Online Safety Policy

Moston Lane Community Primary School

Article 19

Children have the right to be protected from violence, abuse and neglect.

Updated	**September 2025**
Reviewed	**Annually**
Headteacher	**Mrs. E Hardwick**

Introduction

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. At Moston Lane Community Primary School, we understand that it is important to teach pupils about the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. We also understand that all staff need an understanding of the risks that exist online to allow us to tailor our teaching and support to the specific needs of our pupils. At Moston Lane Community Primary school, we are committed to supporting pupils at risk. This includes the exploitation of vulnerable young people, aiming to involve them in terrorism or to be active in supporting terrorism. Please see the Moston Lane Safeguarding Policy for further information.

Scope and Responsibilities

This policy applies to all employees in school and those who provide services for or on behalf of the school. This includes trainee teachers and any other trainees, apprentices, self-employed staff, agency staff, external consultants and volunteers. This policy also applies to school governors/trustees.

Curriculum Context

In line with the National Curriculum, from September 2020, Relationships Education will be compulsory for all primary aged pupils. Through these new subjects, pupils will be taught about online safety and harms, including what positive what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online. At Moston Lane, teachers will always endeavour to address online safety and appropriate behaviour in an age appropriate way that is relevant to our pupils' lives.

This will complement the computing curriculum at Moston Lane, which covers the principles of online safety at all key stages, with progression in the content to reflect the different and escalating risks that pupils face.

This includes:

- *Using technology safely, respectfully and responsibly*
- *Keeping personal information private*
- *Identifying where to go for help and support when they have concerns about content or contact*
- *Recognising acceptable/unacceptable behaviour*
- *Distinguishing fact from opinion and the role of the media in informing and sharing public opinion*
- *The ability to evaluate what they see online*

At Moston Lane, we understand that the online world develops and changes at great speed. New opportunities, challenges and risks are appearing all the time. Therefore, we consider it important to focus on the underpinning knowledge and behaviour that helps pupils to navigate the online world safely and confidently. This teaching will be built into existing lessons across the curriculum, covered within specific online safety lessons and school wide approaches.

Underpinning knowledge and behaviours include:

- *How to evaluate what they see online*
- *How to recognise techniques used for persuasion*
- *Online behaviour*
- *How to identify online risks*
- *How and when to seek support*

Age specific advice on potential harms and risks can be found in the following sections of the Education for a Connected World framework:

- *Managing online information*
- *Copyright and ownership*
- *Privacy and Security*

At Moston Lane, our Online Safety Curriculum planning is continually reviewed and monitored by the safeguarding team alongside the subject leader to ensure coverage of all areas. The 'Google – Be Internet Legends' scheme is implemented across KS2, whilst KS1 use specific online safety resources in discre. All year groups from EYFS to KS2 also use Project Evolve resources throughout the year. Further details of this can be found in the Online Safety curriculum map.

Teaching and Learning

At Moston Lane, all teachers are responsible for promoting and supporting staff behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Teachers must create a safe environment that is sensitive to the pupils in their class. Where staff are already aware of a child who is being abused or harmed online they should carefully plan any lesson to consider this, including not drawing attention to that child in a way that would highlight or publicise the abuse. It is good practice to include the Designated Safeguarding Lead (or a deputy) when considering and planning any safeguarding related lessons or activities (including online) as they will be best placed to reflect and advise on any known safeguarding cases, and how to support any pupils who may be especially impacted by a lesson.

All key stages spend time in the Autumn term learning about and embedding the key principles for online safety. Further to this, Online Safety is discussed and re-capped prior to any online activity and as a beginning to every discrete computing lesson. Regular opportunities are taken to reinforce online safety measures in all lessons and to teach pupils to be critically aware and consider the accuracy of information they access online. Online safety measures are also reinforced through other subjects and through a planned programme of other activities such as assemblies and whole school events.

Filtering and Monitoring/Safety Measures

Surfing the Web

Aimless surfing should never be allowed. Pupils should be taught to use the internet in response to an articulated need e.g. a question arising from work in class. Search engines can be difficult to use effectively. The teacher will need to choose a topic with care, select the search engine and then discuss with pupils sensible search words, which should be tested beforehand.

Roles and Responsibilities

DSL (Mel Adams) Nic Higgins (Assistant Head – KS1) and Governor (***)
will undertake regular checking and monitoring of our filterning and monitoring systems, in-line with the checklist (appendix 1 of this policy)

> "All staff must receive safeguarding and child protection training
> which includes online safety and an understanding of the expectations,
> applicable roles and responsibilities in relation to filtering and monitoring."
> (KCSIE 2024)

All staff

All staff have received training around their roles and responsibilities around filtering and monitoring, and know they have a responsibility to report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks

- *they notice abbreviations or misspellings that allow access to restricted material*

Education Programmes:

Pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering and monitoring.

This school:

- *Fosters a 'No Blame' environment that encourages pupils to tell a teacher/responsible adult immediately if they encounter any material that makes them feel uncomfortable.*
- *Ensures pupils and staff know what to do if they find inappropriate online material*
- *Has a clear and progressive Online Safety education to be taught throughout all key stages, built on LA/LGfL/National guidance.*
- *Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;*
- *Makes training available annually to staff on the Online Safety education program;*
- *Runs a rolling programme of advice, guidance and training for parents, including:*
  Information in safety leaflets; in school newsletters; on the school web site;
  Demonstrations, practical sessions held at school;
  Suggestions for safe Internet use at home;
  Provision of information about national support sites for parents.

