E-Safety & Acceptable Use Policy

Long Sutton Church of England Primary School

<table>
<tr><th>Date of Last Review</th><th>Date of Next Review</th></tr>
<tr><td>September 2021</td><td>September 2022</td></tr>
<tr><th colspan="2">Responsibility for Review and Monitoring / Auditing</th></tr>
<tr><td colspan="2">Headteacher in partnership with staff & Foundation Governors</td></tr>
<tr><th colspan="2">Purpose</th></tr>
<tr><td colspan="2">To outline how we ensure the safety of staff, Governors and children in their use of the internet and IT equipment</td></tr>
</table>

Long Sutton Church of England Primary School
E- Safety and Acceptable Use Policy

The welfare of the students at our school is of paramount importance. We recognise that pupils today are growing up in an increasingly complex world. IT and new technologies offer many opportunities but that there are also challenges and risks. This policy shows how we address these key issues.

E – safety encompasses new technologies, internet and electronic communications such as mobile phones, collaboration tools (e. g. Wikis) and personal publishing (e.g. podcasts).

The school is aware that an increasing number of adults and children use social media sites such as TikTok, Twitter, Snapchat and Intagram.

E- safety at Long Sutton CE Primary is coordinated by both the Computing leader and the head teacher, who is also the Designated Safeguarding Leader. Our E- Safety Policy has been agreed by the governors and staff of the school and can be accessed on the school's website. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why internet use is important

We believe that the internet and other digital technologies are powerful resources, which when utilised effectively, can transform and enhance both teaching and learning. The internet is an essential element within 21st century life for education, business and social interaction. The school provides pupils with the opportunities to use the excellent resources on the internet, alongside developing the skills necessary to access, analyse and evaluate them in a safe, considered and respectful way. The reliance on the internet during periods of remote teaching and learning has shown why it is an ongoing priority.

Internet use and safety is a part of the statutory curriculum and is an integral part of the whole school ethos of being kind, respectful and being the best you can be.

Internet use will enhance learning

The schools internet access will be designed expressly for pupil use and will use filtering appropriate to the age of pupils (provided by HCC).

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum and embed this within a wider whole school approach. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- Pupils will be taught how to evaluate internet content
- Pupils will be taught how to recognise techniques for persuasion
- Pupils should be helped to understand the need for a Pupil Acceptable Use agreement and encouraged to adopt safe and responsible use of the internet both inside and outside of school. This links to our school values of love, courage and hope.
- Pupils will be taught to be critically aware of the materials that they read and shown how to validate information before accepting the accuracy.
- Pupils will be helped to understand safe ways in which to seek support if they see something online that makes them feel upset or uncomfortable.
- The school will ensure that all staff and children are aware that the use of internet derived materials should comply with copyright law.

See appendix 1 for specific details on the acceptable use of ICT at Long Sutton CE Primary.

Managing Internet Access

Information system security

The school will be responsible for ensuring that the school network is as safe and secure as is possible and that the policies and procedures approved within this policy are implemented.

The school ICT systems capacity and security will be regularly reviewed.

Virus protection will be updated regularly. The school uses the HPSN2.1 web filtering services, as recommend by Hampshire County Council.

Security strategies will be discussed with the network manager, who works for Rocket Computer Services.

Personal security of staff and pupils with their documents will come through the use of personal log ins and passwords for staff as well as individual accounts for pupils with a set password.

Published content and the school website

The contact details available on the school website are the school address, email address and telephone number. Staff, governors' or pupils' personal information will not be published.

The headteacher will take overall editorial responsibility for the website and ensure that content published is accurate and appropriate. The class teachers will be responsible for the content published onto their class pages.

Publishing pupils' images and work.

Pupils' full names will not be used anywhere on the school website, particularly with association to photographs.

Photographs that include pupils will be selected carefully. Permission forms are completed by all parents when children begin the school before photographs of pupils are published on the school website. Permission lists are kept in the school office and staffroom. Class teachers are to ensure that they are checking this when adding photographs to the school website and class pages.

Social networking and personal publishing

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority group liable to the injured party.

The school ensures that personal information is not published.

Staff should ensure that;

- No reference should be made in social media regarding pupils, parents and carers and other material against the school.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinion should not be attributed to the school or local authority.
- Security settings are regularly checked to minimise risk of loss of personal information

Hampshire County Council blocks/filters access to social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents will be advised that there are a variety of social network spaces outside school. While some are designed for children of primary age, other have age restrictions and therefore are deemed inappropriate.

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy

- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken. Where deemed appropriate any concerns/actions may be entered on CPOMS in order to monitor.

Managing filtering

The school will work with both the network manager and Internet service provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover an unsuitable website, this is to be reported immediately to either the headteacher or the network manager.

