Long Furlong Primary School
E-safety Policy

The following whole-school policy refers to the safe, acceptable and responsible use of the Internet.

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing.It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

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

ÅResponsible ICT use by all staff and students
ÅSound implementation of e-safety policy in both administration and curriculum.
ÅSafe and secure broadband including the effective management of a filter.
ÅNational Education Network standards and specifications.

School e-safety policy

ÅThe e-Safety Policy relates to other policies including those for ICT, bullying and safeguarding as well as the staff code of conduct.
ÅThe school has appointed a named person to co-ordinate e-Safety.
ÅOur e-Safety Policy has been approved by governors, following consultation with staff and parents.
ÅThe e-Safety Policy and its implementation will be reviewed every two years.

Teaching and learning

Why Internet use is important

ÅThe Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.
ÅInternet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
Internet use will enhance learning

The school Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.

ÅPupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
ÅPupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
ÅThe school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Last reviewed: July 2013

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

Managing Internet Access

ÅInformation system security, School ICT systems capacity and security will be reviewed regularly.
ÅVirus protection will be updated regularly.
ÅSecurity strategies will be discussed with the schoolôs technical support provider.

E-mail

ÅPupils may only use approved e-mail accounts on the school system.
ÅPupils must immediately tell a teacher if they receive offensive e-mail.
ÅPupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
ÅE-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on
school headed paper.

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 pupilsôpersonal information will not be published. The Head Teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

ÅPupilsôfull names will not be used anywhere on the school website.
ÅWritten permission from parents or carers will be obtained before photographs of pupils are published on the website.
ÅPupilsôwork can only be published with the permission of the pupil and parents.

Social networking and personal publishing

ÅThe school will block/filter access to social networking sites.
ÅNewsgroups will be blocked unless a specific use is approved.
ÅPupils will be advised never to give out personal details of any kind which may identify them or their location.
ÅPupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

ÅThe school will work with its technical support consultant and the Broadband Service Provider to ensure systems to protect pupils are reviewed and improved.
ÅIf staff or pupils discover an unsuitable site, it must be reported to the named e-Safety person and communicated to others members of staff.

ÅThe schoolôs technical support consultant will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Emerging Technologies

ÅMobile phones should not be used during formal school time ï if children require access to mobile phones before or after they are asked to hand them into the school office for safe keeping during the school day.
ÅThe sending of abusive or inappropriate text messages is forbidden.
ÅEmerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

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

ICT access

ÅAll staff will be given the School e-Safety Policy and its importance explained.
ÅAll staff must read and sign the óAcceptable ICT Use Agreementôbefore using any school ICT resource.
ÅPupilsôaccess to the Internet will be under adult supervision at all times.
ÅEveryone will be made aware that Internet traffic can be monitored and traced to the individual user
ÅRules for good online behaviour will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year.
ÅPupils will be informed that network and Internet use will be monitored.
ÅParentsôattention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
ÅThe 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
ÅComplaints of Internet misuse will be dealt with by the Head Teacher.

ÅThe designated e-Safety officer will undertake an e-Safety audit each year to assess whether the e-safety basics are in place.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-safety incident, reported to the e-safety officer and an incident sheet completed.

Social networking ï is allowed in school in accordance with the e-safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become ñfriendsòwith parents or pupils on personal social networks

Use of Email ï staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student, or IT support.

Data Protection ï If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the e-Safety Officer.

Viruses and other malware - any virus outbreaks are to be reported to the Mouchel Helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

e-Safety ï like health and safety, e-safety is the responsibility of everyone to everyone. As such you will promote positive e-safety messages in all use of ICT whether you are with other members of staff or with students.

Last reviewed: July 2013

Long Furlong Class Agreement for ICT

I Promise ï to only use the school ICT for schoolwork that I have been asked to do.

I Promise ï not to look for or show other people things that may be upsetting.

I Promise ï to show respect for the work that other people have done.

I will not ï use other peopleôs work or pictures without permission to do so.

I will not ï damage the ICT equipment, if I accidentally damage something I will tell an adult.

Keeping Safe

I will not ï share personal information online with anyone.

I will not ï download anything from the Internet unless an adult has asked me to.

I will ï let an adult know if anybody says or does anything to me that is hurtful or upsets me or if I am asked for personal information.

I will ï be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell an adult if I am ever concerned in school or my parents if I am at home.

Last reviewed: July 2013

e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Last reviewed: July 2013