LEEHURST SWAN

E-Safety Policy

Last reviewed by the Headmaster and the E-Safety Co-ordinator in March 2017

This policy is published on the school website for parents

Applies to the whole school including EYFS

Introduction

Students are growing up in the digital generation, where the internet provides them with a world of opportunities to learn, communicate and express themselves. The internet presents students with tremendous opportunities for learning and personal development. Digital technology and online content are changing all the time. Students use computers at school, have internet-enabled mobile phones, and on-line game consoles, smart TV's, tablets and laptops at home. As such this policy document seeks to protect pupils and staff from adverse effects of e-communication specifically in regard to:

- receiving inappropriate content
- predation and grooming
- requests for personal information
- cyberbullying – see Child Protection policy
- identity theft
- corruption or misuse of data
- publishing inappropriate content
- online gambling
- Sexting – sex texting and images
- misuse of computer systems
- Pornography
- Terrorist activity
- Extremism
- publishing personal information
- hacking and security breaches

Leehurst Swan takes Child Protection and e-Safety and Prevent Duty seriously:

- the appointed e-Safety Co-ordinator is responsible for dealing with any e-Safety issues that arise, in conjunction with the Designated Safeguarding Lead and Pastoral Co-ordinators
- the e-Safety Co-ordinator manages e-Safety training and keeps abreast of local & national e-Safety awareness campaigns
- the school works in partnership with ICT contractors to ensure filtering systems are as effective as possible
- the school recognises the Prevent Duty of care placed upon it by DfE.
- complaints of internet misuse by pupils are dealt with by the e-Safety Co-ordinator
- concern about staff misuse must be referred to the Headmaster
- The school helps parents plan supervised use of the Internet at home and alerts them to potential dangers.
- rules for Internet access are displayed in networked rooms
- pupils are informed that Internet use is monitored
- virus protection for the whole network is installed and maintained
- servers must be located securely and physical access restricted
- portable media must not used without specific permission and a virus check
- The IT network manager reviews system security regularly.

All Users

All users should adhere to the following rules.

- Be polite.
- Use appropriate language.
- Do not reveal addresses, phone numbers or personal details.
- Do not use the network in such a way that would disrupt the use of the network by other users.
- Do not open e-mail links, unless sure of the content and do not add contacts to lists unless sure of them.
- E-mail is not guaranteed to be private.
- Do not upload photographs or videos of anyone connected to the school.

School Staff e-Safety
It is a condition of employment that all staff follow the policies and procedures relating to use of the computer network and e-safety policy. The school can monitor network and Internet use, to help ensure it is being used legitimately with regard to the e-Safety policy.
Teaching staff should take responsibility for regularly checking that effective filtering and monitoring is appropriate for their lessons.
Because of the dangers of contacting pupils via social network sites, (facebook, myspace etc), private e-mail and text messaging; staff should not use these means of communication with pupils, in or out of school, or allow pupils to access their wall. Staff should be guarded about other means of communication including use of their official school email address and allowing pupils to contact them in an informal way.
Staff must follow the policy on 'The use of e-mail to contact parents and pupils'.
Staff are also reminded of the requirement to maintain confidential and professional about school matters and school matters must not be discussed in open forums or social networking sites.

Pupil e-Safety
Parents are informed that pupils will be provided with supervised Internet access and parents and pupils sign an acceptable use agreement.
Pupils should understand that the use of the school's network is a privilege which could be removed should misuse arise.
Mobile 'phones
Phone's that are able to access the internet must have "parental controls" enabled if brought into school.
Pupils are allowed to use mobile phones at school, but not during lessons, study times, assemblies, corridors or other public gathering times. The School is not responsible for the safety of the phone and it should be kept securely when not in use. Staff ensure that mobile phone use is monitored and enforced especially in areas used by the EYFS pupils.

