Moorside Community Primary Academy.

Back Lane,
Skelmersdale.
WN8-9EA.

Online Safety Policy

At Moorside Academy our primary aim as educators is to ensure that our pupils are safe, happy and ready to learn. The ethos of our school is that the foundations are built firmly on peace and respect, regardless of an individual's role in the academy. Our children and their families are at the heart of everything that we do here at Moorside and our curriculum has been developed in partnership with our children to be stimulating and engaging and to promote a lifelong love of learning. Our nurturing approach ensures that our curriculum is fully inclusive for all learners and we work hard to challenge all of our children and develop in them the resilience that will accompany them on their future learning journey.

This online safety policy has been developed by the following staff:

- Head Teacher/Online Safety Lead/Designated Safeguarding Lead – Richard Davis
- Computing Coordinator – Laura Mills
- Backup DSLs – Olive McSorley, Anna Jameson, Kate Aspden
- Reviewed by the Board of Governors

Schedule for Monitoring

Online Safety Policy was approved by the Board of Governors:	Date
The implementation of the policy will be monitored by:	Natalie Dutton(Computing Coordinator) Richard Davis (Head Teacher/DSL)
The Board of Governors will receive a review about the implementation of the Online Safety Policy on (including effectiveness of filtering, monitoring and management of online safety incidents):	Date
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:	Date
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Lancashire Safeguarding Officer Police

The school will monitor the effectiveness 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 pupils and staff

1: Who is this policy for?

This policy applies to all members of the school community (including staff, pupils, volunteers, parents, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Head teachers 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 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 Behaviour Policy. The school/academy 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.

2: Roles and Responsibilities

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

Governors –

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 necessary information about online safety incidents and monitoring reports. A member of the Governing Board has taken on the role of Online Safety Governor (Safeguarding Governor).

The role of the Online Safety Governor will include:

- Regular meetings with the Head Teacher and DSLs.
- Regular monitoring of online safety incident logs.
- Regular monitoring of filtering logs.
- Reporting to relevant Governors meeting.

Head Teacher 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 Online Safety Lead.

The Headteacher and Senior leaders should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See Appendix: Flow chart on dealing with online safety incidents).

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead –

- 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/MAT/relevant body.
- 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.
- Reports regularly to Senior Leadership Team.

Network Manager -

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 of the Local Authority's online safety guidance.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Head teacher and Online Safety Lead for investigation.
- That monitoring software/systems are implemented and updated as agreed in school's 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.
- They report any suspected misuse or problem to the Headteacher/Online Safety Lead for investigation.
- 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 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 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 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.

Pupils -

- Are responsible for using the school's digital technology systems in accordance with the pupil acceptable use agreement. (Appendix 1)
- Need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school.

Parents and 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, 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 (Class Dojo).
- Their children's personal devices in the school (where this is allowed).

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.

3: Policy Statements

Education of 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 should be a focus in all 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited. (JIGSAW, Purple Mash Online Safety Curriculum).
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be 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 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education of parents and 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, newsletters, web site, Learning Platform (Class Dojo)
- High profile events e.g. Safer Internet Day.
- Reference to the relevant web sites/publications.
- Information which can be found on the 'Online Safety' page of the school website.

Education and Training of Staff and 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 planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly. (NSPCC Online Safety Training).
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and acceptable use agreements.
- 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 external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The Online Safety Lead will provide advice/guidance/training to individuals as required.
- All staff will attend annual safeguarding training which will include regular updates on changes to online safety policy.

Training of Governors –

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 or National Online Safety Platform.
- Participation in school training/information sessions for staff or parents.

Filtering of equipment and monitoring –

The school is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

It will also need to 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 pupil users (at KS2 and above) will be provided with a username and secure password by the Computing Coordinator (Laura Mills) who will keep an up to date record of users and their usernames. 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 or other nominated senior leader and kept in a secure place.
- **Virtue Technologies** (Network Managers) 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.
- 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.
- In line with the Internet Watch Foundation, the school internet service ensures that the users are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering. The filtering solution is based on the Sophos Security Gateway and provides a robust Internet filter with automated updates to inappropriate sites, including the IWF blocked sites list.
- 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.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person. Any incidents are to be reported to the Online Safety Lead/Headteacher who will take appropriate action.
- 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.

- 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. (See Appendix 2- Acceptable use of Technology)
- An agreed policy is in place that forbids staff from downloading executable files and installing programmes on school devices. (See Appendix 2- Acceptable use of Technology)
- 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. (See Appendix 2- Acceptable use of Technology)

Use of Mobile Devices -

Complete with reference to mobile devices policy

	School Devices			Personal Devices		
	School Owned for Single Use	School Owned for Multiple Users	Authorised Device	Pupil Owned	Staff Owned	Visitor Owned
Allowed in School	✓	✓	✓	✘	✘	✓*
Full Network Access	✓*	✓*	✓*	✘	✘	✘
Internet Access	✓*	✓*	✓*	✘	✘	✓**

*** - Pre-determined permissions apply according to Network Policy.**

**** - Authorised visitors only.**

Use of Digital Images and Videos -

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.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection –

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation. (See Data Protection Policy).

- 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.

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

- Data must be encrypted and password protected.
- Devices must be password protected.
- Devices 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 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 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 –

	Staff				Pupils			
Communication Technologies	Allowed	Allowed at certain Times (Staff room or designated break area)	Allowed by certain staff	Not allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permissions
Mobile phones may be brought to school		✓						✓
Use of mobile phones in lessons				✓	✓			
Use of mobile phones in social times (e.g. Staff room)	✓				✓			
Taking photos with personal mobile phones/cameras				✓	✓			
Use of other personal mobile devices (games consoles, tablets)				✓	✓			
Use of school email for personal use				✓				
Use of messaging apps		✓			✓			

Use of social media		✓			✓			

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. 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.
- Pupils at KS2 and above will be provided with individual school email addresses for educational use. (Provided through Purple Mash).
- 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, 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 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/academy 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.

Personal Use:

- Personal communications are those made via a 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 during designated break times, and must take place in a designated break area. (Staff room).

Dealing with unsuitable/inappropriate activities –

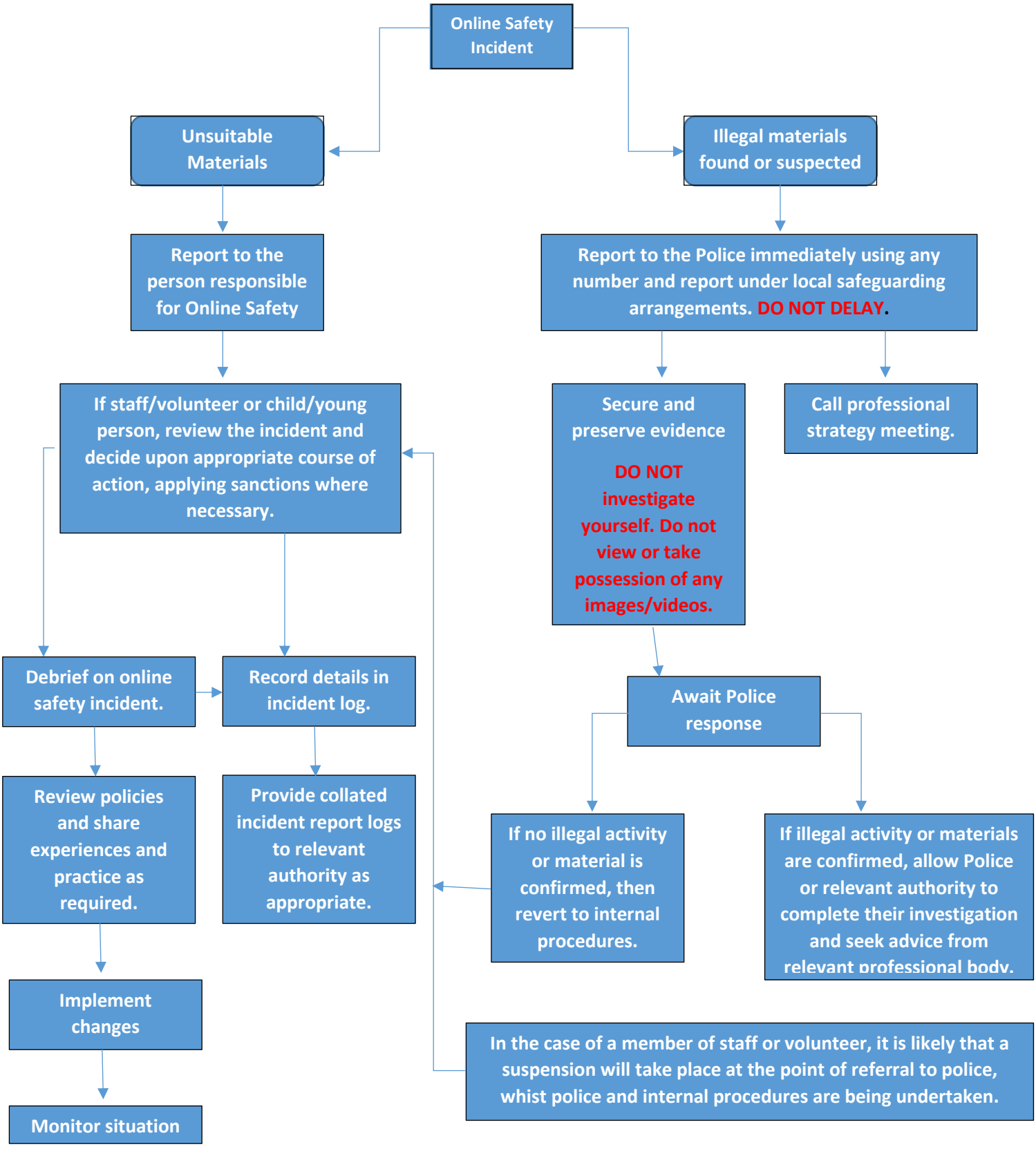
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Accepted 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.					X
	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	

User Actions	Acceptable	Acceptable at certain times	Accepted for nominated users	Unacceptable	Unacceptable and illegal
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.				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).				X	
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 gambling.				X	
On-line shopping/commerce.		X			
File sharing.		X			
Use of social media.		X			
Use of messaging apps.		X			
Use of video broadcasting e.g. Youtube.			X		
On-line gaming (non-educational).				X	

Responding to incidents of misuse –

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 for responding to online safety incidents and report immediately to the police.



Richard Davis 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.

School Actions and 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 and Sanctions						
Pupil Incidents	Refer to class teacher	Refer to head teacher	Refer to Police	Refer to technical support staff to adjust filtering/security	Inform parents/carers	Removal of internet/network access	Further sanctions at the discretion of the head teacher
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			
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		
Unauthorised downloading or uploading of files.	X			X			
Allowing others to access school/academy network by sharing username and passwords.	X						
Attempting to access or accessing the school/academy network, using another student's/pupil's account.	X						
Attempting to access or accessing the school/academy network, using the account of a member of staff.		X		X	X		X

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

	Actions and Sanctions						
Staff Incidents	Refer to line manager	Refer to head teacher	Refer to Police	Refer to technical support staff to adjust filtering/security	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).	X	X	X	X	X		
Inappropriate personal use of the internet/social media/personal email.	X						
Unauthorised downloading or uploading of files.	X						

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.	X	X		X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner.	X	X		X	X		
Deliberate actions to breach data protection or network security rules.	X	X					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software.	X	X		X			
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature.	X	X		X	X		
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils.	X	X	X	X	X	X	X
Actions which could compromise the staff member's professional standing.	X	X	X	X	X	X	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy.	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's/academy's filtering system.	X	X		X			
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X	X	X	X
Breaching copyright or licensing regulations.	X	X		X	X		
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X

Appendices

Appendix 1 –

Acceptable Use of Technology Policy – KS1/KS2 Pupils

To stay safe when we are using technology we must remember the following:

- I understand that for the safety of myself and others that the school will monitor my use of technology in school on computers and all other devices.
- I understand that school will contact my parents/carers if an adult at school is concerned about me or my use of technology.
- I will keep my username and passwords safe and secure. I will not share them with others.
- I will not use anyone else's username and password.
- When I am using a device I will only open the app or other software that my teacher has asked me to open.
- I will not open any links or attachments sent to my email account without checking with a trusted adult or teacher first.
- I will only use school devices when a teacher or trusted adult has given me permission to do so. I will make sure I am careful and I will look after all of the devices in my school.
- I will notify a teacher or trusted adult if I notice something on a device isn't working properly or is damaged in some way.
- If I feel upset or worried about anything I see on screen, then I **MUST** tell a teacher or trusted adult immediately.
- If I see anything that I know is inappropriate on screen, then I **MUST** tell a teacher or trusted adult immediately.
- When I communicate with others on email or any other messenger service, I will always be kind, careful, respectful, responsible and polite.
- I **will not** post or share personal information about myself or others online.
- I **will not** send or share anything online or in a message that I know could make others feel upset.
- I will be thoughtful about others feelings when I communicate online.
- I **will not** search or save anything that might make others feel upset.
- I must **NEVER** communicate with strangers online.

- I must **NEVER** meet with strangers that have contacted me online.
- If I receive a message online from someone that I don't know, I must tell a teacher or trusted adult immediately.
- I know that if I do not follow these rules, or in any way behave unkindly or inappropriately with technology in school, I may not be allowed to use school devices in the future and my parents/carers will be informed.

Please sign and date below:

Pupil's Signature: _____

Parent/Carer's Signature: _____

Date: _____

Appendix 2 –

Acceptable Use of Technology Policy – Staff and visitors

As a professional organisation with responsibility for safeguarding, all members of staff are expected to use Moorside CP Academy's IT systems in a professional, lawful, and ethical manner. To ensure that members of staff understand their professional responsibilities when using technology and provide appropriate curriculum opportunities for children/pupils/students, they are asked to read and sign this staff Acceptable Use of Technology Policy (AUP).

Our AUP is not intended to unduly limit the ways in which members of staff teach or use technology professionally, or indeed how they use the internet personally, however the AUP will help ensure that all staff understand Moorside CP Academy's expectations regarding safe and responsible technology use and can manage the potential risks posed. The AUP will also help to ensure that school systems are protected from any accidental or deliberate misuse which could put the safety and security of our systems or members of the community at risk.

Policy scope

1. I understand that this AUP applies to my use of technology systems and services provided to me or accessed as part of my role within school both professionally and personally. This may include use of laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies.

2. I understand that the Acceptable Use of Technology Policy (AUP) should be read and followed in line with the school child protection/online safety policy, staff behaviour policy/code of conduct and remote/online learning AUP.

3. I am aware that this AUP does not provide an exhaustive list; all staff should ensure that technology use is consistent with the school's ethos, school's staff behaviour and safeguarding policies, national and local education and child protection guidance, and the law.

Use of school/setting devices and systems

4. I will only use the equipment and internet services provided to me by the school for example school provided laptops, tablets, mobile phones, and internet access, when working with children/pupils/students.

5. I understand that any equipment and internet services provided by my workplace is intended for education purposes and/or professional use and should only be accessed by members of staff. Reasonable personal use of setting IT systems and/or devices by staff is allowed.

6. Where I deliver or support remote/online learning, I will comply with the school's remote learning Policy.

Data and system security

7. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or securing/locking access.

8. I will use a 'strong' password to access school systems. A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system. You will be asked to change your password regularly and are asked not to share your passwords with anyone.

9. I will protect the devices in my care from unapproved access or theft. Do not leave devices visible or unsupervised in public places.

10. I will respect school system security and will not disclose my password or security information to others.

11. I will not open any hyperlinks or attachments in emails unless they are from a known and trusted source. If I have any concerns about email content sent to me, I will report them to the IT system manager.

12. I will not attempt to install any personally purchased or downloaded software, including browser toolbars, or hardware without permission from the IT system manager.

13. I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school's information security policies.

14. All personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely.

15. Any data being removed from the school site, such as via email or on memory sticks or CDs, will be suitably protected. This may include data being encrypted by a method approved by the school/setting.

16. I will not keep documents which contain school related sensitive or personal information, including images, files, videos, and emails, on any personal devices, such as laptops, digital cameras, and mobile phones. Where possible, I will use the school learning platform to upload any work documents and files in a password protected environment or school approved/provided VPN.

17. I will not store any personal information on the school IT system, including school laptops or similar device issued to members of staff, that is unrelated to school activities, such as personal photographs, files or financial information.

18. I will ensure that school owned information systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

19. I will not attempt to bypass any filtering and/or security systems put in place by the school.

20. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the ICT lead (Virtue Technologies/Laura Mills/Richard Davis) as soon as possible.

21. If I have lost any school related documents or files, I will report this to the ICT Support Team (Virtue Technologies) and school Data Protection Officer (Jane Lee) as soon as possible.

22. Any images or videos of children/pupils/students will only be used as stated in the school camera and image use policy. I understand images of children/pupils/students must always be appropriate and should only be taken with school provided equipment and only be taken/published where children/pupils/students and/or parent/carers have given explicit written consent.

Classroom practice

23. I am aware of the expectations relating to safe technology use in the classroom, safe remote learning, and other working spaces as listed e.g. Safeguarding Policy and Data Protection Policy.

24. I have read and understood the school mobile and smart technology and social media policies.

25. I will promote online safety with the children/pupils/students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create by:

- Exploring online safety principles as part of an embedded and progressive curriculum and reinforcing safe behaviour whenever technology is used.

- Creating a safe environment where children/pupils/students feel comfortable to report concerns and say what they feel, without fear of getting into trouble and/or be judged for talking about something which happened to them online.
- Involving the Designated Safeguarding Lead (DSL) (Richard Davis) or a deputy (Anna Jameson, Rachel Russell) as part of planning online safety lessons or activities to ensure support is in place for any children/pupils/students who may be impacted by the content.
- Make informed decisions to ensure any online safety resources used with children/pupils/students is appropriate.

26. I will report any filtering breaches (such as access to illegal, inappropriate, or harmful material) to the DSL in line with the school/setting child protection/online safety policy.

27. I will respect copyright and intellectual property rights; I will obtain appropriate permission to use content, and if videos, images, text, or music are protected, I will not copy, share, or distribute or use them.

Mobile devices and smart technology

28. I will ensure that my use of mobile devices and smart technology is compatible with my professional role, does not interfere with my work duties and takes place in line with the staff behaviour policy/code of conduct and the school mobile technology policy and the law.

Online communication, including use of social media

29. I will ensure that my use of communication technology, including use of social media is compatible with my professional role, does not interfere with my work duties and takes place in line with the child protection/online safety policy, staff behaviour policy/code of conduct, social media policy and the law.

30. As outlined in the staff behaviour policy/code of conduct and school social media policy:

- I will take appropriate steps to protect myself and my reputation, and the reputation of the school, online when using communication technology, including the use of social media.
- I will not discuss or share data or information relating to children/pupils/students, staff, school business or parents/carers on social media.

31. My electronic communications with current and past children/pupils/students and parents/carers will be transparent and open to scrutiny and will only take place within clear and explicit professional boundaries.

- I will ensure that all electronic communications take place in a professional manner via school approved and/or provided communication channels and systems, such as a school/setting email address, user account or telephone number.
- I will not share any personal contact information or details with children/pupils/students, such as my personal email address or phone number.
- I will not add or accept friend requests or communications on personal social media with current or past children/pupils/students and/or their parents/carers.

- If I am approached online by a current or past children/pupils/students or parents/carers, I will not respond and will report the communication to my line manager and (Richard Davis) Designated Safeguarding Lead (DSL).
- Any pre-existing relationships or situations that compromise my ability to comply with the AUP or other relevant policies will be discussed with the DSL and/or headteacher.

Policy concerns

32. I will not upload, download, or access any materials which are illegal, such as child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act.

33. I will not attempt to access, create, transmit, display, publish or forward any material or content online that may be harmful, inappropriate or likely to harass, cause offence, inconvenience, or needless anxiety to any other person.

34. I will not engage in any online activities or behaviour that could compromise my professional responsibilities or bring the reputation of the school into disrepute.

35. I will report and record any concerns about the welfare, safety or behaviour of children/pupils/students or parents/carers online to the DSL in line with the school child protection policy.

36. I will report concerns about the welfare, safety, or behaviour of staff online to the headteacher, in line with school's child protection policy and/or the allegations against staff policy.

Policy Compliance and Breaches

37. If I have any queries or questions regarding safe and professional practise online, either in school or off site, I will raise them with the DSL and/or the headteacher.

38. I understand that the school may exercise its right to monitor the use of its information systems, including internet access and the interception of messages/emails on our systems, to monitor policy compliance and to ensure the safety of children/pupils/students and staff. This monitoring will be proportionate and will take place in accordance with data protection, privacy, and human rights legislation.

39. I understand that if the school believes that unauthorised and/or inappropriate use of school systems or devices is taking place, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

40. I understand that if the school believes that unprofessional or inappropriate online activity, including behaviour which could bring the school into disrepute, is taking place online, the school may invoke its disciplinary procedures as outlined in the staff behaviour policy/code of conduct.

41. I understand that if the school suspects criminal offences have occurred, the police will be informed.

I have read, understood and agreed to comply with Moorside CP Academy's Staff Acceptable Use of Technology Policy when using the internet and other associated technologies, both on and off site.

Name of staff member: ……

Signed: ……

Date (DDMMYY)……

Appendix 3 –

Digital images/video permission form

PARENTAL CONSENT FORM

Occasionally, we may take photographs of the children at our school. These images may be used in our school prospectus, in other printed publications that we produce, on our website, or on project display boards in school. Very occasionally, we may be visited by the media who will take photographs or film footage of pupils (eg at a high profile event, to celebrate a particular achievement etc.). Such images may appear in local or national newspapers, or on televised news programmes.

In order to comply with the Data Protection Act 1998, we need your permission before we can photograph or make any recordings of your child for promotional purposes. Equally we are committed to continue to work closely with parents in an attempt to take all reasonable steps towards making the school environment as safe as possible.

Please answer questions 1-4 below before returning the completed form (one for each child) to school as soon as possible.

1. May we use your child's photograph in the school prospectus and other printed publications that we produce for promotional purposes or on project display boards? Yes / No

2. May we use your child's image on our school website? Yes / No

3. May we record your child's image on video? Yes / No

4. Are you happy for your child to appear in the media as part of school's involvement in an event? Yes / No

have read and understand the conditions of use attached to this form.

Childs Name: _____

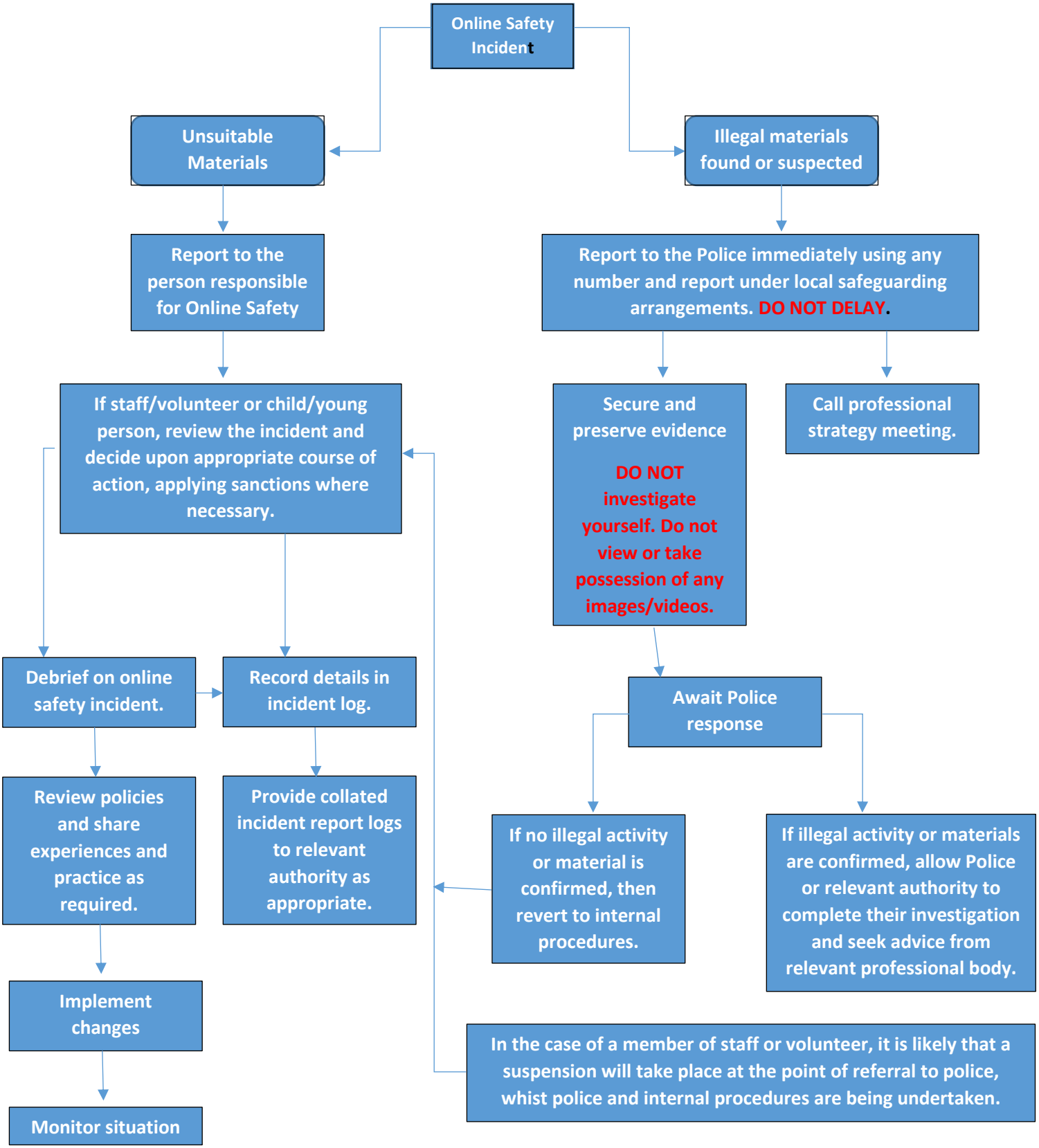
Parent's or Guardian's signature: _____

Name (block capitals) _____

Date: _____/_____/_____

Appendix 4 - Responding to incidents of misuse

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 for responding to online safety incidents and report immediately to the police.



Richard Davis 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.

Appendix 5 – Response to incidents of misuse record form

Date	Details of incident	Action Taken

Appendix 6 - Training needs audit log

Staff Name	Training need identified	Course attended/completed	Date

Appendix 7 - Social media policy

USE OF SOCIAL MEDIA POLICY

THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA (DEC 2018)

The Governing Body of Moorside C P Academy adopted this policy on 20th March 2019. The policy will be reviewed on an annual basis.

This Policy has been developed in consultation with the recognised Trade Unions and professional Associations.

1. **PURPOSE**

   This Policy sets out the school's position regarding the use of social networking sites and other forms of social media. The aim of the document is to ensure that all employees are fully aware of the risks associated with using such sites and their responsibilities with regards to the safeguarding and protection of both children and themselves.

2. **APPLICATION**

   This Policy applies to all staff employed in schools.

3. **BACKGROUND**

3.1 The use of social networking sites such as Facebook, Twitter, Pintrest, LinkedIn, What's App and MySpace have over recent years become the primary form of communication between friends and family. In addition, there are many other sites which allow people to publish their own pictures, text and videos such as YouTube, Instagram and Snapchat.

3.2 It would not be reasonable to expect or instruct employees not to use these sites which, if used with caution, should have no impact whatsoever on their role in school. Indeed, appropriate use of some sites may also have professional benefits. For example, many schools now use sites such as Facebook and Twitter as a means to enhance parental engagement.

3.3 It is now widely acknowledged that use of such sites does not provide a completely private platform for personal communications. Even when utilised sensibly and with caution employees are vulnerable to their personal details being exposed to a wider audience than they might otherwise have intended. One example of this is when photographs and comments are published by others without the employees consent or knowledge which may portray the employee in a manner which is not conducive to their role in school.

3.4 Difficulties arise when staff utilise these sites and they do not have the relevant knowledge or skills to ensure adequate security and privacy settings. In addition there are some cases when employees deliberately use these sites to communicate with and/or form inappropriate relationships with children and young people.

4. GUIDANCE AND ADVICE

4.1 Employees who choose to make use of social networking site/media should be advised as follows:-

(i) That they should not access these sites for personal use during working hours;

(ii) That they familiarise themselves with the site's 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;

(iii) That they do not conduct or portray themselves in a manner which may:-

- bring the school into disrepute;
- lead to valid parental complaints;
- be deemed as derogatory towards the school and/or it's employees;
- be deemed as derogatory towards pupils and/or parents and carers;
- bring into question their appropriateness to work with children and young people.

(iv) That they do not form on-line 'friendships' or enter into communication with *parents/carers and pupils as this could lead to professional relationships being compromised.

(v) On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18 years.

(vi) That they could face legal proceedings if comments they post about named individuals are found to have harmed their reputation.

*(*In some cases employees in schools/services are related to parents/carers and/or pupils or may have formed on-line friendships with them prior to them becoming parents/carers and/or pupils of the school/service. In these cases employees should be advised that the nature of such relationships has changed and that they need to be aware of the risks of continuing with this method of contact. They should be advised that such contact is contradictory to this Policy and as such they are potentially placing themselves at risk of formal action being taken under the school's Disciplinary Procedure*.)

4.2 Schools should not access social networking sites in order to 'vet' prospective employees. Such practice could potentially create an un-level playing field and lead to claims of discrimination if for example the selection panel were to discover a candidate held a protective characteristic as defined by the Equality Act.

5. SAFEGUARDING ISSUES

Communicating with both current and former pupils via social networking sites or via other non-school related mechanisms such as personal e-mails and text messaging can lead to employees being vulnerable to serious allegations concerning the safeguarding of children and young people.

