of children in our school will not be approached or contacted through social networks, and any requests to become online 'friends' with parents will be refused.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……..

Print Name: ……

Date: ……..

Accepted for school: Signed: ……

Print name: ……