Allowing a 'phone to disrupt a school activity will result in confiscation for a period of time, determined by the Deputy Head. Pupils are not allowed to record sounds or images during school time without the explicit permission from the teacher in charge of the activity or on duty. Taking selfies in school is also forbidden. Sending or forwarding explicit images, materials or messages by pupils is an offence and is prohibited. The misuse of mobile phones in sexting, accessing pornography, gambling sites and sites excluded by the school filters, is strictly forbidden and any pupil receiving such information is urged to report it to the E-safety Co-ordinator or the Deputy Head. See mobile phone policy.

Prevent duty
The school recognises the responsibility to prevent pupils being drawn into terrorism and radicalised groups especially those contactable through the internet and social media websites. Social media sites are blocked in school and filters are in action to prevent harmful information and images being accessed by the school computer networks.

E-mail
- Pupils must 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 adult permission.
- The forwarding of chain letters is not permitted.

Social Networking Sites
Pupils are not allowed to access social networking sites from school. However, pupils should be taught the safe use of these sites in e-safety education.
Internet Use
Pupils bringing their own laptops or net books into school must have Parental Controls enabled on them. They are not allowed to access the school net work without specific written permission from the Headmaster or the Head of E-safety or the ICT Coordinator or the Head of Learning support.
Some pupils may, inadvertently or deliberately, access unsuitable sites with violent, pornographic, harmful images or information even on school computers. In view of the risks, Prep pupils should be supervised at all times when using the internet. Staff should check, before allowing pupils to use Internet wide search engines such as Google, that filtering is working. The school uses Rocket lightspeed as a filtering system. However, NO filtering-based search engine is completely safe.

Response to Misuse of a Computer or Access of Inappropriate Material:
All staff should take immediate action.
The activity of pupils and staff on the ICT system is monitored by the Esafety manager and the external consultant on a weekly basis. Breaches of use, and attempted breaches, show up in the data log and are reported to the safety co-ordinator and or the Headmaster.
They are also reported as safeguarding incidents to the deputy Head (Designated Safeguard Lead) and the Governor responsibly for safeguarding will be informed.
Close or minimize the window immediately. Do not shut down the computer. Remove the pupil from the computer and report the incident to the e-Safety Co-ordinator, the ICT Co-ordinator or the Headmaster. Leave the investigation to someone else. If pupils saw the page, talk to them about what has happened, and reassure them. Later, technical staff will investigate the history of visited sites to get details to find how the pupil got there. In the event of extremist material or terrorist websites, staff are remind of the requirement under the Prevent Duty, to report all suspicions to the lead safeguard person (Mrs North) and the police.

E-Safety Education

- Every school pupil should receive, annually, an e-safety course appropriate to their age. This will normally be in their ICT lessons.
- Discussion about safety should be an important part of planning tasks or before pupils use the internet.
- Staff should ensure that the use of internet derived material complies with copyright law, pupils should be made aware of plagiarism and issues relating to work research being undertaken for coursework.
- Pupils will be trained to become critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Increasingly concern is expressed about the use and storage of images generated in school and this policy extends to:

Taking, using and storing images of children
Parents are invited to agree to the school using anonymous photographs of their child which may be published in the prospectus or on the web site, as well as displayed within the premises. Parents indicate their consent on the form for this purpose. Photographs are taken extensively of

pupils in the foundation stage to provide evidence of their achievements. These photographic records will only be shown to the parents and staff.
Cameras or other recording devices must never be used whilst changing a child or in the games changing rooms. To avoid allegations such devices must be switched off before entering the room or left outside the room. In Pre Prep all staff must secure mobile phones in the staff room before the session. Only school owned equipment may be used during the session. See EYFS Personal care policy.

Use of images: displays etc
We will only use images of our pupils for the following purposes:

- Internal displays (including clips of moving images) on digital and conventional notice boards within the school premises,
- Communications with the school community (parents, pupils, staff, Governors and alumni) via password-protected sections of the school's web site,
- Marketing the school both digitally by web site, by prospectus, which includes a DVD, by displays at educational fairs and other marketing functions and by other means.
- Informing parents of the activities of their own child, for example in Interactive Learning Journeys.

