

Longmoor Primary School

Online-Safety Policy



Date of Issue: Spring Term 2019
Date of Review: Spring Term 2020

**Members of staff responsible: Mr B Lyons KS1 Computing/Online-Safety
Coordinator Miss A Hughes - KS2 Computing/Online-Safety Coordinator**

Signed: Mrs J Wright - Chair of Governors (30.1.19)

LONGMOOR PRIMARY SCHOOL

ONLINE-SAFETY POLICY

Online safety is having knowledge of all forms of the dangers related to potential issues online and when using electronic devices e.g. using social media, CSE, grooming and exploitation and cyber bullying.

Online safety has a high profile at Longmoor Primary School for all stakeholders. We ensure this profile is maintained and that pupil needs are met by the following:

- ✓ A relevant up-to-date online safety curriculum which is progressive from Early Years to the end of Year 6.
- ✓ A curriculum that is threaded throughout other curriculums and embedded in the day-to-day lives of our pupils.
- ✓ Training for staff and governors which is relevant to their needs and ultimately positively impacts on the pupils.
- ✓ Scheduled pupil voice sessions and learning walks steer changes and inform training needs.
- ✓ Through our home/school links and communication channels, parents are kept up to date with relevant online safety matters, policies and agreements. They know who to contact at school if they have concerns.
- ✓ Pupils, staff and parents have Acceptable Use Policies which are signed and copies freely available.
- ✓ Our online safety policy (part of our safeguarding policy) clearly states how monitoring of online safety is undertaken and any incidents/infringements to it are dealt with.
- ✓ Filtering and monitoring systems for all our online access.
- ✓ Data policies which stipulate how we keep confidential information secure.

SCOPE OF POLICY

Longmoor Primary School believes that online safety is an essential part of safeguarding and acknowledges it's duty to ensure that all pupils and staff are protected from potential harm online. The school identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life and believes that pupils should be empowered to build resilience and to develop strategies to manage and respond to risk online.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as pupils and parents/carers.

This policy applies to all access to the internet and use of technology, including personal devices, or where pupils, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

Longmoor Primary School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm.

LINKS WITH OTHER POLICIES AND PRACTICES

This policy links with a number of other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use policies (AUP) and/or the Code of conduct
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE)
- Computer security policy
- Staff iPad agreement/policy

ROLES AND RESPONSIBILITIES

The Headteacher and Governors oversee the safe use of technology when children and learners are in their care and act immediately if they are concerned about bullying, radicalisation or other aspects of children's well-being. They are responsible for ensuring the safety (including online and the prevention of being drawn into terrorism) of all members of the school community. They have concern for the online reputation of the school.

The Online Safety Leaders will work with the Headteacher and the Designated Safeguarding Lead (DSL) to have an overview of the serious child protection issues that arise from sharing of personal data, access to illegal or inappropriate materials (including extremism and radicalisation, inappropriate online contact with adults, potential or actual incidents of grooming and cyber-bullying).

The online safety committee will work to implement and monitor the online safety policy and AUPs (Acceptable User Policies). This group is made up of online safety leaders, designated safeguarding lead (DSL), teachers, governors, members of support staff, technicians, member of senior leadership team and pupils. Pupils are an important part of this group, working with them through the school council, to contribute their knowledge and use of technology. They meet on a termly basis.

Role	Responsibility
Governors	<ul style="list-style-type: none"> • Monitor the effectiveness of the online safety policy • Delegate a governor to act as online safety link • Online safety governor works with the online safety leaders to carry out regular monitoring and report to Governors • Verify that the filtering, monitoring and or supervision systems are in place to identify children accessing or trying to access harmful and inappropriate content online
Head	<ul style="list-style-type: none"> • Ensure that all staff receive suitable CPD to carry out their online safety

