Mere Green Primary School

Online Safety Policy

December 2016

Identified staff members mentioned in this policy:

Head Teacher = Anna Balson
Online Safety officer / ICT leader = Terri Coombs
Technical Support Team = Andrew Coveney

WHAT IS ONLINE SAFETY ?

Online Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The Online Safety Policy will operate in conjunction with other school policies including but not limited to: Safeguarding, Anti-Bullying, Data Protection Policy and our curriculum statement. This Online Safety policy will also operate alongside the child, parent, staff and visitor Acceptable Use Agreements.

Policy Statements

Education – pupils

The education of *pupils* in Online Safety is 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 education is also an integral part of the Computing Curriculum established at Mere Green.

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 at Mere Green is broad, relevant and provides progression, with opportunities for creative activities and will be provided in the following ways:

- A planned Online Safety curriculum (Digital Literacy) should be provided as part of Computing lessons and should be regularly revisited
- Key Online Safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities (Online Safety week / Safer internet Day)
- Students / 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.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- *Students / pupils should agree to sign the student / pupil Acceptable Use Agreement and be 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 students / 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 students / 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 (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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 – parents / carers

The school will seek to provide information and awareness to parents and carers through:

- *Curriculum activities*
- *Letters, newsletters, web site, Twitter, text*
- *Parents / Carers evenings / sessions*

- *High profile events / campaigns eg Safer Internet Day*
- *Reference to the relevant web sites / publications eg www.swgfl.org.uk*
  www.saferinternet.org.uk/   http://www.childnet.com/parents-and-carers

Education – The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's Online Safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and Online Safety*
- *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*
- *Supporting community groups eg Our Place, Early Years Settings, Childminders,*

Education & Training – Staff / Volunteers

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

- A planned programme of formal Online Safety training will be made available to staff and regular volunteers, delivered by the onsite CEOP Ambassador. This will be regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly.
- All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Agreements. Regular volunteers will sign an appropriate Acceptable Use Agreement.
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) 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 / team meetings / INSET days.
- The Online Safety Coordinator (or other nominated person) 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 sub committee / group involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

AUTHORISATION OF INTERNET ACCESS- PUPILS

- All staff will read and discuss the 'Acceptable Use Agreement' with their class in September (or when a new child joins) before using any school ICT resources and will remind pupils of the agreement whenever appropriate, agreements will be displayed in all classrooms and ICT areas
- The school will keep a written record of all staff and pupils who are granted Internet access. This record will be kept up-to-date, for example if a member of staff or pupil leaves.

- At Foundation level and Key Stage 1, access to Internet will be led by adult demonstration, directly supervised activities and approved online materials.
- Our pupil's will only use e-mail accounts under staff supervision.

AUTHORISATION OF INTERNET ACCESS- STAFF

- Staff at Mere Green are assigned their own personal e-mail account through the school OFFICE 365 email system for official correspondence. Staff are to respect each-other's privacy with regards to any other form of correspondence
- Staff may access personal e-mail accounts that are not provided by the school, but must agree to the "Acceptable Use Agreement" and be aware that the school has the right to monitor internet use via Policy Central and personal accounts
- Staff at Mere Green will NOT attempt to gain *unauthorised* access to any other computer system through or beyond the school authorised access account
- Staff at Mere Green will NOT access any other person's account or files as these actions are illegal, even if 'browsing'
- Staff at Mere Green will seek advice when wishing to download programs or files from the ICT Co-ordinator/Technician.
- Staff internet usage will be monitored using 'Policy Central' accessible only by the Technical support team.

SAFEGUARDING (see Safeguarding policy)

At Mere Green School we must decide on the right balance between controlling access, setting rules and educating pupils for responsible use. Undoubtedly, we will all come into contact with something inappropriate by the most innocent of searches or actions, this is something that is unavoidable and under such circumstances we encourage our students to report incidents with the confidence they will not be blamed, educating and encouraging them to deal with issues in a sensible and appropriate manner. The use of 'Hector' to cover anything that upsets children is taught continuously from Nursery to Yr6.

