Moor First E-Safety Policy and Acceptable Use Agreement.

May 2018
(Revised May 2019)
(Revised June 2020)
(Revised May 2022)

‘Together we unlock potential and learn for life!’

Access to IT facilities, the internet and social media must be in support of educational activities and appropriate to the aims of the school. The aims of this policy and agreements is to ensure that all pupils and staff are clear about what constitutes appropriate use of technology, the internet and social media, within the school and when using school IT resource and that all users are aware of the possible consequences of inappropriate use, which could include temporary or permanent loss of access to computing facilities, or even result in serious disciplinary action being taken. Misuse of technology from the age of ten upwards can result in legal prosecution and charges.

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.

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.

DATA SECURITY AND PRIVACY

All data is stored in accordance with provision of the General Data Protection Regulations. This references the use of the Cloud.

SAFETY, SOCIAL MEDIA PLATFORMS, 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 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 cyber-bullying, 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 Co-Headteachers. 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 online platforms called Tapestry **(Nursery and Reception)** and Seesaw (Year 1-Year 4) to record and store all observations and assessments relating to each child. These are safe and secure systems and enable 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, 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. Most recently, all staff completed an online safety course (22nd March 2021). During this session, staff were updated on the latest guidance that was published in 'Keeping Children Safe'. In addition, all staff were given a list of resources and websites they could access to assist them with their e-safety teaching.

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 Discipline / Anti Bullying.
• Safeguarding
• Pupil / Staff Acceptable Use Agreements
•Teacher Professional Standards
• GDPR Policy
. Code of Conduct for Staff
. Staff Handbook

PARENTAL SUPPORT

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.

School liability statement removed

PUPIL MONITORING

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

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

STAFF MONITORING

Monitoring of staff activity must be authorised by the Co-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 Co-Headteacher or Office Support Manager.

Co-Headteacher 1 name: Signed: Date:
Co-Headteacher 2 name:
Chair of governor’s name: Signed: Date:

MOOR FIRST SCHOOL
COMPUTING ACCEPTABLE USE POLICY – STAFF

‘Together we unlock potential and learn for life’

As a member of staff at Moor First School, I agree to use computing facilities, social media and the internet responsibly. I agree to follow the rules set out below when using the schools computing facilities:

I will keep my login, email address and password confidential. I will take care to ensure that others cannot use my accounts to access confidential information about pupils or staff by always logging off when I have finished work or locking my computer when it is left unattended.
I will not use anyone else’s login, email address or password.
I will ensure laptops and desktops must be password protected and never left unattended while logged in.
I will never allow SIMs to be accessed/viewed by pupils or visitors
I will not use any personal social media accounts for school business.
I will register with the school’s Office Support Manager / Head Teacher any social media accounts specifically created for school business.
I will ensure I will only post via schools social media using a professional tone and appropriate content.
I will not access anyone else’s work on the school network without their permission.
I will not download or install software, shareware or freeware on the school’s network directly or via portable devices without consulting the Co-Headteachers.
I will not violate copyright laws or licensing agreements.
I will screen all USB pens, digital media and portable devices for malicious software before I download any files on to the network and take care when opening unknown email attachments. I will seek advice from the IT Curriculum Leader / Office Staff if I am unsure about the safety of any such devices or attachments.
I will not attach any device to the network which may contain files which breach copyright, data protection or other laws.
I agree not to bring in computing hardware from outside of the school and use this hardware on the school network without appropriate authorisation from the Co-Heads.
I agree to use the schools computing facilities, social media and internet only for work related use.
I will not send photographs of pupils as email attachments or post photographs of pupils on websites unless I have permission to do this from pupils, parents or carers and the permission of the School’s Leadership Team.
I will not search, view, send or display offensive content such as pornography, extremism or radicalisation material.
I will not use the school’s computing facilities for personal financial gain, gambling, political purposes, advertising, or cause damage to the school’s reputation.
I will only access social networking sites to enhance the teaching and learning experience for pupils.
I will not befriend pupils or their parents on social media unless they are related to me or personal friends.
I will not send offensive, threatening or time-wasting messages nor post inappropriate images on websites. All emails sent will be of a professional nature and appropriate to its audience.
I will take care when giving out personal information, for example, to pupils and parents.
I will not open emails that contain no subject content, are chain mail or have been sent by an unknown sender.

