LONG FURLONG PRIMARY SCHOOL
ONLINE SAFETY POLICY

Policy Statement

The Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents, regular users of the premises and its wifi (e.g. Christ Church on Long Furlong members).

Safeguarding is a serious matter. At Long Furlong School, we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety, is an area that is constantly evolving and as such, this policy will be reviewed on an annual basis or in response to an online safety incident, whichever is sooner.

This policy is to be used alongside our Safeguarding and Anti-Bullying Policies.

The primary purpose of this policy is two-fold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.

- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

This policy is available for anybody to read on the Long Furlong School website; upon review all members of staff will sign as read and understood both the online safety policy and the Staff Acceptable Use Policy. The letter to parents and Pupil Acceptable Use Policy will form part of the 'welcome pack' when pupils join the school.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that the school has effective policies and procedures in place; as such, it will:

- Review this policy at least annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher regarding training, identified risks and any incidents.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within the school. The day-to-day management of this will be delegated to a member of staff, the online safety Officer as indicated below.

The Headteacher will ensure that:

- Online safety training throughout the school is planned, up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer has had appropriate CPD to undertake the day-to-day duties.
- All online safety incidents are dealt with promptly and appropriately.

Online Safety Officer

The day-to-day duty of the Online Safety Officer is devolved to Rose-Marie Smith.

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher and governing body on online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, ICT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose, through liaison with ICT Technical Support.

- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any online safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety Officer and Headteacher.
    - Passwords are applied appropriately to all users regardless of age.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online safety incident is reported to the Online Safety Officer (and an online safety Incident report is made) or, in his/her absence, to the Headteacher. If unsure, the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision.

All Pupils

The boundaries of use of ICT equipment and services in this school are given in the pupil Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour policy.

Online safety is embedded into the curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly, all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through school newsletters and other publications, the school will keep parents up to date with new and emerging online safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand that the school needs to have rules in place to ensure that their child can be properly safeguarded.

Technology

Long Furlong School uses a range of devices including PC's, laptops, and iPads. To safeguard pupils and to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use filtering software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, Online Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Sophos software that prevents any infected email being sent from the school, or being received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately.
(Note: Encryption does not mean password protected.)

Anti-Virus – All capable devices will have Sophos anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the "Guidance on the use of Photographic Images and Videos of Children in Schools" document. All parents must sign a photo/video release slip when their child joins the school; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Long Furlong School School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. Any member of staff who wishes to use a social network on behalf of the school should first consult the Headteacher.

The following is to be strictly adhered to:

- Parental permission must be checked via school office staff before any image or video of any child is uploaded.
- There is to be no identification of pupils, e.g. listing a pupil's name or clearly hearing his/her name being stated in a video.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the school's attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any online safety incident is to be brought to the immediate attention of the Online Safety Officer or, in his/her absence, the Headteacher. The Online Safety Officer will assist in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk-free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. online safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning.

As well as staff training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the online safety Policy. Once you have read and understood both you must sign this policy sheet

Internet access - You must not use school devices to 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 online safety incident, reported to the online safety officer and an incident sheet completed.

Social networking – is allowed in school in accordance with the online safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff should not become "friends" with parents or pupils on personal social networks. *Please refer to the "Social Media policy" for further information.*

Use of Email – staff are not permitted to use school email addresses for personal business, or personal email for school 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 pupil, or IT support.

Data Protection – If it is necessary for you to take work home or off site, you should ensure that your device (laptop, memory stick, 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 (e.g. staff outings).

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

Online safety – like health and safety, online safety is the responsibility of everyone to everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with pupils.

NAME :

SIGNATURE : **DATE :**

Acceptable Use Policy – Pupils

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that a teacher or other adult in school has asked me to do.

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

I Promise – to show respect for the work that other people have done and not interfere with it.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher or another adult in school.

I will not – share my password with anybody. If I forget my password I will let my teacher or another adult in school know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher or another adult in school has asked me to.

I will – let my teacher or another adult in school know if anybody asks me for personal information.

I will – let my teacher or another adult in school know if anybody says or does anything to me online that is hurtful or upsets me.

I will – 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 my teacher or another adult in school if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Child's Name: ………………………………………………………………………..

Signed (Parent): ………………………………………………………………………..

Date: ………………………………………………………………………..

Letter to Parents to accompany Acceptable Use Policy (Pupils)

Dear

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes extensive use of the Internet to enhance their learning and provide facilities for research, collaboration and communication.

It is very important to us that your child feels safe online and helps others to feel safe online. We therefore teach the children about online safety, which covers areas such as reporting inappropriate behaviour towards them, using electronic devices responsibly, not sharing personal information and treating others with respect. There is a specific area on the school website to support you at home in this respect, which can be found at http://longfurlongprimaryschool.org.uk/curriculum/online safety/ - the school's online safety policy can also be found here.

You will be aware that the Internet is host to a great many illegal and inappropriate websites, and we will ensure as far as possible that your child is unable to access sites such as these in school.

Please support us in our efforts to help all the children at Long Furlong to be online by going through the attached "Acceptable User Policy", explaining it to him or her, and signing/dating it and returning it to us.

Yours Sincerely

Carol Dunne (Mrs)
Headteacher

Online safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, online 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:**	

Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	online safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - pupils	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Pupil laptops	Pupils taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: How likely is it that the risk could happen (foreseeability).
Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk