Online Safety Policy

Moss Hey Primary School

Development/Monitoring/Review of this Policy

This online safety policy has been developed by our Senior Leadership Team and subject leaders made up of:

- Headteacher
- Deputy Head Teacher
- ICT lead
- PSHE lead
- Staff – including teachers, support staff, technical staff
- Governors/Board

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*Insert date*
The implementation of this online safety policy will be monitored by:	Headteacher: Mrs Messham Deputy Head: Mrs Malkin PSHE Lead: Miss Roberts ICT Lead: Mr Ramsey
Monitoring will take place at regular intervals:	Termly
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group at regular intervals:	Termly in the full Governing Body Meetings
The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	Autumn 2021
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*Insert names/titles of relevant persons/agencies e.g.: LA Safeguarding Officer, Academy Group Officials, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of

    - students/pupils
    - parents/carers
    - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school technology 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 online-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 school will deal with such incidents within this policy and associated behaviour and anti-bullying policies 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/Board of Directors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor within their Safeguarding role. The role of the Online Safety Governor will include:

- regular meetings with the Headteacher
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governors

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community.
- The Headteacher and Deputy Head Teacher are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- leads the Online Safety Group
- 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
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors

Network Manager/Technical staff

Moss Hey Primary School has a managed ICT service provided by an outside contractor; RPTechnic and they are fully aware of the schools' online safety policy and procedures.

Those with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis
- 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 networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders; for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to the Headteacher or Deputy Head Teacher in their absence for investigation/action/sanction
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills
- they monitor the use of digital technologies, 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 Lead

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

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

Online Safety Group

The Online Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding online safety and the monitoring the Online Safety Policy including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body

Members of the Online Safety Group will assist the Headteacher with:

- the production/review/monitoring of the school online safety policy/documents.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- consulting stakeholders – including parents/carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills
- 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 schools' 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 internet safety evenings, Moss Hey Messenger, letters, school website, social media 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/Learning Platform and on-line student/pupil records
- their children's personal devices in the school – children are not permitted to have their mobile phone / personal devices in school; if they require them they are to be signed in to the class teacher and then signed out at the end of the day

Community Users

Community Users who access school systems or programmes 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/digital literacy 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 is a focus in our PSHE curriculum and staff reinforce online safety messages across the curriculum. Our online safety curriculum is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- Our planned online safety curriculum is provided as part of Computing and PHSE lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of activities and circle times
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils to 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 to 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 are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet in small groups, staff to 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 online 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:

- Curriculum activities
- Letters, the messenger and our web site
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications

Education – The Wider Community

The school will provide opportunities for members of the community to gain from the school's online safety knowledge and experience. This may be offered through the following:

- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local schools

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:

- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at Local Authority termly safeguarding network meetings and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings/training sessions.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors/Directors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any 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
- Participation in school training/information sessions for staff or parents

Technical – infrastructure/equipment, filtering and monitoring

Our ICT service is managed by RPTechnic; our service provider carries out all the online safety measures. The school will work with RPtechnic to ensure that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. We will also ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

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
- Servers, wireless systems and cabling must 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. Users are responsible for the security of their username and password.
- The administrator" passwords for the school systems, used by the Network Manager must also be available to the Headteacher and kept in a secure place
- RPtechnic and Moss Hey Primary are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations: this is a joint role between RPtechnic, the ICT Coordinator and School Business manager, as some software is on a subscription basis, requiring annual payments to remain valid.

Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. The Broadband is protected by an approved UTM (Universal Threat Management device) provided by Fortigate (This meets the requirements stipulated for Educational use and is used by many Schools and Authorities in the UK and around the world) It uses the IWF CAIC list as well as other methods. Fortigate has been tested against (and meets) the UK Safer Internet Centre requirements for approval by the Department for Education. The device provides a Firewall, Virus checking, Application Filtering and Content Filtering. The device updates on a daily basis.

- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/pupils/students etc) The Fortigate does this, Staff / Pupils have different levels of filtering , also different devices may have different filtering levels depending on use.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement. We use: SECURUS Monitoring Software, Fortigate logs and server logs
- An appropriate system is in place. Users to report any actual/potential technical incident/security breach to the relevant person, as agreed. The Headteacher / ICT Coordinator will be informed
- 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. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software. The Antivrus software updates automatically as the manufacturer releases new definitions, this is generally daily. Sensible precautions are taken for devices, network equipment is generally in wall mounted data cabinets, mobile devices have locked storage cabinets. The suite is a secure room.
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems. RPtechnic create accounts for users when requested by the school, normally Office staff or ICT Coordinator
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. The system is locked down to a level that restricts most software being downloaded and installed by end users, this has to be a balance between usability and security.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. Teachers have remote access which reduces the need to use memory sticks. Any removable media that is used must be encrypted.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices are owned by the school and include: staff smartphone, tablets, and laptops that has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

- The school acceptable use agreements for staff, pupils and parents/carers will give consideration to the use of mobile technologies

School owned/provided devices:

- Will be allocated to all classes
- Where, when and how their use is allowed – in the computer suite, classrooms, designated work spaces. Classes / groups to be timetabled
- Access to networks/internet – this is filtered
- Management of devices/installation of apps/changing of settings/monitoring – Rptechnic use a MDM (Mobile Device Management) (currently Meraki but moving to Mosyle) solution to restrict the devices and install apps
- Network/broadband capacity QOS (quality of service) settings are applied to try and ensure all devices get a fair share of the network without impacting other users
- Technical support provided by RPtechnic
- Filtering of devices - Fortigate
- Access to cloud services - Fortigate application and URL filtering applied
- Data Protection – policies accessible on our website
- Taking/storage/use of images – only take photographs on school owned devices and stored securely on the school server
- Exit processes – what happens to devices/software/apps/stored data if user leaves the school. The school notifies RPtechnic of a person leaving whereby we will lock the for a period of time whilst it is decided what data needs to be kept.
- Liability for damage
- Staff training

Personal devices:

- Personal mobile devices in school are only to be used by staff and visitors under supervision
- Restrictions on where, when and how they may be used in school – personal phones only to be used in staff designated areas (staffroom / PPA room)

- Storage – staff to keep mobile devices in their lockers in the staffroom. Spare lockers for visitors
- Lead staff are allowed to use personal devices (phones) for school trips
- The right to take, examine and search users devices in the case of misuse (England only)
- Taking/storage/use of images is not permitted
- Liability for loss/damage or malfunction following access to the network (likely to be a disclaimer about school responsibility).
- How visitors will be informed about school requirements – access to policies, verbally told when entering the building
- Education about the safe and responsible use of mobile devices is included in the school online safety education programmes.

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 pupils are published on the school website/social media/local press
- 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.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school must ensure that:

- it has a Data Protection Policy
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice

- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- If a maintained school, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

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

- data must be encrypted and password protected.
- 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/academy policy (below) once it has been transferred or its use is complete.

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 understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any school/academy 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

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

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

- The official school email service is regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. *Personal email addresses, text messaging or social media must not be used for these communications.*
- All pupils are provided with individual school email addresses for educational use.
- Pupils should 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.

Social Media - Protecting Professional Identity

All schools, academies, MATs and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies, MATs and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority/MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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 in social media 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 or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there should be:

- A process for approval by senior leaders – only school administrator to have access – HT to approve before posting
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- 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. cyber-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,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding					X

data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	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					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
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)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes					X	

