Online Safety Policy

Policy Leader	**Mr A Kellett**
Safeguarding Governor / Chair of Governors	**Mr S Whittaker**
Last Updated	**November 2024**
Approved by the Governing Body	**November 2024**
Date to Review	**Spring 2025 (at the latest)**

Moss Side Primary School

Online Safety Policy

Development / Monitoring / Review of this Policy

This Online Safety policy has been developed by the Computing / IT coordinator with the cooperation of:

- Headteacher
- SLT including Safeguarding Leads
- School staff
- Governors

Schedule for Development / Monitoring / Review

This Online Safety policy was approved by the Governing Body	October 2023
The implementation of this Online Safety policy will be monitored by the:	Computing coordinator & Senior Leadership Team
The Governing Body will receive regular reports on the implementation of the Online Safety Policy, which will include anonymous details of online safety incidents at regular intervals	Termly through safeguarding updates and headteacher report
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Spring 2025
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Local Authority Designated Officer (LADO): **01772 536694** https://www.lancashiresafeguarding.org.uk/ Concerns about a child should be reported on 0300 123 6720 or out of hours 0300 123 6722 (8pm - 8am)

The school will monitor the impact of the policy using:

- Logs of reported incidents (CPOMS)
- Monitoring logs of internet activity (including sites visited) / filtering

Moss Side Primary School

Online Safety Policy

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers and visitors who have access to and are users of school IT systems, both in and out of the school). The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place outside of the school but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Positive Behaviour Policy.
The school will deal with such incidents within this policy including our approach to anti-bullying and peer on peer abuse and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Computing / ICT coordinator alongside the DSLs.
The Headteacher and the Computing / ICT coordinator, a member of the Senior Leadership Team, are 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 the later section – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures.)

The Headteacher & Senior Leaders are responsible for ensuring that the Computing /ICT Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Senior Leadership Team will receive monitoring reports from the Computing / IT coordinator.

Online Safety Coordinator:

The member of staff with a day to day responsibility for Online Safety is the Computing / IT coordinator who:

- is a member of the Senior Leadership Team
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body (Children's Safeguarding Assurance Partnership)
- liaises with the school's technical support
- receives reports of online safety incidents and creates a log of incidents using CPOMS to inform future online safety developments
- reports to the Senior Leadership Team as necessary
- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the school's network and devices through password protection
- 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 network / internet is monitored in order that any misuse / attempted misuse can be reported for investigation / action / sanction

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 Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher or IT Coordinator for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in aspects of the curriculum
- pupils understand and follow the Online Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- 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, 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

Designated Safeguarding Leads

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 and / or peer on peer abuse

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- are taught to have 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

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website

Community Users

Community users who access school systems as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.
Online safety should be a focus in many areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing and PSHE
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be 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 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.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.
The school will therefore seek to provide information and awareness to parents and carers through:

- Links / reminders in the newsletter, twitter feed and/or Class Dojo
- The school's website
- Flyers e.g. timely advice from the Childrens' Safeguarding Assurance Partnership
- *Reference to the relevant web sites & publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers Vodafone's Digital Parenting publication*

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of online safety training will be made available to staff through CPD from the Online Safety Coordinator. This will be updated and reinforced annually. The next planned date is February 2025. There are regular informal opportunities to discuss this throughout the year.
- Some staff might identify online safety as a training need within the performance management process.
- The Online Safety Coordinator will receive updates through attendance at external training events from the local authority and / or Childrens' Safeguarding Assurance Partnership and by reviewing guidance documents and resources released by relevant organisations.
- This Online Safety Policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Online Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in technology / online safety / health and safety /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Our school technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems by the technician
- Servers, wireless systems and cabling will be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.

- All users will be provided with a username and secure password by the IT coordinator who will have access to a record of users and their usernames. Users are responsible for the security of their username and password. A class login is assigned to children in Reception class.
- Currently the school's stock of iPads does not require a login to access the device. Therefore, filter reports do not identify specific users if, for example, a child uses an inappropriate search term. To overcome this issue, ipads have been numbered and are assigned to 1 child per year group. Only 2 or 3 children in the school can use their assigned ipad making it easier to track users should an incident occur which is flagged up by the filtering and monitoring reports.
- Currently a search through browser histories could identify individual users. By January 2025, we will have static ip addresses for all ipads which will help to identify individual users flagged up by our filtering and monitoring reports, without the need for a manual check of devices.
- The master passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.
- **Internet access is filtered for all users**. Illegal content (child sexual abuse images) is filtered by the filtering provider (Lancashire CC Education Digital Services - Netsweeper) by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Requests for filtering changes can be made in discussion with the Computing / IT coordinator who will liaise with the school technician.
- Internet filtering ensures that users are safe from terrorist and extremist material when accessing the internet.
- The school provides differentiated user-level filtering allowing different filtering levels for different groups of users – staff and pupils.
- The Computing / IT coordinator occasionally monitors the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. The school uses Netsweeper filtering and monitoring software provided by the school's ISP (Lancashire CC Education Digital Services)
- Any actual / potential technical incident / security breach needs to be reported to the Computing / IT coordinator or other member of SLT in the first instance.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date Sophos antivirus software.

- Provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school system is granted through discussion with the headteacher / bursar or Computing / IT coordinator
- A safe usage and loan agreement is in place for all any school laptops loaned to pupils.
- An agreed policy is in place that forbids staff from downloading executable files and installing programs / apps on school devices – the technician and/or Computing coordinator should be consulted before any changes are made.
- USB ‘pen’ drives can be used within school and on school devices – but should not contain sensitive data. Sharepoint and OneDrive should be used to store files for access at school and remotely.

Mobile Technologies

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet. Personally owned devices should not be connected to the school internet / network. The only exception being members of the governing body who bring their own device. They will be required to have signed the acceptable use agreement.

Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's Online Safety education programme.

*Pupils should not bring mobile technologies into school unless there are extenuating circumstances. In these cases, they must be given to a member of staff immediately. It should be noted that school cannot be responsible for these devices.
Adults using personal mobile technologies should only use them in non-teaching spaces during teaching times unless there is prior permission from the headteacher.

- The school Acceptable Use Agreements for staff, pupils and visitors will give consideration to the use of mobile technologies

The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No*

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about

potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press. Permission is requested at least at the start of each department.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Parents are allowed to take photos at school events e.g. class assemblies but should not distribute these photos especially via social media. The school makes regular attempts to remind parents of this.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

Moss Side Primary School has a separate data protection policy.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school has considered the benefit of using these technologies for education as well as the risks and disadvantages. The table below details which is and isn't permissible at Moss Side Primary School:

Communication Technologies	Staff & other adults				Students/Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	✓						✓	
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on mobile phones/cameras				✓				✓
Use of other mobile devices e.g. tablets, gaming devices		✓					✓	
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails		✓						✓
Use of messaging apps		✓						✓
Use of social media		✓						✓
Use of blogs		✓					✓	

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected unless instantly removed
- device must be password protected.

- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.
- school cameras are exempt from these procedures although data should be removed from these devices as quickly as possible (all photos should be saved on the server or in a designated folder on Sharepoint). *All photos to be saved to Sharepoint by September 2024.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- will not transfer any school personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

When using communication technologies, the school considers the following as good practice:

- The official *school* email service may be regarded as safe and secure and is monitored. Staff should therefore use only the school email service to communicate with others when in school, or on school related activities.
- Multi-Factor Authentication (MFA) has been implemented on all school Office365 (including email) accounts (June23). This is to increase security and protect against hacking and cyber-attacks.
- Users must immediately report, to the headteacher / Computing IT coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to **(or delete)** any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, Dojo etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS1 and KS2. (On occasions, pupils at KS2 will be provided with individual school email addresses, temporarily and for educational use only.)

- Pupils will be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- *Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff. In reality, only limited accounts are made public (headteacher, bursar, SENDCo, family support worker)*

Social Media - Protecting Professional Identity

To be read in conjunction with Moss Side Primary School Policy on the use of social networking sites and other forms of social media.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made to pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise the risk of a loss of personal information

Official school social media accounts:

- (Twitter/X) Only used for retweeting information or a general news posts.

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. online bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

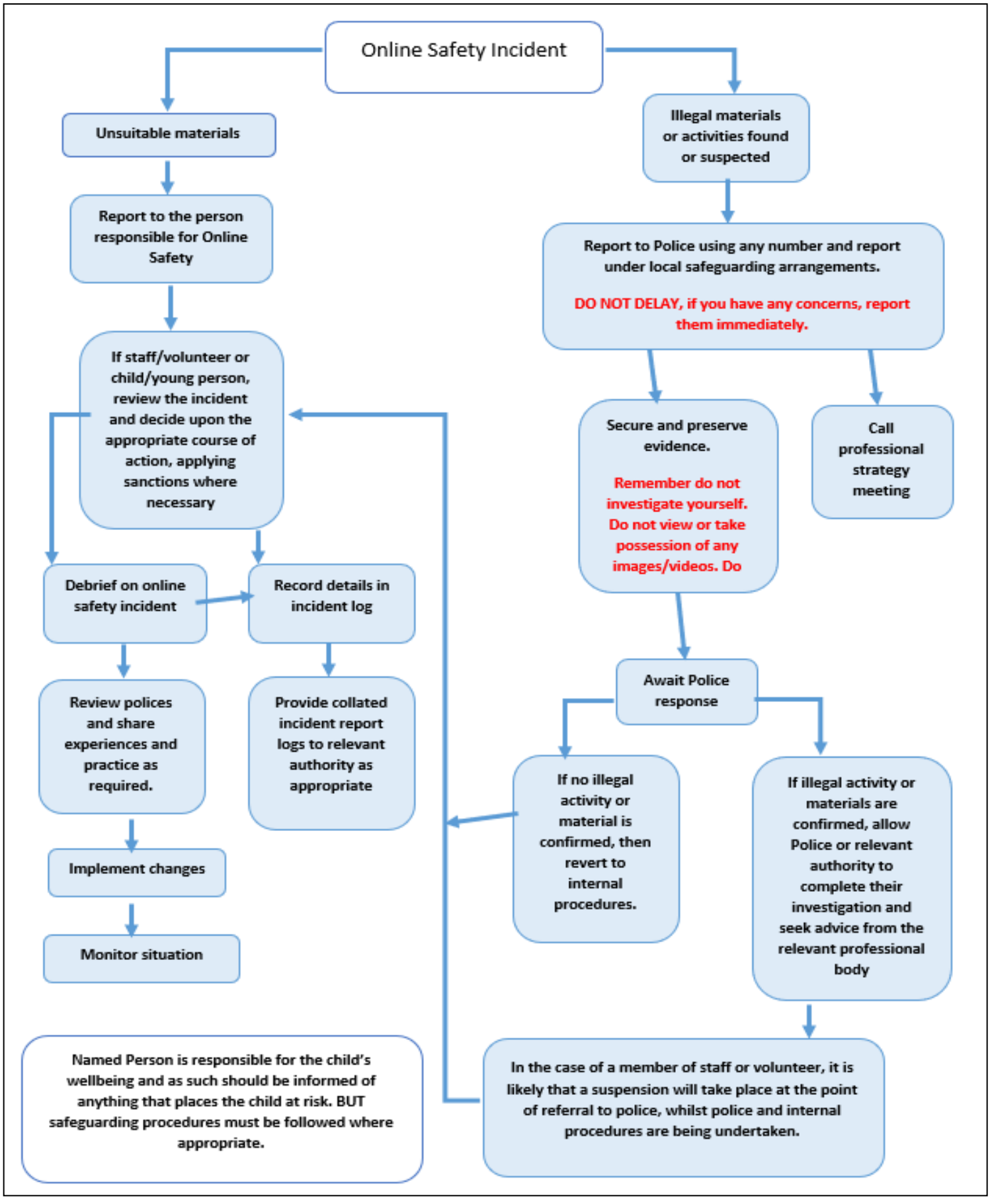
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					✓
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					✓
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					✓
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					✓
	Pornography				✓	
	Promotion of any kind of discrimination				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	Promotion of extremism or terrorism				✓	

	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing • equipment (without relevant permission)						✓
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					✓	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					✓	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					✓	
Using school systems to run a private business					✓	
Infringing copyright					✓	
On-line gaming (educational)			✓			
On-line gaming (non-educational)					✓	
On-line gambling					✓	
On-line shopping/commerce			✓			
File sharing					✓	
Use of social media				✓		
Use of messaging apps				✓		
Use of video broadcasting e.g. Youtube				✓		

Moss Side Primary School

Online Safety Policy

Responding to incidents of misuse



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national/local organisation (as relevant).
    - Police involvement and/or action
- **If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is

intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher	Refer to Computing / ICT Coordinator	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. suspension/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓		✓	✓		✓
Unauthorised use of non-educational sites during lessons	✓							✓	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	✓	✓	✓					✓	
Unauthorised/inappropriate use of social media/ messaging apps/personal email	✓	✓	✓			✓		✓	
Unauthorised downloading or uploading of files	✓	✓						✓	
Allowing others to access school network by sharing username and passwords	✓	✓	✓		✓			✓	
Attempting to access or accessing the school network, using another pupil's account	✓	✓	✓			✓			✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓			✓			✓

Corrupting or destroying the data of other users	✓	✓	✓			✓			✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓	✓		✓			✓
Continued infringements of the above, following previous warnings or sanctions		✓	✓						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		✓	✓			✓			✓
Using proxy sites or other means to subvert the school's filtering system		✓	✓		✓	✓	✓		✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓		✓	✓		✓	
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓	✓			✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓	✓	✓					

Actions/Sanctions

Staff Incidents	Refer to Computing / ICT Coordinator	Refer to Headteacher	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		✓	✓	✓			✓	✓
Inappropriate personal use of the internet/social media/personal email		✓				✓		
Unauthorised downloading or uploading of files	✓	✓				✓		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		✓				✓		
Careless use of personal data e.g. holding or transferring data in an insecure manner		✓			✓	✓		
Deliberate actions to breach data protection or network security rules		✓	✓				✓	✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓	✓				✓	✓
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		✓	✓			✓	✓	✓
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils		✓	✓	✓			✓	✓
Actions which could compromise the staff member's professional standing		✓				✓		
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy		✓				✓		

Using proxy sites or other means to subvert the school's/academy's filtering system		✓	✓				✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓		
Deliberately accessing or trying to access offensive or pornographic material		✓	✓	✓	✓		✓	✓
Breaching copyright or licensing regulations	✓	✓			✓	✓	✓	
Continued infringements of the above, following previous warnings or sanctions		✓	✓	✓	✓		✓	✓