Use of images: internal identification
All pupils are photographed annually for the purposes of internal identification and to provide a facility for parents
These passport-sized photographs identify the pupil by:

- Name
- Year Group and form/tutor group

They are securely stored in the password-protected area of the staff database, where access is restricted to academic, pastoral and school office staff. Staff are not permitted to use images for any other purposes than the above. Staff are not permitted to share images with parents other than the specific parents of the child. Parents are supplied by the photographer with a copy of the photograph.

Images that we use in displays and on our web site
The images that we use for displays and communications purposes never identify an individual pupil. Instead, they name the event, the term and year that the photograph was taken (for example, "First XV rugby team, Lent Term 2009"). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc in their proper context. We never use any image that might embarrass or humiliate a pupil. Pupils are always properly supervised when professional photographers visit the school. Parents are given the opportunity to purchase copies of these photographs where possible.

Storage and review
Our images are stored securely either in locked filing cabinets, or in a password protected section of the school's database. Records of children' achievements in learning journeys are shared only with the appropriate adults and are held securely between viewings.

Media coverage
We will make every effort to ensure that children whose parents or guardians have refused permission for images of their children to be used are excluded from any event in which the media are present or prevent them from being photographed.

We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the children of celebrities.

Use of cameras and recording equipment by parents and guardians.

Parents are welcome to take photographs of their own children taking part in sporting and outdoor events. Mobile phones, cameras and other recording devices are not permitted to be used at any time within the Pre Prep setting. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.

Parents must not take photographs of other pupils, without the prior agreement of that child's parents. Such photographs containing images of other children must not be displayed on social network sites or published in any format without the explicit written consent of the parents. Any images taken in school cannot be sold or used for commercial gain without the explicit written permission of the headmaster.

Data Storage and Data protection:

All staff should be aware of the requirement to preserve confidential information held by the school in electronic format concerning: staff, parents and pupils. Information such as names, contact details and academic information, including reports, should be stored securely.

Encryption is the most secure form of storage and must be used for any pupil details or identifiable information (birth dates etc) stored in electronic form on computers, data sticks, CDs, hard drives or similar.

Reports (including those in Word format) mark books and other similar information, must be stored in a password protected, secure form, on any of the above devices but need not be encrypted. If in doubt, staff are advised to password protect every document.

The above applies both to information stored in school (other than on the main server) and especially, to any information that may be taken home. Should a data storage device be mislaid or stolen, it is vital that the confidential information cannot be accessed. Staff are advised also to hold only the information which is absolutely essential, away from the main school server. Staff are also required to report immediately any loss of a data storage device which contains pupil details. Staff are also reminded they must not share information or photographs with individuals other than the designated parent and accredited third parties including examination boards.

Protection and Monitoring Web-use

Web filtering software 'Rocket' by Lightspeed Systems is currently being used to monitor and filter sites when web browsers Google Chrome and Internet Explorer are being used.

Administration rights have been given to the Head of ICT to block unsuitable sites and to release sites deemed educational.

Annex A: Notes on the legal framework of e-safety

Prevent Duty of care: June 2015 DfE

Sexual Offences Act 2003

- Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

- Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image.)

- Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

- Abuse of positions of trust - Staff must be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, connexions staff)

The Computer Misuse Act 1990
makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data.
.
Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Communications Act 2003 - There are 2 separate offences under this act:
a. sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
b. sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

Malicious Communications Act 1988 – it is an offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.

