Langshott Primary School

Online Safety Policy

March 2017

Written by: Sally Lane	
Date of policy revision	**March 2017**
Review date	**March 2019**
Date of Governor Approval	**March 2017**

Langshott Primary School online safety policy

Online safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding, anti-bullying, mobile phone, acceptable use and the use of images.**

Using This Policy

- This policy must be read in accordance to the Child Protection Policy.
- The school will form an Online Safety Committee and will appoint an Online Safety Co-ordinator.
- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy was revised by: Sally Lane.
- It was approved by the Governors on: March 2017
- The Online Safety Policy and its implementation will be reviewed annually. The next review is due on: March 2018.
- The Online Safety Policy covers the use of all technology which can access the school network and the internet, or which facilitates electronic communication from school to beyond the bounds of the school site. This includes, but is not limited to; workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.
- **This policy has been written in accordance with the Keeping Children Safe in Education (KCSIE) 2016 guidelines.**

Managing Access and Security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering, provided by a recognised filtering system, which is regularly checked to ensure that it is working, effective and reasonable, **as referenced in Keeping Children Safe in Education (KCSIE 2016)**.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by **personal** passwords for both staff and pupils. (Staff and Key Stage Two children have their own personal login and passwords).
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform Online Safety Policy. The school uses Netsupport system to monitor online usage **as referenced in Keeping Children Safe in Education (KCSIE 2016)**.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use
The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.

All communication between staff and pupils or families will take place using school equipment and/or school accounts.

Pupils will be advised not to give out personal details or information which may identify them or their location.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published Content (eg: school web site, school social media accounts)

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher, or nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreycc.gov.uk/?a=168635

Parents Taking Photographs

- In the light of emerging, mobile technology and the ease of uploading photographs onto social media sites, it has been agreed that parents may take photographs at class assemblies and similar school events. However, parents will be asked to use photographs for personal use only and not to upload onto social media sites. A message will be given out at every class assembly or similar event.

Social Networking and Personal Publishing on the School Learning Platform

- The school does not allow children to access social networking sites, as they are blacklisted by our cachepilot.
- 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 not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Parents will be reminded at all school events that they are welcome to take images for their personal use as part of a community of trust. If these images are placed on social networking sites, the school will review this agreement.

- No member of staff /student will linked on-line with pupils.
- No inappropriate photographs, status updates or conversations will be uploaded.
- Staff/ students will not comment on school related issues, nor engage in school related conversations.

Use of Personal Devices

- Personal equipment may be used by staff and/or pupils to access the school IT systems, provided their use complies with the Online Safety Policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.
- Staff and students working in school will ensure that mobile phones are switched off, or turned to silent mode, during lessons, (ensuring phones do not ring/vibrate). Staff and students should never use mobile phones for making/receiving calls and sending/receiving text messages and emails when children are present. Staff and students need to use their professional judgement to determine if it is appropriate to make/receive calls and send/receive messages at lunchtime and after school, taking into consideration their location in school and the presence of children. Staff and students have been asked not to walk through school talking on mobile phones and to keep mobiles out of sight of children (for example, not left on desks in the classroom).
- Continued vigilance in school is important; everyone is responsible for the safe guarding of children and must ensure mobile phones are used in-line with this policy. **(*Everyone is accountable; if you see someone using a mobile phone, which breeches the policy this needs to be challenged*).**
- If the agreed codes above are broken, action will be taken in-line with the school's disciplinary policy. The same applies to trainee teachers and students as well as being reported to their university and/or college/school.

Protecting Personal Data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- All staff, (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors), must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- **At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.**
- **At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy. Key Stage 2 children will have individual logins and passwords.**
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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

Handling online safety complaints

- Complaints of internet misuse will be dealt according to the school Behaviour Policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behavior policy.

Sexting (Youth Produced Sexual Imagery)

- Langshott Primary School views "sexting" as a safeguarding issue and all concerns will be reported to and dealt with by the Designated Safeguarding Lead.
- The school will not view the image unless there is a clear need or reason to do so.
- The school will not send, share or save indecent images of children and will not allow or request children to do so.
- If an indecent image has been taken or shared on the school/settings network or devices then the school will take action to block access to all users and isolate the image.
- The school will need to involve or consult the police if images are considered to be illegal.
- The school will take action regarding indecent images, regardless of the use of school/setting equipment or personal equipment, both on and off the premises.
- The school will follow the guidance as set out in "'**Sexting' in schools: advice and support around self-generated images. What to do and how to handle it**".

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP, so it is expected that their use will be in accordance with the school Online Safety Policy.

Communication of the Policy

To pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their online safety education.
- Online safety rules will be posted in all classrooms.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by 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.
- Pupils will be taught how to report unpleasant Internet content to the class teacher or their parent if they are at home.
- Pupils to be taught to use the Hector the Protector safety button and seek adult help to report unpleasant Internet content.
- Pupils to be taught how to be a responsible online citizen.
- Pupils to be taught appropriate behavior on social media apps and how to report unpleasant / inappropriate behavior on apps.

To staff

- All staff will be shown where to access the Online Safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training on an annual basis.

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the school Online Safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be offered online safety training regularly.
- Parents helping on Educational/school trips must not use their mobile phone during the course of the day for making and receiving phone calls, sending messages and emails, accessing social media sites or taking photographs. It is the responsibility of the teaching staff leading the trip to ensure that parents are aware of this policy and the information is communicated to parent helpers both verbally, during the briefing.

Appendix 1

School Rules for EYFS /

KS1 Internet Use

Rules for using the Internet safely

I will :

- ☑ only visit websites suitable for children my age;
- ☑ be polite and show respect when communicating with others;
- ☑ keep my personal information secret (including passwords);
- ☑ report any unpleasant messages/inappropriate websites to a member of staff.

School Rules for KS2 Internet Use

STOP and THINK before you CLICK

- Be polite. (no bad or abusive language or other inappropriate behaviour)
- Keep personal information private
- Do not post or share detailed accounts of your personal life. (contact information, daily routines, location, photographs and videos)
- Do not post pictures or videos of others without their permission.
- If you see any inappropriate materials, tell your teacher immediately.
- If you see any abuse including cyberbullying, tell your teacher immediately.
- Do not click on any pop-ups. (buying on-line; on-line gaming / gambling etc.)
- Do not open attachments unless you are sure the source is safe
- Tell your teacher immediately if you see something which makes you feel uncomfortable.
- Do not respond to malicious or threatening messages (but do not to delete them. keep them as evidence of bullying)
- Do not arrange to meet anyone without having discussed it with an adult and taking a responsible adult with you.