The Department for Education document 'Guidance for Safer Working Practices for those Working with Children and Young people in Education Settings (October 2015) states:-

12. Communication with Pupils *(including the Use of Technology)*	
In order to make best use of the many educational and social benefits of new and emerging technologies, pupils need opportunities to use and explore the digital world. E-safety risks are posed more by behaviours and values than the technology itself. Staff should ensure that they establish safe and responsible online behaviours, working to local and national guidelines and acceptable use policies which detail how new and emerging technologies may be used. Communication with children both in the 'real' world and through web based and telecommunication interactions should take place within explicit professional boundaries. This includes the use of computers, tablets, phones, texts, e-mails, instant messages, social media such as Facebook and Twitter, chat-rooms, forums, blogs, websites, gaming sites, digital cameras, videos, web-cams and other hand held devices. (Given the ever changing world of technology it should be noted that this list gives examples only and is not exhaustive.) Staff should not request or respond to any personal information from children other than which may be necessary in their professional role. They should ensure that their communications are open and transparent and avoid any communication which could be interpreted as 'grooming behaviour' Staff should not give their personal contact details to children for example, e-mail address, home or mobile telephone numbers, details of web based identities. If children locate these by any other means and attempt to contact or correspond with the staff member, the adult should not respond and must report the matter to their manager. The child should be firmly and politely informed that this is not acceptable. Staff should, in any communication with children, also follow the guidance in section 7 'Standards of Behaviour'. Staff should adhere to their establishment's policies, including those with regard to communication with parents and carers and the information they share when using the internet.	*This means that adults should:* • *not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work* • not give out their personal details • *use only equipment and Internet services provided by the school or setting* • *follow their school / setting's Acceptable Use policy* • *ensure that their use of technologies could not bring their employer into disrepute*

6. RECOMMENDATIONS

(i) That this policy document is shared with all staff who come into contact with children and young people, that it is retained in Staff Handbooks and that it is specifically referred to when inducting new members of staff into your school/service.

(ii) That appropriate links are made to this document with your school/services Acceptable Use Policy

(iii) That employees are encouraged to consider any guidance issued by their professional association/trade union concerning the use of social networking sites

(iv) That employees are informed that disciplinary action may be taken in relation to those members of staff who conduct themselves in a way which is contrary to the advice and guidance outlined in this Policy. If such conduct is deemed to amount to gross misconduct this may lead to dismissal.

Appendix 8 - Links to support / websites

Think You Know

www.thinkuknow.co.uk

Get the inside information on staying safe while having fun online, with games and useful links. This Home Office sponsored site has separate areas for Age Groups 5-7, 8-10, 11-16, plus parents and teachers sections.

CEOP Safety Centre

www.ceop.police.uk/safety-centre

CEOP, the Child Exploitation and Online Protection Centre, part of UK policing, is dedicated to eradicating the sexual abuse of children. Their Internet Safety Centre offers advice, help and a chance to report suspicious online behaviour.

BBC Guide to Online Safety

www.bbc.co.uk/onlinesafety

This page aims to help you use the internet in a safe way. It links to sites that are kept up to date with useful information, along with explanations and helpful hints for you and your family to get the most out of the internet.

Get Safe Online

www.getsafeonline.org

This site, set up by the government and the IT industry, provides useful guides to staying safe online, protecting your PC, avoiding rip-offs and advice for both adults and children.

UK Safer Internet Centre

www.saferinternet.org.uk/advice-and-resources

For more information about internet safety, and safe and responsible use of the internet and new technologies, with guides for parents, teachers and children.

Google Family Safety Centre

www.google.co.uk/...familysafety

Tips and advice for keeping your family safe online.

Childnet International

www.childnet-int.org/

Childnet International is a non-profit organisation working with others to “help make the Internet a great and safe place for children”. This website gives news and background to Childnet’s work

Digizen

www.digizen.org

Digizen is concerned with building safe spaces and communities, understanding how to manage personal information, and about being internet savvy - using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do

Know IT All

www.childnet-int.org/kia

Know IT All is a multi award-winning site from Childnet, with a suite of education resources designed to help educate parents, teachers and young people about safe and positive use of the internet.
Currently there are four sections for Parents and Carers

KidRex – Kid Safe Search

www.kidrex.org

This is a child safe internet search with uses a combination of google safe search and its own filters to produce child related and family friendly results. There is a parent's help section where any problems can be reported.

Stay Safe Online

www.staysafeonline.org

Brought to you by the National Cyber Security Alliance, this site offers advice on safety in the home, in the classroom and in business. Includes teaching materials for schools.