I will notify the Co-Headteahcers if I encounter materials or messages that are inappropriate to the work of the school or if I suspect someone else of misusing computing facilities, social media or the internet.
I understand that I must inform the Headteacher immediately if I suspect another member of the school of serious or illegal misuse of computing facilities, social media or the internet. I will inform the Chair of Governors if that person is the Headteacher.
I understand that I must also inform the Designated Child Protection Officer if this misuse may be a safeguarding, child protection or a Prevent issue.
I will ensure that all pupils under my supervision use computing facilities, social media and the internet appropriately to support learning. I will challenge and report any misuse.
I will ensure that I follow relevant Health and Safety regulations when using computing facilities such as not looking in to the light beam from a projector and not leaving pupils unsupervised around projectors.
I understand I am responsible for the use and care of any personal device allocated to me whilst a member of staff.
I understand that I am responsible for the safekeeping of any computing equipment which I use, including such equipment which I may take off site.
I understand that the school may check files and monitor the internet sites used by staff.
I understand that I must ensure that I 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.
I understand that the school email system is not to be used for personal communication or sharing of information. This includes any non-school activities and events.
I understand that I must not do anything which may bring the school into disrepute for example posting comments and/or inappropriate images on social media and website that do not align with the ethos of the school.
I understand that I must not malign the school, pupils, staff, parents, nor stakeholders on social media.
I understand that serious misuse of computing facilities, social media and the internet could result in disciplinary action being taken against me.
I must inform the DPO if I suspect a breach of data protection within 24 hours; including damage/loss of school laptops, USBs and iPads/tablets.
I must remove images from school devices on a regular basis.
I must follow the procedures as stated in ‘A Mobile Phone and Camera Toolkit for Early Years Settings’ when using my own personal device.
Staff must use parental permission data when using online learning platforms.
I understand that I am able to access our learning platform from my own device but must not download any pictures to this device.

I have read and understood the above statements and I agree to comply with the Schools rules for use of computing facilities, social media and the internet. I understand that failure to do this could result in disciplinary action being taken against me.

Staff signature: ______________________________ **Date:** ____________

Staff Name: _________________________________

MOOR FIRST SCHOOL
COMPUTING ACCEPTABLE USE POLICY – Pupils

‘Together we unlock potential and learn for life’

In school, your child will use computing as part of their learning and sometimes as a reward in golden time. In line with the GDPR Policy, all schools are requested to share with parents a list of rules that schools will be teaching children in order to keep themselves and others safe (when using technology.)

Your child will be taught these in classes and assemblies using child friendly language. Posters will be placed around school and specific lessons will be taught regarding E-Safety. It is understandable that many of these rules are only relevant if age appropriate, however it is extremely useful for parents of children in KS1/KS2 to read some of these with their child as it may also help them to stay safe when using technology at home.

I will only use my own login, email address and password, which I will not share and I will sign out of programmes.
I will not access anyone else’s work on the schools network without their permission.
I will not eat or drink near computer equipment.
I will not download or install software, shareware or freeware on the schools network either directly or via portable devices.
I will not violate copyright laws or licensing agreements.
I will not pass off work downloaded from the internet as my own. I will give clear references to sources where I have downloaded someone else’s work.
I will not take photographs, video or audio of staff or other pupils without their permission.
I will not share or post images or audio of staff or pupils without their permission.
I will not use software, devices or mobile hot spots that get round the schools internet safeguards.
I will
I will not bring in disks, USB pens or other portable devices without permission. I will ensure that staff screen all such devices for malicious software before I connect or load any files on to the school network.
I will not attach any device to the school network which may contain files which breach copyright, data protection or other laws.
I agree not to bring in computing hardware from outside of the school and use this hardware on the school network.
I will not play computer games or access social networking sites during lessons
I will not search, view, send or display offensive, threatening or time-wasting materials or post inappropriate images on websites.
I will only print copies of my work when it is necessary. I will reduce my printing by selecting pages. I will only print in colour when this is essential. I understand that the school will monitor any printing that I do and may take action if this is excessive.
I will not use chat rooms during the school day or access social networking websites without permission.
I will not use the schools computing facilities for personal financial gain, gambling, political purposes, advertising or cause damage to the school’s reputation.
I will not access my personal ‘home’ email account during lessons unless given direct permission to do so in association with a task.
I will not give out personal information such as full name, home address, telephone numbers or personal email to anyone whose identity I cannot be certain of over the internet.
I will not arrange to meet anyone I have met over the internet.
I will notify an adult immediately if I encounter materials or messages that make me feel uncomfortable

I will notify an adult immediately if I suspect someone else of misusing computing facilities, social media or the internet.
I will respect schools resources and not damage or steal computing facilities.
I understand that the school will check files and monitor the internet sites used by pupils.
I understand that sanctions will be used if I misuse computing facilities, social media or the internet.