We do not believe blocking access is always the answer, our internet connection is heavily filtered externally and monitored with Policy Central Software, something that is not readily available in most homes, therefore we view the education of our pupils is paramount to keeping them safe in the real world. Together, education in Online Safety and providing an understanding of our Acceptable Use Policy (AUP) will help keep our students safe while using information technologies.

To ensure the safeguarding of all stakeholders it is our school policy that personal mobile phones are not used on site during the school day when children are present. (There are a small number of staff who have 'school' mobile phones who use these during the day for communication across the site and to enhance safeguarding / this also applies to staff while on off-site school trips) If children have access to a mobile phone they are required to hand it in at the school office before the start of the school day and collect it after the school day has finished. The internal school telephone system can be used to make and receive necessary phone calls. If staff wish to check their mobile phones during the working day they must do so during designated break times and away from children; where possible mobile phones should be used in staff only areas.

Staff are required to only use school owned devices (including school owned memory cards) to take photographs or videos, including digital cameras and iPads. If personal devices are used during an offsite school trip, it is the responsibility of each individual to remove images and other content from their personal devices asap on return to school.

Resources used by pupils in school are carefully chosen by the teacher and determined by curriculum policies. Use of the Internet, by its nature and speed of change, will provide access to information which has not been selected by the teacher. Whilst pupils will often be directed to sites and web pages which provide reviewed and evaluated sources, at times, they will be able to move beyond these, to sites unfamiliar to the teacher. It is also possible that a search term used one moment can bring up different results the next time it is used, due to the speed at which new information is introduced.

CYBER BULLYING (see anti-bullying policy)

Cyber bulling is particularly invasive and can be very difficult to eliminate. It can begin as a joke or a relatively innocent comment and can quickly escalate into a very destructive and upsetting means of targeting individuals. At Mere Green we have Acceptable use Agreements for both children and staff that outlines our approach to internet and mobile phone use (see Appendix 1 and 2). Cyber Bullying is taken very seriously and the Online Safety curriculum provides opportunities for pupils to discuss their use of the internet and some precautions they might take. Pupils know that if cyber bulling is taking place they should notify their teacher immediately. Incidents that occur outside of school but impact on school life should be reported to the Head or Assistant Head Teacher who will investigate. If necessary the school will

- Confiscate equipment such as mobile phones
- Withdraw access to the internet for a set amount of time
- Limit the use of the internet or only allowing it to be used under close supervision

INNAPROPRIATE MATERIAL

The children will be supervised at all times when accessing information from websites. The filtering service provided through **BGFL and Link2ICT** is very effective, but it may be possible for some content to escape filtering. In the event any content deemed unsuitable escapes filtering, the use of Hector the Protector Dolphin enables pupils to blank the computer screen and inform the supervising member of staff immediately. The Online Safety incident log forms should be completed and this should then be reported to the Online Safety Officer or ICT Co-ordinator to record and deal with the incident as deemed appropriate.

School monitoring software continuously works in the background of school devices, checking for misuse and inappropriate usage. Information is recorded of each incident at the time and is checked by the school Online Safety officer, we use this information in decisions of inappropriate use and resulting consequences, this also works effectively in helping us realise innocent or unintentional issues when they arise.

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

INFRASTRUCTURE

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems by the Technical support team
- 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 at KS2 and above will be provided with a username and secure password by Terri Coombs / Andrew Coveney *who will keep an up to date record of users and their usernames.*

- Users are responsible for the security of their username and password *and will be required to change their password every 100 days.*
- The "administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Headteacher on request* or other nominated senior leader and kept in a secure place this being the System Access File located on the Arthur Terry Server.
- *The Technical Support team* is 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 Service Birmingham using the MacAfee filtering system. There is a clear process in place to deal with requests for filtering changes *(requests are made through Link2ICT for any changes)*
- *An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person. Incident support logs are present in Key locations throughout school (ICT suite, KS1 iPad trolley, KS2 iPad trolley) for users to access, complete and return to the Online Safety officer or Head Teacher.*
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- An agreed policy is in place (Volunteer and Visitor Acceptable Use Policy) for the provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- *An agreed policy is in place* (Laptop and Ipad loan agreements) *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* (Laptop Loan Agreement) *that allows staff to / forbids staff from downloading executable files and installing programmes on school devices.*
- *An agreed policy is in place* (Acceptable Use Policy) *regarding the use of removable media (eg 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.*

