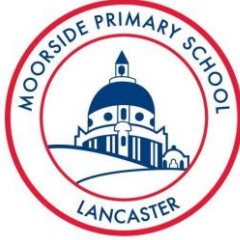


Moorside Primary School		
Document Name	Online Safety Policy	
Date	September 2023 Next Review: September 2024	
Version	4	
Audience	Staff, Governors, Volunteers, Parents, Website	
Approved by	The Governing Body, 14th September 2023	

Background and Scope of the Policy

This Online Safety Policy is one of a number of policies which form part of the school's approach to safeguarding. Other documents which are specifically related to it are the:

- Child Protection and Safeguarding Policy
- Cyberbullying Policy,
- the school's statements about Responsible Computer Use displayed in school for pupils
- the staff 'Acceptable Use Policy'.
- use of IT agreements signed by pupils
- Monitoring and Filtering Policy

Through this policy, we aim to set out:

- how technology can enhance learning and describe the range of technology used in school
- how we balance security measures with the need for children to learn effectively
- how we educate pupils to recognize the risks associated with technology and how to deal with them

The policy also sets out how we respond when inappropriate use has been made of technology.

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Curriculum and Pupils Sub Committee receiving regular information about online safety incidents and monitoring reports. At Moorside, the Safeguarding Governor takes on responsibility for online safety and monitoring and filtering. The role of the Online Safety *Governor* will include:

- regular meetings with the Online Safety Lead/DSL
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering logs

- reporting to relevant governors' meetings

Headteacher and Senior Leaders

- In conjunction the DSL team and the Online Safety Lead, the Headteacher is responsible for the development of policy and practice
- The Headteacher also has a duty of care for ensuring the safety (including online safety) of members of the school community on a day-to-day basis (ie incidents arising out of any breaches of the filtering system). The Headteacher will liaise with the Online Safety Lead and technician about issues which may arise.
- The Headteacher is responsible for liaising with the provider which monitors the effectiveness of the school's filtering system.
- The Headteacher and DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – “Responding to incidents of misuse” and relevant *Local Authority* disciplinary procedures).
- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Online Safety Champion/Lead

At Moorside the Online Safety Lead is the Computing Subject Leader. Their responsibility is for curriculum provision, technical support and advice to colleagues about aspects of teaching. They work in conjunction with the DSL team to promote safeguarding and respond when issues arise.

- the lead DSL and Online Safety Lead meet with the pupil group who report on online safety issues
- they have a leading role in establishing and reviewing the school online safety curriculum provision
- provides training and advice for staff
- liaises with school technical staff
- they liaise with the Headteacher and DSL about issues which have been identified and adapt teaching and provision accordingly
- liaise with the Online Safety *Governor* to discuss current issues
- reports to Senior Leadership Team if issues arise relating to use of technology in school

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any *Local Authority* online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and DSL for investigation and appropriate action
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school safety policy and practices
- they have read, understood and signed the staff acceptable use agreement
- they report any suspected misuse or problem to the Headteacher for investigation and appropriate action
- all digital communications with pupils and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (at age-appropriate levels)
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- computer use is carried in line with the Monitoring and Filtering Policy

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

Online Safety Group

At Moorside the school council acts as our 'Online Safety Group' and provides a consultative group that has wide representation from the school community with responsibility for issues regarding online safety and the monitoring of the Online Safety Policy including the impact of initiatives.

Members of the Online Safety Group will assist the school leadership with:

- monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety/digital curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and the pupils about the online safety provision

Pupils:

- are responsible for using the school digital technology systems in accordance with the student/pupil acceptable use agreement

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Education – Parents/carers

Parents can play a key role in helping their child to stay safe online, however, their understanding of the risks children face online will be variable.

Moorside School will therefore seek to provide information and awareness to parents and carers through:

- curriculum activities
- letters, newsletters and the school web-site,
- workshop sessions
- high profile events/campaigns e.g. Safer Internet Day
- reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)

Community Users

Community Users who access school systems are asked to sign the school's Acceptable Use Agreement.

Why the internet and digital communications are important

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience. Children are taught how to use the internet effectively, critically and safely in specific computing lessons. They also make use of it as a tool for research within other subjects.

Teaching about online safety

There are a number of approaches to our teaching about online safety

1. Explicit teaching about online safety takes place **through dedicated sessions**. These include:
 - computing lessons which explore different issues and allow children to apply their learning in a range of contexts
 - PSHE lessons
 - Kidsafe which addresses online safety at age appropriate levels as the children move through school
 - assemblies

More detail about the teaching of online safety is included in the curriculum coverage section of our website.

2. Children also learn about **keeping safe online through the use of technology in other subjects**. For example, they are given reminders within other subjects when the internet is being used for a range

of purposes; within these, children are taught to evaluate what they see and to be critically aware of content and materials and an environment should be created where they feel comfortable to discuss issues arising from the materials.

3. Other aspects to the teaching of safety online

- pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school.
- staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.