The Computing Lead and Admin Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable across all devices capable of accessing the Internet.

Managing mobile technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

The use of mobile technologies within school is carefully managed and falls within the acceptable use agreement for details of use within the school setting.

Use of video conferencing tools for online teaching (eg Teams or Zoom) will only be used in group/class work and links for access will always be sent through parent email accounts.

The use of mobile phones by pupils is not permitted on the school premises.

Contact with children should be via the school phone only.

The use of digital and visual images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. This message will be reinforced through staff training, the computing and PSHE curriculum.

YouTube and Google Images

Videos on the file-sharing website YouTube can be used to effectively support many areas of the curriculum. When these videos are used safely and appropriately, they can be an extremely beneficial resource for Class Teachers and Support Staff.

In the same way google images provides a plethora of curriculum enhancing opportunities to make teachers resources more relevant, accessible and powerful.

However, there are potential risks when working with YouTube, Vimeo and Google Images that staff should be aware of. For example, despite a filter/flagging policy being in use on YouTube, inappropriate images, unsuitable written comments, or bad language can still all be accidentally revealed to the children. In order to prevent this from happening, the following precautions should be taken:

Finding suitable videos and images.

- Searches, or first observations of a potential video and images, should not be carried out with any child in the class room.
- Before showing a video or image to the class, the video should be watched and listened to carefully by the Class Teacher or LSA, who should look out for inappropriate content material along with any inappropriate comments that appear underneath the video.
- It is the class teacher's responsibility to make the final approval of a video or image used.

Playing the video for the children

- Using the remote control, the whiteboard should be frozen, stilled or muted (depending on the option available on your remote) prior to Full Screen mode being selected for the video. (This is so that no comments or any other videos can be seen by the children).When the video is ready, the whiteboard can be unfrozen and the video watched.

• Before the end of the video, pause it so 'recommended' videos that might potentially contain inappropriate language, are not revealed.
• When the video is finished, the whiteboard should once again be frozen, stilled or muted (or even turned off) so that the video can be exited and the YouTube window closed safely.

Educating the children about safe use of these sites.
Children will have these sites explicitly demonstrated as part of their yearly E-safety teaching. Pupils will be made aware of best practices if they come across unsuitable content online including; turning off the screen, telling an adult and protocol for reporting inappropriate material to websites with the help of a website. Under no circumstances will children be using image or video sharing websites unsupervised.

Security, Data and Confidentiality

When accessing, amending and saving any data or information relating to the school or pupils, school staff follow the guidelines set out in the General Data Protection Regulations 2018.

Authorising internet access

All pupils and parents are made aware of the 'Online safety Acceptable Use Agreement' (See appendix 2) before using any school ICT resources.

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 or device. Neither the school nor HCC can accept liability for the material accessed, or any consequences of internet access.

The monitoring and decision making of the teachers will determine which websites are accessed when using the internet within lessons.

The school will audit ICT provision to establish whether the e-safety policy is adequate and that its implementation is effective, particularly in light of new developments with technology.

Handling e-safety complaints

Complaints of pupil internet misuse will be dealt with by the appropriate member of staff. This may be the class teacher, Senior Leadership Team including the head teacher. An E-safety incident form should be completed and a copy given to the DSL. Guidance on this is given through the NSPCC flow chart (Appendix 3 & 4).

Any complaint about staff misuse must be referred to the head teacher.

Complaints of a bullying nature must be dealt with in accordance with the school anti bullying policy.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (See the Child Protection Policy)

Dealing with Online Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff or governor involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation.

Once this has been completed and fully investigated senior leadership and the Computer Lead will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures.
- Involvement by Local Authority.
- Police involvement and/or action.

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of ‘grooming’ behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for
The school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes.

Introducing the E-Safety Policy to pupils

E-safety rules will be posted in all networked rooms (See appendix 5) and discussed with the pupils at the start of each year. Pupils will be informed that network and internet use will be monitored. The pupils will also discuss the Online Safety Rules within their PSHE lessons to further understand these and bring these more into the forefront. The Google Scheme: 'Be Internet Legends' will form part of the internet safety curriculum at KS2 and will include lessons to develop their understanding of social media.

School recognises that some children have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. The school has a list of vulnerable children and all staff will be responsible for being aware of their additional needs.

Staff and the E-Safety Policy

All staff will be given the opportunity to read the E Safety Policy.

Staff will have appropriate training on Online Safety as part of their annual safeguarding training.

All staff can use the school network, which includes internet and email access. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents support

Parents' attention will be drawn to the E-Safety Policy in newsletters and on the school website.

The school will promote e-safety with links on the school website to support and helplines, and regular updates via school newsletters.

Parent's will be asked to read through the 'Acceptable use of the internet and computers' policy with their child and sign accordingly.