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 students / 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 eg on social networking sites.**
- 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 *students / pupils* in the digital / video images**. Parents have agreed to his by signing the Parental Acceptable Use Policy.**

- *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. As described in the Acceptable Use Agreements that have been signed by all Staff and visitors.* **Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes unless as described in the above section SAFEFUARDING whilst on a school trip or with prior consent and reason by Headteacher.**
- *Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.*
- *Students / pupils must not take, use, share, publish or distribute images of others without their permission*
- *Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.*
- *Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.*
- *Written permission from parents or carers will be obtained before photographs of students / pupils are published. (* see Parents / Carers Acceptable Use Agreement / digital photo permission in the appendix)
  ALL staff will be aware of the children currently on the NO PHOTO PERMISSION list located in the staff room and ensure these children are not included in any published photographs.
- *Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

Data Protection (see data protection policy)

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school / academy must ensure that:

- It will hold 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.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It has clear and understood arrangements for the security, storage and transfer of personal data (Personal data should not be transferred with the exception of via our MUS system which has been designed for such purposes)
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear routines for the deletion and disposal of data
- There are clear policies (STAFF AUA) about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.
- Use personal data 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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (encrypted memory sticks have been provided for all teaching staff)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications -PUPIL EMAIL

It is recognised and encouraged by the government that e-mail should be used as an essential means of communication for staff and for pupils. All use of e-mail within Mere Green Primary School, is regulated and monitored. Pupils will therefore: -

- be supervised at all times when using the Internet
- use approved school e-mail accounts based upon the school system
- have access to individual school email account where deemed age appropriate
- use email in a polite and appropriate manner
- access to email account will be removed if use is deemed inappropriate
- inform the supervising teacher immediately if they receive anything deemed offensive via the Internet
- 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.

Use of none school email accounts for school correspondence or forwarding of school emails to none school email accounts, could be in breach of the Data Protection Act as these systems are not as secure as school email systems.

Communications -STAFF EMAIL/ TWITTER

- Staff at Mere Green are assigned their own personal e-mail account through the school Office 365 email system for official correspondence. Staff are to respect each-other's privacy with regards to any other form of correspondence
- Staff may access personal e-mail accounts that are not provided by the school, but must agree to the "Acceptable Use Agreement" and be aware that the school has the right to monitor internet use via Policy Central and personal accounts
- Users must immediately report, to the nominated person – in accordance with the school / academy 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 students / pupils or parents / carers (e.g email) must be professional in tone and content. *These communications may only take place on official (monitored) school / academy systems or accounts (school twitter). Personal email addresses, text messaging or social media must not be used for these communications.***

- Use of none school email accounts for school correspondence or forwarding of school emails to none school email accounts, could be in breach of the Data Protection Act as these systems are not as secure as school email systems.

- *Personal contact 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 (see Social Networking policy)

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the *school* 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 limiting access to personal information:

- Training to include: 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 when using personal accounts:

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

The *school's / academy's* use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

REPORTING

ALL Online Safety concerns, and valid use of Hector by a child, must first be reported to an adult who will then complete an Online Safety incident log report. These forms can be found in previously agreed locations next to key ICT equipment or in the main reception office. (ICT suite, iPad or Laptop trollies, Head teachers office). The incident log should then be taken to either Terri Coombs (Online Safety Ambassador) or Anna Balson (Headteacher / Child Protection Officer) who will follow guidelines given by Keeping Children Safe Online (NSPCC) to decide course of action. Any relevant incidents will be recorded using the online safeguarding system My Concern.

