

Online Safety Policy

‘Together we unlock potential and learn for life’



This policy was approved by the Governing Body of Moor First School at their meeting on:

SignedChair of Governors

SignedHeadteacher

Review Frequency: Every 2 years

Next Review: June 2028

Version	Date	Reason for change
Version 1	January 2025	New Policy
Version 2	June 2026	Revisions to bring in line with CFLP and Governor Handbook Updates

Introduction

Moor First is committed to ensuring that all learners and staff are safe, responsible and empowered users of digital technologies. Moor First recognises the uniqueness of every child, champions inclusion, promotes aspiration, inspires learning, and encourages all learners to become responsible citizens of the future. These values underpin our approach to digital safety, ensuring that all schools create environments where learners understand both the opportunities and risks associated with technology.

This policy aims to:

- Ensure every learner becomes a safe, respectful and responsible digital citizen.
- Provide clarity for staff, governors, pupils and parents on safeguarding expectations.
- Support schools in implementing consistent online safety practice across the school.
- Embed online safety in all areas of curriculum and school life.

All pupils and staff, who access the internet or social media from the school site or using school technology resources when off site, must be aware that they are responsible for everything that takes place on their computers, tablets or mobile phones and that all activity, including use of the internet may be logged.

Benefits

Access to the internet, email and social media will enable pupils and staff to:

- Access and explore a wide variety of sources of information to support and enhance the educational experience
- Access curriculum resources and exchange work with staff and other pupils
- Access webinars, videos and other resources to support the curriculum
- Keep informed of news and current events
- Take part in live discussions and other events
- Extend the curriculum and be included in initiatives relevant to their education and take part in global educational projects
- Make links with experts
- Publish and display work via websites
- Communicate with other internet users around the world

Effective Use

Internet and social media access will be planned to enrich and extend learning. Pupils will make best use of the internet and social media if:

- They have been given clear objectives for using the internet and social media.
- They have been educated in safe, responsible and effective internet or social media use.
- They are supervised when appropriate.

- They appreciate and control their internet use, ensuring that they balance learning and they understand and apply safeguarding principles, how to handle themselves safely on-line and how and where to report any Child Exploitation, On-line Protection, counter-terrorism and radicalisation issues.
- They are encouraged to evaluate sources and to discriminate between valid and inappropriate materials.
- They know how to copy, save and edit material from the internet or social media without infringing copyright and data protection.

Curriculum Intent and Digital Citizenship

Moor First ensures that online safety is woven into the wider curriculum intent, recognising the need for a progressive, knowledge-rich and contextually relevant education. Beginning in EYFS, pupils learn how to explore technology safely. As they progress, they are introduced to concepts such as the SMART rules, recognition of trustworthy information, respectful communication, privacy awareness and safe online identity behaviours.

At Moor First, digital citizenship includes:

- Understanding online rights and responsibilities.
- Evaluating the reliability and credibility of online content.
- Respecting intellectual property, including copyright and plagiarism awareness.
- Demonstrating empathy, kindness and respect in online interactions.
- Understanding digital footprints and long-term online reputation.

Through Computing, PSHE, English, and cross-curricular digital experiences, pupils learn how to navigate online environments safely and effectively. Learning objectives are mapped across the Computing Progression Documents to ensure coherence and age-appropriate sequencing across all phases.

The 5Cs Model of Online Safety

Moor First adopts the updated 5Cs model of online risk, which builds on the traditional 4Cs and reflects the addition of “Credibility” in the 2025 KCSIE update. Each category is explicitly taught and reinforced across the curriculum:

1. **Content** – Exposure to harmful or inappropriate material, including extremist content, pornography, violence, self-harm or hate.
2. **Contact** – Risks of harmful or manipulative interactions such as grooming, coercion, unwanted communication or contact via gaming, messaging apps or social networks.
3. **Conduct** – Behaviours that can harm oneself or others, including cyberbullying, aggression, sharing inappropriate images, hacking attempts, or online rule-breaking.
4. **Commerce** – Commercial exploitation such as scams, gambling, phishing, fraudulent messaging and online financial targeting.
5. **Credibility** – Misinformation, disinformation, conspiracy theories, online fakeness (including deepfakes), deceptive AI-generated content, and misrepresentation.



Pupils are taught to critically evaluate online information, understand how algorithms and persuasive design influence behaviour, and recognise when information may be misleading or manipulated.

Implementation

Implementation strategies reflect the developmental stages of pupils and ensure consistent practice:

EYFS:

- Early exposure to safe technology use.
- Recognising trusted adults and knowing when to ask for help.
- Beginning awareness of personal information and privacy.

Key Stage 1:

- SAFE online behaviours through the SMART rules.
- Understanding private vs. public information.
- Recognising upsetting or confusing content and seeking help.
- Introduction to digital citizenship and respectful communication.