How will e-mail be managed?

Technology Safety:

Procedures

In the school context, e-mail should not be considered private and most schools, Moston Lane Community Primary School reserve the right to monitor e-mail. There is a balance to be achieved between monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. The use of email in the school is limited to the use of accounts on the school domain within the school network. Personal e-mail addresses, such as Hotmail are blocked by the school system. Pupils will have class based email addresses which allow them to send and receive messages to and from the wider world, need to be carefully allocated to appropriate situations. All lessons that involve children sending or receiving emails must have full planning approved by the computing coordinator.

This school:

- *Does not publish personal e-mail addresses of pupils or staff on the school website.*
- *We use anonymous or group e-mail addresses.*
- *If one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law we contact the police.*
- *Accounts are managed effectively, with up to date account details of users.*
- *Do not to give out their e-mail address unless it is part of a school managed project or someone they know and trust and is approved by their teacher or parent/carer;*
- *That an e-mail is a form of publishing where the message should be clear, short and concise;*
- *That any e-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;*
- *They must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc;*
- *To 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;*
- *The sending of attachments should be limited;*
- *Embedding adverts is not allowed;*

- That they must immediately tell a teacher / responsible adult if they receive an e-mail which makes them feel uncomfortable, is offensive or bullying in nature;
- Not to respond to malicious or threatening messages,
- Not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
- Not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
- That forwarding 'chain' e-mail letters is not permitted;

- Pupils sign the school Agreement Form to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with.
- Staff sign the appropriate LA / school Agreement Form to say they have read and understood the Online Safety rules, including e-mail and we explain how any inappropriate use will be dealt with

Using Digital Images and Video Safely

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety.computing coordinator to oversee / authorise the website's content and check suitability. It should be clear who has authority to upload content into sections of the website.

Use of still and moving images

Procedures:

Use excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked before inclusion on a school website to ensure that the content is appropriate both to the school and for the intended audience. Remember that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too. Text written by pupils should always be reviewed before publishing it on the school website. Make sure that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Although it may seem obvious, check that pupils' work doesn't contain any statements that could be deemed defamatory. Ensure also that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

Technical:

Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period. When saving pictures, ensure that the image file is appropriately named. Do not use pupils' names in image file names or in <ALT> tag references when published on the web. *[An ALT tag is the HTML text describing a displayed image, used mostly for reasons of accessibility, since the tag can be voiced by screen readers].*

1

Education:

Ensure staff and pupils know who to report any inappropriate use of images to and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work. In this school:

The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
Uploading of information is restricted to SLT, Computing coordinator, Website lead teacher.
The school web site complies with the school's guidelines for publications;
Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
The point of contact on the web site is the school address and telephone number.
Home information or individual e-mail identities will not be published;
Photographs published on the web do not have full names attached;
We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted when children leave the school – unless an item is specifically kept for a key school publication;
We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website;
We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;

Pupils are only able to publish to their own safe' KidBlog in school;

Pupils are taught about how images can be abused in their eSafety education programme as part of the national curriculum.

How will infringements be handled?

Whenever a student or staff member infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

Students

Category A infringements:

Use of non-educational sites during lessons

Unauthorised use of email

Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends

Use of unauthorised instant messaging / social networking sites.

Sanctions reffered to computing coordinator.

Category B infringements

Continued use of non-educational sites during lessons after being warned

Continued unauthorised use of email after being warned

Continued unauthorised use of mobile phone (or other new technologies) after being warned

Continued use of unauthorised instant messaging / chatrooms, social networking sites, NewsGroups

Use of Filesharing software e.g. Napster, Vanbasco, BitTorrent, LiveWire, etc

Accidentally corrupting or destroying others' data without notifying a member of staff of it

Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Sanctions: referred to Class teacher, Online Safety Coordinator / removal of Internet Access rights for a period / contact with parent.

Category C infringements

Deliberately corrupting or destroying someone's data, violating privacy of others

Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)

Deliberately trying to access offensive or pornographic material

Any purchasing or ordering of items over the Internet

Transmission of commercial or advertising material

Sanctions: as category B and referred to deputy head.

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site

Category D infringements

Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned

Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent

Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988

Bringing the school name into disrepute

Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / removal of equipment / refer to Community Police Officer / LA Online Safety officer

Other safeguarding actions:

1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider

Staff

Category A infringements (Misconduct)

Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.

Misuse of first level data security, e.g. wrongful use of passwords

Breaching copyright or license e.g. installing unlicensed software on network

Sanction - referred to line manager / Headteacher. Warning given.

Category B infringements (Gross Misconduct)

Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;

Any deliberate attempt to breach data protection or computer security rules;

Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;

Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;

Bringing the school name into disrepute.

Sanction - Headteacher.

Tackling extremism and radicalisation

As a school we are fully committed to safeguarding against radicalisation and extremism. The aim is to protect individuals against radicalisation, or being exposed to extremist views, by identifying who they are and providing them with support. We are trained to recognise or identify safeguarding issues (Please see extremism and radicalisation policy).

Indicators:

Increased usage of social media.

Secretive usage of social media.

Attempting to access inappropriate websites.

Attempting to keep online activity secret.

Attempting to keep online peers secret.

Usernames or avatars that relate to a particular group.

Public comments that relate to a group or cause.

Please see the Prevent section of our Safeguarding policy for further information.