Unsuitable / inappropriate activities

Restrictions against Inappropriate language apply to public messages, private messages, and materials posted on web pages. When acting in an official capacity on behalf of the school, or using school e-mail accounts or social networking sites, the following points are to be noted: -

Staff and Students at Mere Green will <u>not</u>:-

- Use obscene, offensive, profane, lewd, vulgar, rude, threatening, or disrespectful language.

- Post information that could cause damage or danger of disruption
- Engage in personal attacks, including prejudicial or discriminatory attacks.
- Harass another person. Harassment is persistently acting in a manner that distresses or annoys another person.
- Knowingly or recklessly post false or defamatory information about a person or organisation.
- Re-post a message that was sent to privately
- Post private information about another person
- Knowingly breach copyright regulations

To maintain personal safety pupils at Mere Green will <u>not</u>

- Post personal contact information about themselves or other people. Personal information includes address and telephone number etc.
- Pupils must ask permission before accessing the Internet and have a clear idea why they are using it
- Attempt to gain unauthorised access to any other computer system through or beyond the school authorised access account. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of 'browsing'.
- Download programs or files without seeking permission from the ICT co-ordinator or supervising member of staff
- Be allowed access to public or unregulated chat rooms, only using regulated educational chat environments when directed by a member of the school teaching staff

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 school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					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	
	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	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	

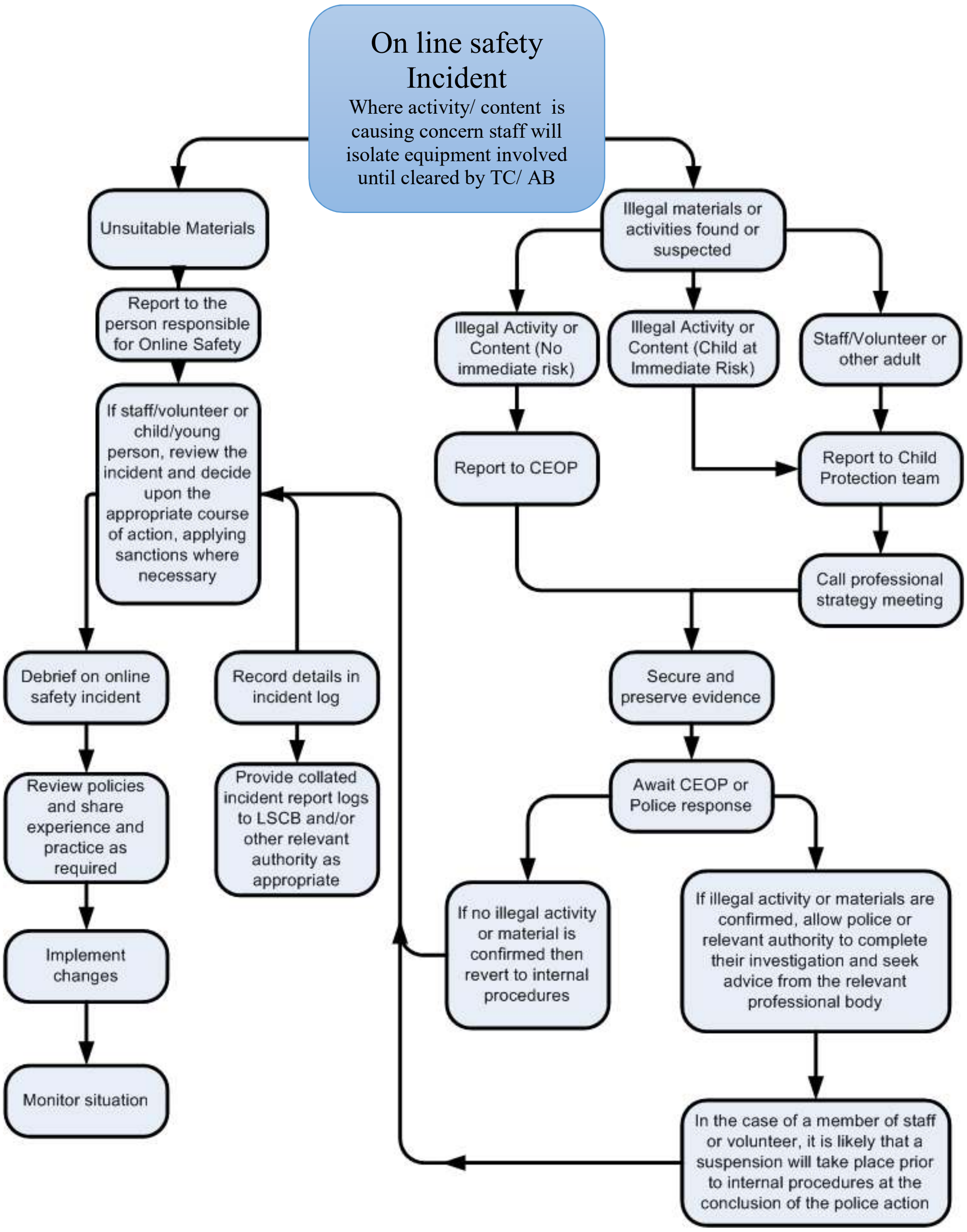
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)	X				
On-line gaming (non educational)		X			
On-line gambling				X	
On-line shopping / commerce (for school purposes)		X			
File sharing			X		
Use of social media		x			
Use of messaging apps				x	
Use of video broadcasting eg 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.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school / academy 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 / volunteer 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
  - 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 / academy* and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School / Academy Actions & Sanctions