As the parent or legal guardian of the pupil above, I grant permission for them to use electronic mail, social media and the Internet. I will help to teach my child to stay safe when using technology, following some of these expectations above that are relevant.

Pupil Name:

Parent/Carer signature: ____

Parent/Carer Name (printed): ____

Date: _____________

MOOR FIRST SCHOOL
COMPUTING ACCEPTABLE USE POLICY – GOVERNORS

‘Together we unlock potential and learn for life’

As a Governor at Moor First School, I agree to use computing facilities, social media and the internet responsibly. I agree to follow the rules set out below when using the schools computing facilities:

I will keep my login, email address and password confidential. I will take care to ensure that others cannot use my accounts to access confidential information about pupils or staff by always logging off when I have finished work or locking my computer when it is left unattended.
I will not use anyone else’s login, email address or password.
I will ensure laptops and desktops must be password protected and never left unattended while logged in.
I will not use any personal social media accounts for school business.
I will ensure I will only post via schools social media using a professional tone and appropriate content.
I will not download or install software, shareware or freeware on the school’s network directly or via portable devices without consulting the Co-Heads.
I will not violate copyright laws or licensing agreements.
I will screen all USB pens, digital media and portable devices for malicious software before I download any files on to the network and take care when opening unknown email attachments. I will seek advice from the IT Curriculum Leader / Office Staff if I am unsure about the safety of any such devices or attachments.
I will not attach any device to the network which may contain files which breach copyright, data protection or other laws.
I agree not to bring in computing hardware from outside of the school and use this hardware on the school network without appropriate authorisation from the Co-Heads.
I agree to use the schools computing facilities, social media and internet only for work related use.
I will not send photographs of pupils as email attachments or post photographs of pupils on websites unless I have permission to do this from pupils’ parents or carers and the permission of the Schools Leadership Team.
I will not search, view, send or display offensive content such as pornography, extremism or radicalisation material.
I will not use the schools computing facilities for personal financial gain, gambling, political purposes, advertising, or cause damage to the school’s reputation.
I will only access social networking sites to enhance the teaching and learning experience for pupils.
I will not befriend pupils or their parents on social media unless they are related to me or personal friends.
I will not send offensive, threatening or time-wasting messages nor post inappropriate images on websites. All emails sent will be of a professional nature and appropriate to its audience.
I will take care when giving out personal information, for example, to pupils and parents.
I will notify my Co-Headteachers if I encounter materials or messages that are inappropriate to the work of the school or if I suspect someone else of misusing computing facilities, social media or the internet.
I understand that I must inform the Head Teacher immediately if I suspect another member of the school of serious or illegal misuse of computing facilities, social media or the internet. I will inform the Chair of Governors if that person is the Head Teacher.

I understand that I must also inform the Designated Child Protection Officer if this misuse may be a safeguarding, child protection or a Prevent issue.
I will ensure that all pupils under my supervision use computing facilities, social media and the internet appropriately to support learning. I will challenge and report any misuse.
I will ensure that I follow relevant Health and Safety regulations when using computing facilities such as not looking in to the light beam from a projector and not leaving pupils unsupervised around projectors.
I understand I am responsible for the use and care of any personal device allocated to me whilst a governor.
I understand that I am responsible for the safekeeping of any computing equipment which I use, including such equipment which I may take off site.
I understand that the school may check files and monitor the internet sites used by staff.
I understand that I must ensure that I 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.
I understand that the school email system is not to be used for personal communication or sharing of information. This includes any non-school activities and events.
I understand that I must not do anything which may bring the school into disrepute for example posting comments and/or inappropriate images on social media and website that do not align with the ethos of the school.
I understand that I must not malign the school, pupils, staff, parents, nor stakeholders on social media.
I must inform the DPO if I suspect a breach of data protection within 24 hours including damage / loss of school laptops, USBs and iPads.
I must remove images from school devices on a regular basis.
I must follow the procedures as stated in ‘A Mobile Phone and Camera Toolkit for Early Years Settings’ (part of the Safeguarding Policy) when using my own personal device.
I understand that serious misuse of computing facilities, social media and the internet could result in disciplinary action being taken against me.