Copyright, Design and Patents Act 1988 - it is an offence to use unlicensed Software

Protection from Harassment Act 1997
Section 2 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Inspecting e-safety in schools (120196) Ofsted, 2014

The safe use of new technologies (090231), Ofsted, 2010; www.ofsted.gov.uk/resources/090231

Other publications
Safer children in a digital world: the report of the Byron Review (PP/D16(7578)/03/08), DCSF and DCMS, 2008; http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

Ofcom's response to the Byron Review, Ofcom, 2008; http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/byron/

Safeguarding children and young people, July 2014,

From:	The Charity Commission
First published:	14 July 2014
Part of:	Managing your charity, Staff and volunteers and Trustee role and board
Applies to:	England and Wales

https://www.gov.uk/government/publications/safeguarding-children-and-young-people

Annex B: Web site addresses related to e-safety

- www.getsafeonline.org
- http://www.bbc.co.uk/schools/parents/cyber_bullying/
- http://www.bbc.co.uk/newsbeat/17874040
- http://www.thinkuknow.co.uk/11_16/
- http://www.thinkuknow.co.uk/parents/ (practical ideas to keep safe)
- https://www.thinkuknow.co.uk/teachers/resources/?tabID=3
- http://www.childline.org.uk/explore/onlinesafety/pages/onlinesafety.aspx
- http://www.childline.org.uk/explore/bullying/pages/cyberbullying.aspx (for Children)
- https://www.childline.org.uk/Explore/OnlineSafety/Pages/staying-safe-online.aspx
- http://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/
- https://www.kidpower.org/library/article/cyber-bullying/?gclid=CKfRzsqF8sgCFYTnGwodGZECMA
- http://www.kidsmart.org.uk/
- http://www.chatdanger.com/ (for children)
- http://www.wikihow.com/Be-Cyber-Safe
- http://www.respectme.org.uk/Cyberbullying-and-the-law.html
- http://www.kidscape.org.uk/cyberbullying/cyberbullying.shtml
- http://puresight.com/Cyberbullying/dos-and-donts-for-cyber-bullying-victims.html
- http://www.stopbullying.gov/cyberbullying/what-is-it/
- http://stopcyberbullying.org/what_is_cyberbullying_exactly.html
- http://www.pawsexplore.co.uk/internet_safety.html
- http://www.ceop.gov.uk/contact_us.html
- http://ceop.police.uk/
- http://www.virtualglobaltaskforce.com/
- http://www.iwf.org.uk/
- http://www.internetsafetyzone.co.uk
- http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm
- http://www.nch.org.uk/stories/index.php?i=324
- http://www.education.gov.uk/ukccis/
- http://www.saferinternet.org.uk/
- http://www.childnet.com/
- http://www.swgfl.org.uk/
- https://cybermentors.org.uk/
- http://www.theparentzone.co.uk/
- http://www.digizen.org/
- https://www.getsafeonline.org/social-networking/social-networking-sites/
- https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

Annex to be reviewed by the E-safety Co-ordinator annually.

Annex C

E-Safety Incident Log

Organisation address			
Organisation contact details			
E-safety lead			
E-safety lead contact details			
Details of incident			
Time		Date	
Where did the incident occur			
Name and contact details of person reporting incident			
Who was involved in the incident	□ child/young person □ staff member □ other (please specify _____		
Names and contact details of those involved			
Type of incident	□ bullying or harassment □ online bullying or harassment (cyberbullying) □ sexting (self-taken indecent imagery) □ deliberately bypassing security or access □ hacking or virus propagation □ racist, sexist, homophobic religious hate material □ terrorist material □ other (please specify) _____		

Description of incident	
Nature of incident	□ deliberate access □ accidental access
Did the incident involve material being	□created □viewed □printed □shown to other □transmitted to others □distributed
could this incident be considered as	□ harassment □ grooming □ cyberbullying □ sexting (self-taken indecent imagery) □ breach of AUP □ other (please specify) _____
Action taken	□ staff □ incident reported to head teacher/senior manager □ advice sought from children's social care □ incident reported to police □ incident reported to CEOP □ incident reported to Internet Watch Foundation □ incident reported to IT □ disciplinary action to be taken □ e-safety policy to be reviewed/amended □ child/young person □ incident reported to member of staff (specify) □ incident reported to social networking site □ incident reported to IT □ child's parents informed □ child/young person debriefed □ e-safety policy to be reviewed/amended □ disciplinary action taken