Key Stage 2:

- Safe use of email, search engines and collaborative tools.
- Identifying cyberbullying and understanding consequences.
- Understanding copyright, ownership and plagiarism.
- Developing research skills and evaluating credibility of content.
- Introduction to AI-generated content, bias and misinformation.

Progression is monitored through PurpleMash, classwork and teacher assessments.

Online safety is embedded not only through Computing but across PSHE, English, Humanities, assemblies, themed weeks and national events such as Safer Internet Day.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Governing Body have ultimate responsibility to ensure that policy and practices are embedded and monitored. The responsibility is delegated to the Headteacher. Any extra permission given by

the Headteacher must be recorded (memos, minutes from meetings) in order to be validated.

The named person (Safeguarding Lead) and Deputy Safeguarding lead, have responsibility for ensuring that all members of the school community uphold this policy and they have been made aware of the implication that this has. It is the role of this member of staff to keep abreast of new guidance such as the LA, CEOP, Childnet and Local Authority Safeguarding Children Board.

As a professional organisation with responsibility for safeguarding, it is important that staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using technology, they are required to read and sign the Acceptable Use Policy.

It is the pupil's responsibility to use these resources in a manner that is efficient, ethical and legal. They are required to read and sign the Acceptable Use Policy. All children will engage in a discussion about this with their teacher to ensure that they fully understand. The use of computing resources is a privilege and therefore, inappropriate use may result in this being withdrawn.

E-safety rules will be posted in classrooms and safer internet day celebrated in school.

KS1 poster:



KS2 poster:



Data Security and Privacy

All data is stored in accordance with provision of the General Data Protection Regulations.

Social Media, Learning Platforms and Reporting Misuse

Internet access from the school site is carefully filtered and monitored. Access to inappropriate websites will be blocked, either on a website-by-website basis or by blocking inappropriate key images, words or phrases. Internet activity on the school premises is monitored and logged. School technology equipment used off site may be checked for inappropriate use. In the case of tablets, pupils, parents and staff have a responsibility to act in accordance with the policy and associated guidance. Appropriate sanctions are in place and will be carried out in the event of misuse.

Staff must obtain permission from Senior Leaders to use any chat room services. Live chat rooms must not be used unless posts are filtered prior to posting.

Social media

If required by the school, the authorised social media platforms available are solely X (formerly Twitter) and Facebook. These platforms can be used by school to celebrate achievements and promote news across the whole school.

Staff must not use any existing personal social media accounts for school social media activity. Staff must only use the school accounts for school social media. Any request for a new social media account must be made to the Headteacher for approval.

All school social media postings must be professional and appropriate in tone and content. If a member of staff has any concern about a social media posting which they have already made they should contact the Headteacher.

It is ultimately the responsibility of staff to ensure that they set and convey appropriate standards for social media and internet use. Staff and pupils should be aware at all times of the potential consequences of inappropriate use of the internet or social media, which could include loss of access to school computing facilities, disciplinary action and, in extreme cases where misuse could constitute a criminal offence (for example, an incident of cyberbullying, exchanging indecent images, accessing extreme pornography or extremist/radicalisation material) will be reported to the appropriate police or other child protection authority.

Staff should not befriend pupils or their families on social media unless they are related to them.

Any pupil who suspects misuse of the internet, social media or computing facilities by another pupil must report this to their classroom teacher. Any member or staff who suspects misuse of the internet, social media or computing facilities must report this to the

Headteacher. Any serious or potentially illegal misuse of the internet or computing facilities such as accessing pornography, cyber-bullying and on site use of internet and school computing facilities for personal financial gain, or damaging the reputation of the school through use of social media must be reported to the Headteacher, or, in the case of misuse by the Headteacher, to the Chair of Governors. If a child protection or radicalisation issue is suspected, a report should also be made to the Designated Safeguarding Lead.

Online Learning Platforms

At Moor First, we use SeeSaw to record and store all observations and assessments relating to each child. This is a safe and secure system and enables parents and carers to access their child's learning journey at any time. Parents/carers can share them with their child, family and friends at home. They may use it for home learning tasks and post any comments/photographs/recordings of their own. This helps to create a fully holistic view of the child and strengthen the parent partnership.

Safety and Security

Staff use iPads/tablets to take the photographs for observations which are be uploaded to the journals. Each staff member has a secure login, which is password and pin protected. The iPads/tablets are kept in a secure facility at school and may only be taken home by staff members for specific reasons and with the express consent of management. Staff should have minimal need to work on journals at home but if they wish to do so, they may access the platforms using their own device. Staff are not permitted to download any photographs of the children onto their own devices. If staff do work on the platforms at home, they should be aware of any other people around them and make sure they are not overlooked. They must logout as soon as they have stopped working. If any member of staff suspects that their login details have been compromised in any way, they must inform the school safeguarding lead and new login details will be created. All data held on these platforms, are bound by the Data Protection Act. Photographs stored on the iPads/tablets are deleted on a regular basis by a member of staff.