Enhancing learning through the use of the internet

Internet access is an essential aspect of a school in the 21st century. The level of access is tailored to the needs of the users across the school and includes filtering appropriate to the age of pupils. Levels of staff access are different to those of pupils, but this higher level of access is restricted to computers used by staff.

At times, pupils will be taught specific skills for searching the internet effectively. At other times, they will use the internet as tool to enhance learning in other subjects.

- pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation
- pupils will be shown how to publish and present information to a wider audience in an appropriate way.

Pupils will be taught how to evaluate internet content

The school makes use of 'Fortinet' as a system for filtering content. Although it is filtered, the system does not provide a complete block as this is seen as limiting pupil ability to learn about appropriate use.

- the school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- pupils will be taught the importance of cross-checking information before accepting its accuracy.
- pupils will be taught how to report unpleasant internet content to teachers or to the Online Safety Lead.

Authorising internet access

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. At Key stage 2, pupils have greater freedom to search the internet, but they should do this according to guidelines set by the teacher.

E-mail

The school recognises the vital role e-mail plays in the 21st Century. The school teaches pupils about the value of e-mail and how to send and receive them safely. The key components of our approach are:

- email is provided to all users via the Lancashire Grid for Learning service.
- pupils may only use approved e-mail accounts on the school system.
- pupils must immediately tell a teacher if they receive offensive e-mail.
- in e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone.
- incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- the school should consider how e-mail from pupils to external bodies is presented and controlled (through staff).
- the forwarding of chain letters is not permitted.
- all users (staff and pupils) should be aware that their emails may be monitored in accordance with the 'Acceptable Use Policy'.
- staff may access private emails in their own time, however they must be aware that the content must not breach 'Acceptable Use' guidelines and must not contain anything illegal or unprofessional.

Staff/Volunteers – Training

Adults in school receive training in line with their responsibilities. Training will be offered as follows:

- a planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- all new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school safety policy and acceptable use agreements.
- the Online Safety Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- this online safety policy and its updates will be presented to and discussed by staff in staff meetings be circulated electronically and be stored in an accessible place on the Teacher Drive.
- the Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.

Governors - Training

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in school training/information sessions for staff or parents

Published content and the school web site

The school website is primarily for the sharing of information about the school with parents, pupils and third parties who wish to find out more about the school's work. A number of basic rules will be followed to ensure that content is appropriate and does not expose staff or pupils to undue risk:

- staff or pupil personal contact information will not be published. The contact details given online should be the school office.
- the number of staff who can physically upload material is restricted.
- the headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- photographs that include pupils will be selected carefully and should never include any pupils whose parents who not given consent.
- a pupil's full name will not be used anywhere on a school website or other on-line space, particularly in association with photographs.
- written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- work can only be published with the permission of the pupil and parents/carers.
- pupil image file names will not refer to the pupil by name.
- parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- the school acknowledges the popularity and widespread use of social networking sites for personal publishing and information sharing. Parents are advised that some social networking sites do not permit membership to children until they are 13 (eg. Facebook).
- the school will not allow access to social networking sites, but educates pupils in their safe use if used out of school.
- newsgroups will be blocked unless a specific use is approved.
- pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- although staff, volunteers or pupils may have social network accounts, they are not permitted to make any comment about any aspect of school life in this forum.

Managing filtering – please refer to the separate Monitoring and Filtering Policy for more detail

- the school will work with the internet provider to ensure systems to protect pupils are reviewed and improved.
- if staff or pupils come across unsuitable on-line materials, the site must be reported to the Headteacher/DSL Team.
- the Headteacher in conjunction with the Online Safety Lead and the IT Technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Photographs

Children may have their photographs taken to provide evidence of their achievements for developmental records. Photographs may be taken during lessons as evidence of a child undertaking learning activity, on school visits or special events eg a show. Any photographs should be taken on school equipment and should be done so in line with the level of permission given by the parents/carers.

Photographs can only be taken by school staff. Parents or other visitors have no permission to take photographs unless permission has been specifically given by the school. – **see separate policy.** Parents are advised on a case-by-case basis on the level of permission being given.

Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own records.

Procedures

Under the Data Protection Act 1998, the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school server, which is password protected. Photographs should be deleted from the memory card of the camera within a week. They should be deleted from the server within two years after a child has left the school. Hard copies of photos may be stored in the school's archive as part of its record of historical events.

The school's digital camera/s or memory cards must not leave the school setting unless on an official school trip. Photos are printed/uploaded in the setting by staff and once done, images need to be removed from the camera's memory within a week.

On admission, parents will be asked to sign the consent for photographs to be taken in school or by the media for use in relation to promoting/publishing the school. This consent will last for a maximum of 5 years only. This does not cover any other agency and if any other agency requests to take photographs of any child then separate consent before photographs are taken will be sought.

It is acknowledged that often photographs may contain other children in the background. If the photograph is likely to be viewed by anyone other than school staff, then 'photo permission' must also have been given for those children.