Teacher and Senior Leaders	<ul style="list-style-type: none"> roles including online risks of extremism and radicalisation • Create a culture where staff and learners feel able to report incidents • Ensure that there is a progressive online safety curriculum in place • Ensure that there is a system in place for monitoring online safety • Follow correct procedure in the event of a serious online safety allegation being made against a member of staff or pupil • Inform the local authority about any serious online safety issues • Ensure that the school infrastructure/network is as safe and secure as possible • Ensure that policies and procedures approved within this policy are implemented
Online Safety Coordinator	<ul style="list-style-type: none"> • Lead the online safety committee • Coordinate work with the school's Designated Safeguarding Lead(DSL) • Log, manage and inform others of online Safety incidents and how they have been resolved where this is appropriate • Lead the establishment and review of online safety policies and documents • Lead and monitor a progressive online safety curriculum for pupils • Ensure all staff are aware of the procedures outlined in policies relating to online safety • Provide and/or broker training and advice for staff • Attend updates, subscribe to appropriate newsletters and liaise with the LA online safety staff and technical staff • Meet with Senior Leadership Team and online safety governor to regularly discuss incidents and developments
Teaching and Support Staff	<ul style="list-style-type: none"> • Participate in any training and awareness raising sessions • Read, understand, sign and act in accordance with the AUP and online safety policy • Report any suspected misuse or concerns to the online safety leaders / Designated Safeguarding Lead (DSL) and check this has been recorded • Provide appropriate online safety learning opportunities as part of a progressive online safety curriculum • Model the safe, positive and purposeful use of technology • Monitor the use of technology in lessons, extracurricular and extended school activities • Demonstrate consistently high standards of personal and professional conduct especially in relation to use of social networks, making sure that these are in line with school ethos and policies, including at the time of a critical incident
Pupils	<ul style="list-style-type: none"> • Read, understand, sign and act in accordance with the Pupil AUP / agreed class internet rules • Report concerns for themselves or others • Make informed and positive choices when using technology in school and outside school, considering the effect on themselves and others
Parents and Carers	<ul style="list-style-type: none"> • Endorse (by signature) the Pupil AUP • Discuss online safety issues with their child(ren) and monitor their home use of technology (including tablets, mobile phones and games devices) and the internet • Keep up to date with issues through newsletters and other opportunities • Inform teacher / Headteacher of any online safety concerns • Use formal channels to raise matters of concern about their child(ren)'s education • Maintain responsible standards when referring to the school on social media
Technical Support	<ul style="list-style-type: none"> • Ensure the school's ICT infrastructure is as secure as possible and is protected from misuse or malicious attack

Provider	<ul style="list-style-type: none"> • Ensure users may only access the school network using an approved password • Maintain and inform the Senior Leadership Team of issues relating to filtering • Keep up to date with online safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse can be reported to the online safety leaders for investigation • Ensure monitoring systems are implemented and updated • Ensure all security updates are applied (including anti-virus and Windows) • Sign an extension to the Staff AUP detailing their extra responsibilities
-----------------	--

EDUCATION AND ENGAGEMENT OF PUPILS

'Children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum.'

Keeping Children Safe 2018

A progressive planned online safety education programme takes place through discrete lessons and across the curriculum, for all children in all years, and is regularly revisited. Breadth and progression is ensured through reference to digital literacy via the Common Sense Education resource.

Within this:

- key online safety messages are reinforced through assemblies, Safer Internet Week (February), anti-bullying week (November) and throughout all teaching
- pupils are taught to keep themselves safe online and to be responsible in their use of different technologies as detailed in the Common Sense Education scheme of work
- pupils are guided to use age appropriate search engines for research activities. Staff are vigilant in monitoring the content of the websites visited and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material
- in lessons where internet use is pre-planned and where it is reasonable, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches
- pupils are taught to be critically aware of the content they access online, including recognition of bias and extreme or commercial content. They are guided to validate the accuracy and reliability of information
- pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- the online safety coordinators maintain and pass on knowledge of current concerns to be included within learning experiences
- pupils are provided with opportunities to influence the online safety curriculum
- pupils are educated to recognise and respond appropriately to 'different forms of bullying, including cyber-bullying' and given opportunities to support each other
- a continuous provision map is used with the youngest learners and SEN learners to establish appropriate habits for responsible use of technology

EDUCATION AND INFORMATION FOR PARENTS AND CARERS

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing online safety risks at

home, reinforcing key messages about online safety and regulating their home experiences. The school supports parents and carers to do this by:

- providing clear AUP guidance which they are asked to sign with their children
- providing regular newsletter items and appropriate support materials
- raising awareness through activities planned by pupils
- inviting parents to attend activities such as online safety week, online safety assemblies or other meetings as appropriate
- providing and maintaining links to up to date information on the school website