Parents/carers logging in to the platforms can only access their own child's Learning. Parents may input new observations, video recordings, completed work and photo's, and add comments to existing observations/work. They do not have the necessary permission to edit existing content. Regarding the platforms, parents/carers are asked to give permission for:

- Their pupil's name to be used
- Classwork and homework to be uploaded to their personal child's journal/journey
- Photos and videos of their child working to be uploaded to their personal child's journal/journey
- Photos and videos of their child's work and their child working to be shared publically with the class and their families.
- Examples of completed work to be shared on social media sites – Twitter.

If parents withhold consent for any of these, class teachers are informed so that they can ensure GDPR compliance when using these platforms.

Parents without internet: we will print all the information from the platforms and collate it into a paper Learning Journey.

When children leave Moor First, we will transfer the account to the new setting, if they also use the same platform. If they do not, we will email a PDF to the setting.

Parents will be given the opportunity to download their work at the end of each academic year and if leaving to a new setting. The child's information and their Learning Journey will be archived from year to year but permanently deleted from our accounts, once the child leaves our school.

Staff Guidelines

Staff are advised to use their school email address only for professional use and avoid using it for personal use in order to avoid concerns or accusations of misuse of school computing facilities. Other important documents can be password protected through the email system.

Staff must **never** allow others to use their accounts and should not reveal their password to others. The Headteacher must be informed if it is suspected that someone else knows your account details or passwords.

Staff must always log off or lock their computer when they finish working. Please do not leave a computer unattended while you are logged on.

Staff must always implement suitable security measures on portable devices such as a PIN or password.

The school network, especially SIMS or Arbor, allows office staff to have access to confidential information about pupils and staff. Staff must ensure that such information remains confidential at all times. The General Data Protection Regulations apply to the school, pupil and staff data. These requirements must be followed. Any queries regarding the requirements and implications of the GDPR must be directed to the School Office Manager.

Staff must not use school computing facilities to access inappropriate internet content, for personal financial gain and must only access social networking sites for the purposes of enhancing the teaching and learning experience for pupils.

Staff must be aware of and comply with copyright and ownership restrictions when they copy, download or use in lessons any materials from the internet.

Staff must not send photographs, video or audio of pupils as email attachments nor post photographs, video or audio of pupils on websites unless they have permission to do this from pupils' parents or carers and the permission of the Schools Leadership Team. No pupil

should be identifiable by name. All materials must represent the school in an appropriate way.

Staff must not send data relating to pupils or any other restricted data to personal email accounts.

When printing confidential material staff must use a secure print method by using a password protected retrieval system. Any confidential material not retrieved by the owner should be put immediately in confidential waste/shredded.

Staff should be aware that email traffic is retained on school servers even if they are deleted from individual accounts.

Staff must obtain permission from Senior Leaders to use any chat room services. Live chat rooms must not be used unless posts are filtered prior to posting.

Staff must ensure that they adhere to all relevant policies and procedures including, but not limited to GDPR Policy, safeguarding and professional standards. As examples the following are not permitted: sharing of personal messages, photographs, video and audio, language must always be professional and appropriate. This list is not exhaustive.

Staff are reminded that misuse of the schools computing facilities, internet or social media to access inappropriate materials or for personal financial gain, or damaging the school's reputation in any way, could result in disciplinary action being taken, including loss of access to computing facilities, a verbal or written warning, suspension or dismissal according to school policy. Extreme cases of misuse and all illegal activity will be reported to the police authorities.

Staff have a duty to report all suspected misuse. This should be to the computing curriculum leader in the first instance. Extreme misuse must always be reported to the Headteacher, or, in the case of the Headteacher, to the Chair of Governors. Any possible child protection issues must also be reported to the Designated Safeguarding Lead.

Staff must not leave portable devices such as tablets or mobile phones unattended. Staff must not use software, systems or devices that circumnavigate school managed internet safeguards including the use of mobile hot spots.

Training

All staff attend regular training sessions to ensure they are up to date with all e-safety regulations and to remain compliant with GDPR regulations. During these sessions, governors are invited to attend and the link governor attends.

Links to other policies and documents

Pupils and staff are reminded that the guidelines and expectations for good conduct in and around the school that are set out in the following policies and apply to use of the schools computing facilities, the internet and social media:

- Pupil Behaviour/ Anti Bullying.
- Safeguarding
- Pupil / Staff Acceptable Use Agreements
- Teacher Professional Standards
- GDPR Policy
- Code of Conduct for Staff

Integration with PSHRE and Safeguarding

Online safety is fully embedded within PSHE, safeguarding teaching, and pastoral systems. Pupils explore topics such as consent, respectful relationships, resilience, emotional wellbeing, digital footprints, peer influence, social pressures, and managing online conflict.