I have read and understood the above statements and I agree to comply with the School’s rules for use of computing facilities, social media and the internet. I understand that failure to do this could result in disciplinary action being taken against me.

Governor’s signature: ______________________________ **Date:** ____________

Governor’s name: _________________________________

MOOR FIRST SCHOOL
COMPUTING ACCEPTABLE USE POLICY – VOLUNTEERS

‘Together we unlock potential and learn for life’

As a volunteer at Moor First School, I agree to use computing facilities, social media and the internet responsibly. I agree to follow the rules set out below when using the schools computing facilities:

I will keep my login, email address and password confidential.
I will take care to ensure that others cannot use my accounts to access confidential information about pupils or staff by always logging off when I have finished work or locking my computer when it is left unattended.
I will not use anyone else’s login, email address or password.
I will ensure laptops and desktops must be password protected and never left unattended while logged in.
I will not use any personal social media accounts for school business.
I will ensure I will only post via schools social media using a professional tone and appropriate content.
I will not download or install software, shareware or freeware on the school’s network directly or via portable devices without consulting the class teacher.
I will not violate copyright laws or licensing agreements.
I will screen all USB pens, digital media and portable devices for malicious software before I download any files on to the network and take care when opening unknown email attachments. I will seek advice from the class teacher if I am unsure about the safety of any such devices or attachments.
I will not attach any device to the network which may contain files which breach copyright, data protection or other laws.
I agree not to bring in computing hardware from outside of the school and use this hardware on the school network without appropriate authorisation from the class teacher.
I agree to use the schools computing facilities, social media and internet only for work related use.
I will not send photographs of pupils as email attachments or post photographs of pupils on websites unless I have permission to do this from pupils’ parents or carers and the permission of the School’s Leadership Team.
I will not search, view, send or display offensive content such as pornography, extremism or radicalisation material.
I will not use the schools computing facilities for personal financial gain, gambling, political purposes, advertising, or cause damage to the school’s reputation.
I will only access social networking sites to enhance the teaching and learning experience for pupils.
I will not befriend pupils or their parents on social media unless they are related to me or personal friends.
I will not send offensive, threatening or time-wasting messages nor post inappropriate images on websites. All emails sent will be of a professional nature and appropriate to its audience.
I will take care when giving out personal information, for example, to pupils and parents.
I will notify the class teacher if I encounter materials or messages that are inappropriate to the work of the school or if I suspect someone else of misusing computing facilities, social media or the internet.
I understand that I must inform the Headteacher immediately if I suspect another member of the school of serious or illegal misuse of computing facilities, social media or the internet. I will inform the Chair of Governors if that person is the Headteacher.
I understand that I must also inform the Designated Child Protection Officer if this misuse may be a safeguarding/child protection or Prevent issue.

I will ensure that all pupils under my supervision use computing facilities, social media and the internet appropriately to support learning. I will challenge and report any misuse.
I will ensure that I follow relevant Health and Safety regulations when using computing facilities such as not looking in to the light beam from a projector and not leaving pupils unsupervised around projectors.
I understand that I am responsible for the safekeeping of any computing equipment which I use, including such equipment which I may take off site.
I understand that the school may check files and monitor the internet sites used by staff.
I understand that I must ensure that I 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.
I understand that the school email system is not to be used for personal communication or sharing of information. This includes any non-school activities and events.
I understand that I must not do anything which may bring the school into disrepute for example posting comments and/or inappropriate images on social media and website that do not align with the ethos of the school.
I understand that I must not malign the school, pupils, staff, parents, nor stakeholders on social media.
I understand that serious misuse of computing facilities, social media and the internet could result in disciplinary action being taken against me.
I must inform the DPO if I suspect a breach of data protection within 24 hours.
I must follow the procedures as stated in ‘A Mobile Phone and Camera Toolkit for Early Years Settings’ when using my own personal device.

I have read and understood the above statements and I agree to comply with the School’s rules for use of computing facilities, social media and the internet. I understand that failure to do this could result in disciplinary action being taken against me.

Volunteer signature: ______________________________ **Date:** ___________

Volunteer name: _________________________________