It is more likely that the school / academy 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 — Actions / Sanctions

Incidents:	Refer to class teacher	Refer to Online Safety Officer	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg 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	x	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X					X		X	
Unauthorised use of mobile phone / digital camera / other mobile device		X	X			X		X	
Unauthorised use of social media / messaging apps / personal email		X	X			X		X	
Unauthorised downloading or uploading of files	X	X			X	X	X	X	
Allowing others to access school / academy network by sharing username and passwords	X	X			X	X	X	X	X
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X	X			X	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	X	X	X
Corrupting or destroying the data of other users	X	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	X		X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	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		X	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	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X		X	X	X	X	

Staff Actions / Sanctions

Incidents:	Refer to Online Safety Offcier	Refer to Headteacher	Refer to Arthur Terry HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	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	X	X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	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 eg holding or transferring data in an insecure manner	X				X	x		
Deliberate actions to breach data protection or network security rules	X	X	X		X	X		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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	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	x
Actions which could compromise the staff member's professional standing	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		
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	X		
Deliberately accessing or trying to access offensive or pornographic material	X	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	

MEMORY STICKS

Pupils must not use memory sticks in school without the authorisation of one of the schools ICT Technicians prior to **each** use, this enables scanning of the device for potential unwanted materials, viruses, spyware, etc.

Staff must not take home memory sticks that have personally identifiable information on them. All memory sticks used for work purposes should be encrypted.

SANCTIONS FOR DELIBERATE MISCONDUCT

Any staff to be contravening the above and found to be deliberately accessing inappropriate materials should be aware that this is a very serious offence and may lead to immediate suspension and possible dismissal pending further investigations.

Any pupils found not complying with the school Online Safety policy and related policies may have their internet access removed with further action decided by the Online Safety officer and Head Teacher.

HANDLING ONLINE SAFETY COMPLAINTS

- Complaints of internet misuse will be dealt with initially by the Online Safety officer
- Any complaint of staff misuse will be reported to and dealt with by the head teacher
- Complaints of a child protection nature must be dealt with in accordance to the school's child protection procedures
- Pupils and parents will be informed of the complaints procedure

PLAGIARISM AND COPYRIGHT INFRINGEMENT

Staff need to be aware of copyright laws with regards to information on the World Wide Web. The same precautions are to be taken with information from the World Wide Web as those found in print. When in doubt you must contact the webmaster of the site you are using.

INAPPROPRIATE ACCESS TO MATERIAL

Staff will **not** use the school computers to access material that is profane or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

DUE PROCESS

The school will co-operate fully with local, national or international officials in any investigation related to any illegal activities conducted through working through the school system.

WORKING WITH CHILDREN

When working with children on the Internet, staff will supervise children at ALL times. If children are observed to be accessing inappropriate materials, there are 2 courses of action: -

1. Where a pupil deliberately accesses inappropriate material, they should be removed from the computer and all computer privileges removed for a period of time that is appropriate to the misdemeanour.

2. Where a pupil inadvertently accesses inappropriate material, the site is to be reported to the Online Safety officer to investigate further.

3. All incoming/outgoing e-mails that are written by pupils will be screened by the teacher. Inappropriate mail will be deleted/not sent.

SCHOOL WEBSITE

- Where photos of pupils are to be uploaded then agreement will be made with parents and only forenames will not be published. Surnames should NOT be used in order to minimise identification.
- Files uploaded will not refer to names. E.g. A photo of Joe Bloggs will not be joebloggs.jpg.
- Group photos will not contain a names list.
- Home information and e-mail identities will not be included only the point of contact to the school i.e. phone number, school address, enquires@meregrn.bham.sch.uk

SYSTEM SECURITY

- Virus detections will be dealt with promptly and where staff laptops are affected staff will be notified immediately and asked to bring the laptop into school ASAP for quarantine.
- All workstations and laptops in school will be updated with Microsoft critical updates on a regular basis or in the case of an urgent update this will be completed at the earliest opportunity.
- School security settings for the network, user accounts and folder structures will be reviewed regularly.
- Any suspected access or security issue will be reported to the head teacher or one of the ICT Technicians at the earliest possible time.

TWITTER AND SOCIAL MEDIA

The school Twitter account is designed to celebrate the successes of Mere Green Primary School

- All photo's tweeted must be within the school guidelines and policies in place to protect pupils
- Photo's and full names (including surnames) must not be posted together as this is deemed personally identifiable information
- Tweets must not include anything listed in the inappropriate behaviour section above
- All use must be in line with wider school policy

PASSWORDS AND ACCESS TO SCHOOL SYSTEMS

- All staff are to be made aware of the importance of having a secure password

- All staff are to ensure their workstation is locked when not being used

- All staff must ensure they do not give out passwords to allow access to school systems

- Personal data must not be saved on shared network drives that students have access to

HOW THE POLICY WILL BE IMPLEMENTED WITHIN SCHOOL

All staff must be familiar with the school ONLINE SAFETY policy and Acceptable Use Agreements, prior to using the internet with their pupil's to enhance learning. Pupils may need to be reminded of the school's rules at the point of Internet use. Safe practice must be taught to the children prior to internet use, which should inform them of the valuable experience of Internet use and also the dangers, both at school and at home.

- Online Safety AUA posters will be visible in all classrooms and where computers are used.(Where the building guidance of the school allows)
- Pupils will be informed that the use of Internet will be monitored at all times.

Whole school participation in termly Online Safety activities, alongside embedded Online Safety lessons throughout the school year will help enforce the school Online Safety policy and general message of staying e-safe.

In order to maintain an effective Online Safety Policy, we will provide opportunities for teachers and teaching assistants undertake Online Safety training which will be refreshed regularly. The staff will need to subscribe to its values and methods in order to maintain its effectiveness. Staff will also be provided with opportunities to discuss arising issues and develop teaching strategies. Staff will also understand that the 'acceptable use policy' will also apply to them within school.

All staff must therefore: -

- Accept the terms of the Acceptable Use Agreements before using any Internet resources in school.
- Have access to a copy of the Acceptable Use Agreements and related policies, ensuring they fully understand it.
- Be aware that school computers are monitored and misuse can be traced to its user
- Maintain professional conduct when using the internet at all times
- Develop their knowledge of safe and responsible Internet use within the classroom as a teaching tool

Appendix

Acceptable Use Agreements for KS1/ KS2 / Parents /Staff / Visitors /
Safeguarding policy
Anti-bullying policy
Data-protection policy
Social media policy
Child-protection policy
Online Safety incident log reporting forms

Acknowledgements