Appendix 1

Acceptable Use of ICT at Long Sutton CE Primary

School Responsibilities

The school has a responsibility to provide all children with safe and secure access to a wide range of IT resources and forms of media, including those available online. Children have a clear minimum entitlement to use IT as part of the National Curriculum and this will be taught alongside a comprehensive internet safety curriculum.

The school has a responsibility to ensure that children have access to a wide range of media to accommodate the digital age we live in and will be given opportunities across the curriculum to use different technologies, including iPads.

Misuse

We take misuse of any form of media (*text, digital image of any type, video and or audio file*) by any member of the school community seriously and will deal with any incidents that occur as if they had occurred on school property during the school day. We take the view that all users do so under the direct code of conduct set out below.

- It is an offence under the school code of conduct for any member of the school community to publish any derogatory remark in any form of media.
- It is an offence under the school code of conduct for any member of the school community to extract any form of media for use in cyber bullying.
- It is an offence under the school code of conduct for any member of the school community to produce, publish or store any sexist, racist, sexually exploitive, radicalisation and propaganda material in any form of media.
- It is an offence under the school code of conduct for any member of the school community to knowingly store or seek to spread a virus.

Dealing with misuse

- We will deal with any incidents of cyber bullying as if the bullying had taken place within the physical bounds of the school.
- We will investigate and work with all parties in any incidents of cyber bullying that take place between members of the school community, where clear evidence is provided. The school takes the position that as these persons would have never met without the school as contact point then the school has a duty to help. Following best practice, where cyber bullying

threatens violence or is of a sexual nature, the police will be asked for their advice/involvement.

- Offences will be dealt with according to the level of the offence in line with school discipline for pupils and guidelines for staff disciplinary procedures. If the offence is a breach of criminal law, the police will be called in and all evidence will be presented to be the best of the schools ability.
- Minor infringements of these rules by pupils will be dealt with by the head teacher.

Homework

Teachers may provide homework that requires the children to have access to a computer and/or the internet. Pupils who don't have access to a computer or internet at home should be sensitively offered the choice of a worksheet or the opportunity to complete their homework using a school computer at break and lunchtime, and at homework club. If a pupil expressed a desire to use the school network then this arrangement can be assumed to be continual.

Password Security

Each individual is responsible for their own login. Children have individual logins but a generic password, this is for ease of access. Children should still be taught about keeping personal information safe and not share their login details with anyone.

Children should be taught to log off and shut down to ensure that access to other pupils accounts can't be accessed.

Communication

E-Mail

- At school pupils may only use approved messaging accounts. (class g-mail accounts)
- Pupils must immediately tell a teacher if they receive an offensive message.
- Pupils must not reveal personal details about themselves or others in online communication, or arrange to meet anyone without specific permission.

Appendix 2

Online Safety Acceptable Use Agreement

These online safety rules help to protect students and the school by describing acceptable and unacceptable computer use.

Think then Click!

- ✓ I understand that I must have permission from an adult before using the internet.
- ✓ I agree to only use wesbites that an adult has chosen.
- ✓ I will tell an adult if I see anything that I am uncomfortable with.
- ✓ I know that I must immediately close any web page that I am not sure about or if I see something I do not like
- ✓ I will only send e-mails to people an adult has approved.
- ✓ I will only send e-mails and messages that are polite and friendly.
- ✓ I know that I must never give out personal information or passwords.
- ✓ I agree never to arrange to meet anyone that I do not know.
- ✓ I understand that I should not open emails sent by people that I do not know.
- ✓ I know that we do not use internet chat rooms in school
- ✓ I know that I should use the internet to access appropriate material
- ✓ I understand that my teacher and/or parents will be involved if I do not follow these rules.

The school may exercise its right to monitor the use of the schools computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the schools 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.

Online Safety Rules

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

Pupil: ***Class:***

Pupil's Agreement:

- ✓ I have read and I understand the school e-Safety Rules.
- ✓ I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- ✓ I know that network and Internet access may be monitored.

Signed: ***Date:***

Parent's Consent:

I have read and understood the school e-safety rules. I understand that the school will take all reasonable precautions to ensure that pupils are safe and protected whilst using computer facilities, including the internet.

Signed: ***Date:***

Please print name:

Appendix 3

NSPCC – Sample E-Safety Incident Report Form

Appendix 4

NSPCC – 'What to Do' Flow Chart

Appendix 5

Online Safety Rules

Key Stage 1

Think then Click!

These rules help us to stay safe on the Internet:

- We only use the internet when an adult is with us.

- We can click on the buttons or links when we know what they do.

- We can search the Internet with an adult.

- We always ask if we get lost on the Internet.

- We can send and open emails together.

- We can write polite and friendly emails to people that we know.

Key Stage 2

Think then Click!

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.