Safeguarding teams monitor online safety issues through behaviour logs, monitoring alerts and filtering systems. Themes emerging in safeguarding data inform future curriculum planning and targeted interventions, including via class assemblies, circle times, adaptation to the planned PSHE curriculum.

Parental Supports

Pupils could potentially have unsupervised internet or social media access at home or at other locations away from the school. All parents or carers should be aware of the concerns and benefits of internet and social media use. Parents and carers are invited to contact the school at any time for advice on safe use of the internet and social media. The school will also provide regular information for parents and carers, for example, through talks on internet safety, the safe use of the internet and social networking sites.

Usage Rules and Guidelines

Privacy

The school will access pupil and staff accounts and may review documents and log files in order to ensure that inappropriate use is not taking place. School equipment such as laptops, tablets or mobile phones may be checked from time to time and will be checked on return to ensure that it has been used appropriately.

Software

Pupils and staff must not download, load or install software, shareware or freeware, nor load any such software from USB pens or other memory storage devices without first consulting and obtaining permission from the Network Manager. All software installed must have an appropriate, current licence which must be provided to the Office Staff / Computing Curriculum Leader.

Sharing Files

Pupils and staff must not copy each other's work or intrude into each other's files without permission. Please be aware of compliance with copyright when copying or downloading any materials from the internet, portable media or memory storage devices.

Back up

The school network is backed up daily by the Office Staff / LA. However, pupils and staff are also encouraged to make back up files for their work and for work not held on the school network. Pupils and staff using personal portable devices such as tablets or mobile phones should ensure suitable backup solutions are implemented and maintained.

Purchasing Hardware and Software

The Network Manager must always be consulted before any hardware or software is purchased to ensure that it is compatible with the school network and GDPR compliant. Failure to do so may prevent this hardware or software from being installed on the network.

Cyber Security and Device Protection

The school network is protected against malicious attack or use by various systems such as anti-virus software and firewalls. It is the responsibility of pupils and staff to ensure that any personal computing equipment is also similarly protected against malicious attack or use. It is also preferable that any portable media such as USB pens or DVD's are also scanned for malicious software before they are used on schools equipment. Care should also be taken when opening emails or attachments; always first contact the IT Curriculum Leader / Office Staff before opening any suspicious or dubious email or attachment.

Inappropriate Materials or Language, Chat Rooms and Computer Games Abusive materials or language should not be used to communicate nor should such materials be accessed. A good rule is never to view, send or access materials, which you would not want governors, pupils, staff or parents to see. If encountered, such materials should be immediately reported in accordance with this policy. Live chat rooms must not be used unless posts are filtered prior to posting.

Pupils and staff should not access chat rooms from the school site unless such chat rooms have an educational purpose and, in the case of pupils, they have been specifically directed to do so by a teacher or other supervising adult.

It is not appropriate for staff and pupils to play computer or internet games during the school day unless they have an educational purpose or at social times and, in the case of pupils, they have been directed to do so by a teacher or other supervising adult.

All teachers and parents should ensure that video looping is turned off on YouTube, and when children are filming. Children need to know the dangers of filming on the internet at home.

Theft, Vandalism and Wilful Damage to Computing Facilities

Theft and vandalism deplete the school's resources and are detrimental to the learning of pupils. Pupils are expected to treat all computing facilities with respect. Staff should ensure that pupils are supervised when using computing facilities and that any incidents of theft or vandalism are challenged, recorded and dealt with in an appropriate manner. It is important that computing facilities remain secure at all times. Rooms and areas containing computing facilities, for example, must not be left unlocked and unsupervised during open days,

parents' evenings and other events when members of the public could be on site unsupervised.

Consequences for Misuse by Pupils

- Access to the wireless network will be removed.
- Device taken away for the period.
- Pupil is not allowed to use personal devices at school.
- Serious misuse of Internet capable devices is regarded as a serious offence and will be dealt with in accordance with this policy.

Pupil Monitoring

Monitoring of pupil activity will be undertaken routinely as part of the school Safeguarding procedures. The authorised personnel are:

- Headteacher / Designated Safeguarding Lead
- Deputy Designated Safeguarding Lead
- IT Technician
- Teachers
- Teaching assistants

Staff Monitoring

Monitoring of staff activity must be authorised by the Headteacher. Monitoring will be at the request of the Headteacher where there is reason to believe the individual has acted inappropriately or contrary to their contract of employment. Monitoring reports will be prepared by 'Future digital'. Reports will be classified **STRICTLY CONFIDENTIAL** and be submitted to the Headteacher.