TRAINING OF STAFF AND GOVERNORS

There is a planned programme of online safety training for all staff and governors to ensure they understand their responsibilities, as outlined in this, and the AUPs. This includes:

- all staff knowing the Designated Safeguarding Lead and the online safety lead and their responsibilities
- an annual audit of the online safety training needs of all staff
- all new staff and governors receiving online safety training as part of their induction programme
- providing information to supply and student teachers on the school's online safety procedures
- the online safety leaders receiving regular updates through attendance at training sessions and by reviewing regular online safety newsletters from the LA etc.
- this online safety policy and its updates being shared and discussed in staff meetings and in Governor meetings
- the online safety leaders providing training within safeguarding training and as specific online safety updates and reviews
- the online safety leaders providing guidance as required to individuals and seeking LA support on issues

ONLINE BULLYING

Online bullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. The school will follow procedures in place to support anyone in the school community affected by online bullying.

Pupils and staff are made aware of a range of ways of reporting concerns about online bullying. This may be by; telling a trusted adult, online WHISPER reporting tool, Childline App and phone number 0800 1111, POSH helpline 0344 381 4772.

Pupils, staff and parents and carers are informed of their responsibilities to report any incidents of online bullying and advised to keep electronic evidence. All incidents of online bullying reported to the school will be recorded by the school. The school will follow procedures to investigate incidents or allegations of online bullying. The school will take steps where possible and appropriate, to identify the bully. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police. Pupils, staff and parents and carers will be required to work with the school to support the approach to online bullying and the school's online safety ethos. Sanctions for

those involved in online bullying will follow those for other bullying incidents as indicated in the schools Behaviour Policy or AUP and may include:

- the bully being asked to remove any material deemed to be inappropriate or the service provider being contacted to remove content if the bully refuses or is unable to delete content
- Internet access being suspended at the school for a period of time.
- the parent and carers of pupils being informed
- the police being contacted if a criminal offence is suspected

SEXTING

The school will provide appropriate support for sexting incidents which take place in and out of school. Within school, any device which has an illegal image of a child under 18, or is suspected of having such an image, will be secured and switched off. This will then be reported to the Designated Safeguarding Lead (DSL). An individual member of staff will not investigate, delete or pass on the image. The Designated Safeguarding Lead (DSL) will record any incident of sexting and the actions taken in line with advice from Derbyshire County Council.

PREVENT

The school works to ensure children are safe from terrorist and extremist material when accessing the internet on the premises. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use will identify attempts to access such material. Children are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

DATA PROTECTION

The school's Data Protection Policy provides full details of the requirements that are met in relation to Data Protection regulations.

The school will:

- at all times take care to ensure the safe keeping of personal and sensitive data, minimising the risk of its loss or misuse which must include regular back-ups and anti-virus protection updates
- use personal data only on secure password protected computers and other devices
- ensure that users are properly 'logged-off' at the end of any session in which they are accessing personal data
- provide staff with secure equipment/services to store or transfer data e.g. remote access, One Drive, SharePoint school portal, encryption and secure password protected devices
- remove data in line with the school's Data Retention Policy
- ensure that all staff are aware of the need to immediately report any loss of personal or sensitive data to the Data Protection Lead
- complete a privacy impact assessment and check the terms and conditions of sites/apps used for learning purposes to ensure that any pupil personal data is being held securely

USE OF DIGITAL IMAGES AND SOUND

Photographs, video and sound recorded within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school's learning platform and to provide information about the school on the website. The school will:

- build a culture where permission is always sought before a photo is taken or video and sound are recorded; including encouraging pupils to seek permission from other pupils to take, use, share, publish or distribute images and sound
- ensure verifiable permission from parents or carers is obtained before images, sound recordings or videos of pupils are electronically published on the school website, on social media or in the local press. The written consent, where pupils' images, video and sound are used for publicity purposes, is kept until the data is no longer in use
- when using digital images, staff educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
- allow staff to take images, record video and sound to support educational aims, following the school policy regarding the sharing, distribution and publication of those. School equipment only is used. Personal equipment of staff is not allowed for this purpose
- make sure that images, sound or videos that include pupils will be selected carefully with their knowledge, taking care when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- make adults and children aware of the risk that any published image, video and sound could be harvested, reused and repurposed
- ensure that pupils' full names will not be used anywhere on the school website, school blogs or within school branded social media, particularly in association with photographs
- not publish pupils' work without their permission and the permission of their parents or carers
- only hold digital/video images on school approved secure storage areas. There is an expectation that images and recordings are not retained longer than necessary and in line with the schools Data Retention Policy
- in accordance with guidance from the Information Commissioner's Office, parents/carers can take videos and digital images or sound recordings of their children at school events for their own personal use. It is made clear that, to respect everyone's privacy and in some cases protection, these are not to be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images or in the sound recording. We ask parents/carers not to take digital/video images or record sound during an event if it is felt that it would spoil the experience for others. A statement is made before an event as to the expectations of the school
- make clear to professional photographers who are engaged to record any events or provide a service that they must work according to the terms of the settings Online Safety Policy and will sign an agreement which ensures compliance with the Data Protection regulations and that images will only be used for a specific purpose, subject to parental consent. Photographers will not have unsupervised access to children and young people

COMMUNICATION (INCLUDING THE USE OF MOBILE DEVICES AND SOCIAL MEDIA)

A wide range of communications technologies increases effective administration and has the potential to enhance learning. The school will:

- with respect to email
- ensure that the school uses a secure business email system for communication
- ensure that personal information is not sent via unsecure email
- ensure that governors use a secure email system
- ensure that any digital communication between staff and pupils or parents and carers is professional in tone and content
- make users aware that email communications will be monitored by the school
- inform users what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature
- teach pupils about email and other communication tools alongside online safety issues through the scheme of work and implementation of the AUP
- only publish official staff email addresses where this required
- protect the identities of multiple recipients by using bcc in emails

With respect to social media e.g. YouTube, Facebook, Twitter, blogging and personal publishing

- enable online learning opportunities to make use of age appropriate educationally focussed sites that will be moderated by the school
- control access to social media and social networking sites in school
- have a process to support staff who wish to use social media in the classroom to safely set up and run a class blog/Twitter/YouTube account to share learning experiences
- provide staff with the tools to risk assess sites before use and check the sites terms and conditions to ensure a) the site is age appropriate b) whether content can be shared by the site or others without additional consent being given
- make sure that staff official blogs or wikis will be password protected and run from the school website with approval from the Senior Leadership Team
- ensure that any digital communication between staff and pupils or parents and carers is open, transparent and professional in tone and content
- discuss with staff the personal use of email, social networking, social media and personal publishing sites as part of staff induction, building an understanding of safe and professional behaviour in line with DfE advice being careful about subjects discussed online
- staff are advised that no reference should be made to pupils, parents/carers or school staff on their personal social networking accounts
- register concerns (e.g. recording in online safety log) regarding pupils' inappropriate use of email, social networking, social media and personal publishing sites (in or out of school) and raise with their parents and carers, particularly when concerning pupils' underage use of sites
- support staff to deal with the consequences of hurtful or defamatory posts about them online
- inform the staff that in the case of a **Critical Incident** they should not make any comment on social media without the permission of the senior management team

With respect to personal devices (including consideration of Keeping Children Safe 2018)

- inform staff that personal mobile phones should only be used at break, lunchtimes and in restricted areas when they are not in contact with pupils, unless they have the permission of the Headteacher
- ensure that staff understand that the AUP will apply to the use of their own portable / wearable device for school purposes
- inform staff and visitors that they are not allowed to use personal devices to take photographs or video in school for any purpose without the express permission of the Senior Leadership Team
- check any use of a personal device for an education purpose (where permission has been given) only uses the school's internet connection on the school site
- remind all that personal devices should be password protected
- advise staff not to use their personal mobile phone to contact pupils, parents and carers
- provide a mobile phone for activities that require them
- challenge staff and visitors when there is suspected misuse of mobile phones or devices
- when pupils are allowed personal devices in school, they are used within the school's behaviour policy / code of conduct, and pupils understand they can be asked to account for their use
- use the right to collect and examine any pupil device that is suspected of containing offensive, abusive or illegal content or is suspected of causing issues on the school internet connection

TECHNICAL INFRASTRUCTURE

The person(s) responsible for the school's technical support and those with administrator access to systems will sign a technician's AUP, in addition to the staff AUP. The school ensures, when working with our technical support provider that the following guidelines are adhered to:

- the School ICT systems are managed in ways that ensure that the school meets online safety technical requirements
- there are regular reviews and audits of the safety and security of school ICT systems.

Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations and other devices from accidental or malicious attempts which might threaten the security of the school systems and data with regard to:

- ensuring ongoing backups take place and, in case of an incident, the school can restore data in line with our critical incident plan
- the downloading of executable files by users
- the extent of personal use that users (staff/pupils/community users) and their family members are allowed on laptops and other portable devices used out of school
- the installing of programs on school devices unless permission is given by the technical support provider or Computing/ICT coordinator
- the use of removable media (e.g. memory sticks) by users on school devices. (see School Personal Data Policy for further detail)
- the installation of up to date anti-virus software

Access to the school network and internet will be controlled with regard to:

- users having clearly defined access rights to school ICT systems through group policies
- users being provided with an appropriate username and password (considering accessibility of users with particular needs where supervision is put in place to monitor activity)
- staff users being made aware that they are responsible for the security of their username and password which they are required to change every 60 days; they must not allow other users to access the systems using their log on details
- the 'master/administrator' passwords are available to the Headteacher and kept in the school safe
- users must immediately report any suspicion or evidence that there has been a breach of security
- an agreed process being in place for the provision of temporary access of "guests" (e.g. trainee or supply teachers, visitors) onto the school system. Anyone allowed unsupervised access must sign the staff AUP and be made aware of this online safety policy

The internet feed will be controlled with regard to:

- the school's responsibility to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" Keeping Children Safe 2016
- Foundation Stage and Key Stage 1 pupils' access will be supervised with access to specific and approved online materials
- Key Stage 2 pupils' will be supervised. Pupils will use age-appropriate search engines and online tools and activities
- requests from staff for sites to be removed from the filtered list being approved by the Senior Leadership Team and logged
- user based filtering used to provide differentiated access for staff and pupils
- filtering issues being reported immediately

The IT System of the school will be monitored with regard to:

- the school IT technical support regularly monitoring and recording the activity of users on the school IT systems
- online safety incidents being documented and reported immediately to the online safety leaders or Designated Safeguarding Lead (DSL) who will arrange for these to be dealt with immediately in accordance with school policies

REPORTING AND RESPONSE TO INCIDENTS

The school will follow Derbyshire's incident flowchart to respond to illegal and inappropriate incidents as listed in those publications. More than one member of staff (at least one should be a senior leader) will be involved in this process and the same designated computer will be used for the duration of any investigation. All sites and content checked will be recorded and screen shots, signed and dated, will be kept where this is appropriate. Should content being reviewed include images of child abuse, the investigation will be referred to the Police immediately.

- All members of the school community will be informed about the procedure for reporting Online Safety concerns (such as breaches of filtering, online bullying, extremism, radicalisation, illegal content)
- Staff will record incidents in the appropriate concerns log. All reported incidents will be dealt with and actions recorded
- The Designated Safeguarding Lead (DSL) will be informed of any online safety incidents involving child protection concerns, which will then be escalated in accordance with school procedures
- The school will manage online safety incidents in accordance with the school behaviour policy where appropriate
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact Derbyshire Children Safeguarding Team and escalate the concern to the police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Education Safeguarding Advisor or Local Authority Designated Officer (LADO).

The police will be informed where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist or terrorist material, verbally abusive or threatening material information which is false and known or believed by the sender to be false

MONITORING AND REVIEW

The online safety committee will review this policy at least annually. The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.

- We will ensure that we regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the headteacher will be informed of online safety concerns, as appropriate.
- The named Governor for safeguarding (Mr. R Wheatley) will report on a regular basis to the governing body on online safety incidents, including outcomes.
- Any issues identified will be incorporated into the school's action planning.

Date implemented: Spring term 2019

Date for review: Spring term 2020

Signed: _____ (Headteacher)

Approved by the *Governing Body* of Longmoor Primary School.

Signed: _____ (Chair of Governors)

Date: _____