Mobile Phones - Staff

Staff are permitted to have mobile phones in school. However, they must not be used in the presence of pupils unless it is an emergency. Ideally they should be used in staff areas ie the staff room or office areas. They may be used at break-times in empty classrooms. They are not to be used in circulation areas unless it necessary to deal with an emergency or school related matter.

Cameras and mobile phones are prohibited in toilet or changing areas.

Staff should approach the Headteacher if there are circumstances where special arrangements are needed with regard to mobile phones.

Mobile Phones – Volunteers/Students/Visiting Staff

Visitors may be asked to leave phones in the lockers provided during their contact time with children.

Pupils and Mobile Phones

Pupils are not ordinarily be permitted to bring mobile phones to school. In the event of a child having a phone in school, then it should be stored in the office safe until the end of the day.

Please refer to our separate 'Cyberbullying Policy' for further comments about our approach to pupils, mobile phones and social networking.

Managing videoconferencing & webcam use

- videoconferencing should use the educational broadband network to ensure quality of service and security.
- pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- videoconferencing and webcam use will be appropriately supervised for the pupil's age.
- it may be necessary to make use of 'Apps' such as Zoom or Teams. Where this is the case, permission will be sought from parents and guidance issued to parents and school staff to ensure that safeguards are in place at both ends of the 'call'.

Managing emerging technologies

- emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- the senior leadership team should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- pupils are not permitted to have or use mobile phones in school unless it is part of a specifically agreed activity.
- games machines including the Sony Playstation, Microsoft Xbox and others have internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- the school may make use of 'Seesaw', an online learning platform when it is necessary to set work for pupils who cannot access school. As parents and pupils use it for the first time, guidance for using it safely and appropriately are issued.
- 'Tapestry' is used for sharing information about learning and development in Reception and Y1. Access is via a secure login to individual accounts. Where a photograph contains more than one child, staff must ensure that the school holds permission for the child's image to be shared with other people.

Security and data management – see the school's IT Acceptable Use Policy

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

Data must be:

- accurate
- secure
- fairly and lawfully processed
- processed for limited purposes
- processed in accordance with the data subject's rights
- adequate, relevant and not excessive
- kept no longer than is necessary
- only transferred to others with adequate protection

In practice this means that:

- all staff computers are password protected
- passwords are required to access emails
- staff should not access pupil data through unsecured wireless systems at home
- mobile devices should be password protected (laptops and mobile phones) but should not contain personal details about pupils if they are used off-site (addresses, date of birth, medical conditions or information relating to safeguarding). They may be used to write comments about achievements or make comments about work
- transfer of information to third parties should be through the LCC secure email system or through another closed system

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Filtering logs are analysed each week to assess how the internet is being used and staff are vigilant in lessons. Pupils are taught what to do if they see something which makes them uncomfortable.

Dealing with Incidents

Handling online safety complaints

Complaints of internet misuse will be dealt with by an appropriate member of staff. Any complaint about staff misuse must be referred to the Headteacher.

Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures. Pupils and parents will be informed of consequences for pupils misusing the internet.

Illegal Incidents

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to external authorities eg Police, CEOP. Staff must not personally investigate, interfere with or share evidence. Always report illegal content to the Internet Watch Foundation.

Examples of illegal offences include:

- accessing child sexual abuse images
- accessing images of child abuse
- accessing criminally obscene adult content
- incitement to hatred or expression or promotion of extremist views

Communicating the Policy

A key principle of our approach is to involve the children in the development of our practice. They contribute via the school council

- online Safety rules will be posted in rooms where computers are used and will be discussed with pupils regularly.
- pupils will be informed that network and internet use will be monitored and appropriately followed-up.
- there is an ongoing programme of online safety training. This includes a number of elements:
i) 'Kidsafe' is followed through school as an approach for teaching about safeguarding and includes an online safety element
ii) Specific teaching about online safety as part of our computing curriculum
iii) Ongoing reminders when using computers in other subjects

Staff and the Online Safety policy

- all staff will be given the School Online Safety Policy and its importance explained.
- staff must be informed that network and internet traffic can be monitored and traced to the individual user.
- staff will use school cameras and school computers for taking, processing and storing images of pupils. Personal mobile phones must not be used

Parent awareness of the school's approach to Online Safety is a vital part of the school's work:

- parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, and on the school website.
- the school will maintain a list of online safety resources for parents / carers.

Evaluation and Review

The policy will be reviewed at least annually or when significant changes in technology occur. We will consider the number of complaints received, the occurrence of inappropriate materials, the receipt of any offensive messages and computer or phone misuse by staff or pupils.

RESOURCES

www.thinkuknow.co.uk KS2

www.hectorsworld.com KS1

www.digizen.org/cyberbullying

www.teachernet.gov.uk

www.thinkuknow.co.uk/teachers

www.childnet.com

www.becta.org.uk/schools