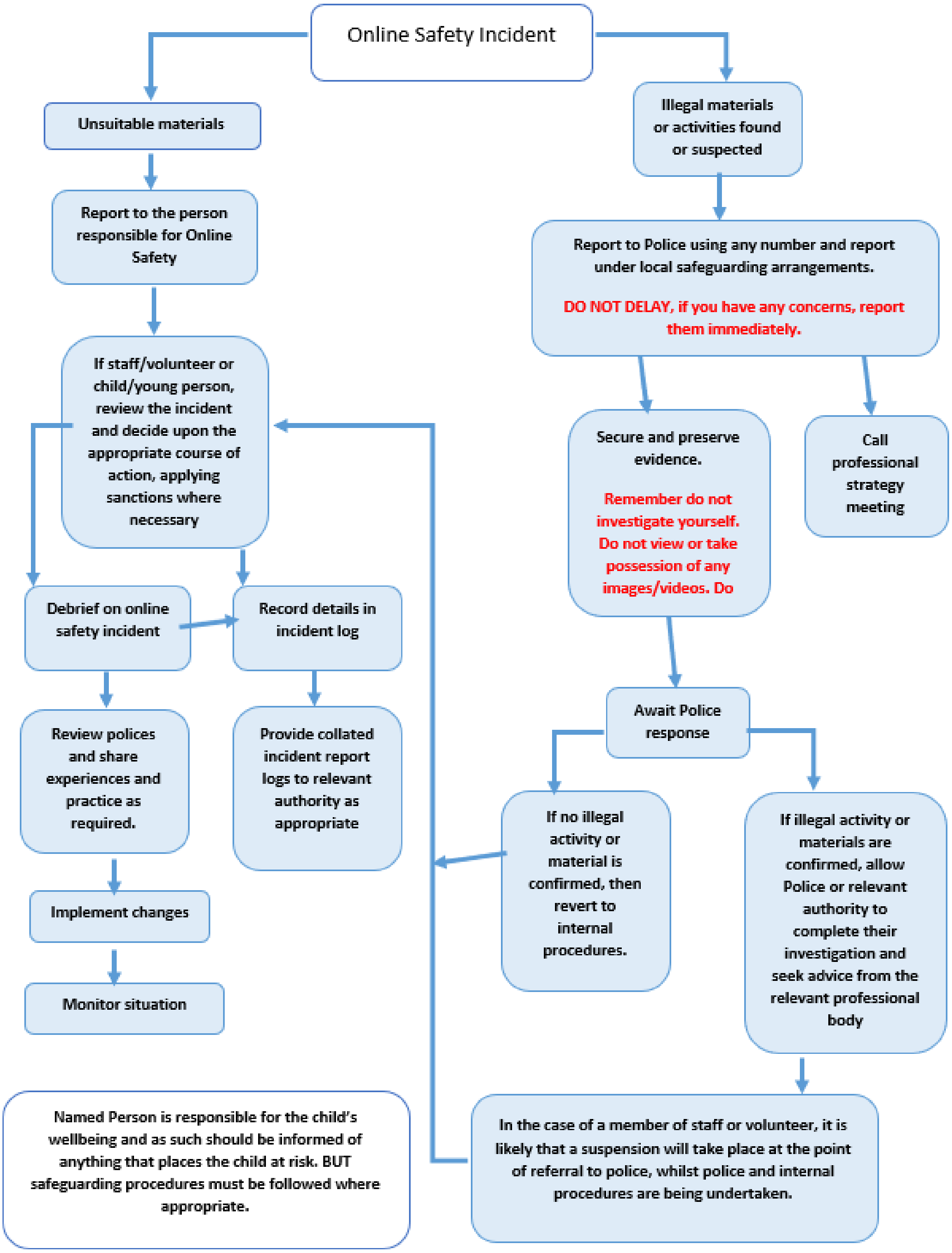
and passwords)					
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (non-educational)				X	
On-line gambling					X
On-line shopping/commerce	X				
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. Youtube			X		

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Online Safety Incident

Unsuitable materials

Report to the person responsible for Online Safety

If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary

Debrief on online safety incident

Record details in incident log

Review polices and share experiences and practice as required.

Provide collated incident report logs to relevant authority as appropriate

Implement changes

Monitor situation

Illegal materials or activities found or suspected

Report to Police using any number and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Secure and preserve evidence.

Remember do not investigate yourself. Do not view or take possession of any images/videos. Do

Call professional strategy meeting

Await Police response

If no illegal activity or material is confirmed, then revert to internal procedures.

If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body

In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.

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:

Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Headteacher/Principal	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. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X		X			
Unauthorised use of non-educational sites during lessons	X				X		X	
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device	X	X			X			

Unauthorised/inappropriate use of social media/ messaging apps/personal email	X	X			X		X	
Unauthorised downloading or uploading of files								
Allowing others to access school/academy network by sharing username and passwords	X	X		X	X			
Attempting to access or accessing the school/academy network, using another student's/pupil's account	X	X		X	X			
Attempting to access or accessing the school/academy network, using the account of a member of staff	X	X		X	X	X		
Corrupting or destroying the data of other users	X	X		X	X	X		
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X			X		X	
Continued infringements of the above, following previous warnings or sanctions	X	X		X	X	X		
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	X	X		X	X		X	
Using proxy sites or other means to subvert the school's/academy's filtering system	X	X		X	X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X			X		X	
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X		

Moss Hey Primary School

Acceptable Use of Technology

e-Safety Rules to keep our children safe

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address (KS1) or my own school e-mail address when e-mailing (KS2).
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will report any unpleasant material or messages sent to me to my teacher
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will not use any social media sites in school.
- I will ask permission before using the internet
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell will close it down immediately and tell my teacher.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behavior when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent will be contacted if a member of school staff is concerned about my use of technology.

We have discussed the e-Safety rules, and my child …………………………… understands them, supporting the safe use of ICT at Moss Hey Primary School.

Parent Signature ………………………………………………………….

Class …………………………………. Date ………………………………