London Meed Primary School

E-Safety Policy

	Date of Next Review:	January 2020
Date of Approval: Pending Full Governors meeting Chair of Governors Name: Jane Davey	Chair of Governor Signature:	Pending FGB meeting

Teaching and Learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by West Sussex and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They will be encouraged to report any inappropriate material to an adult.

Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly
- Virus protection will be updated regularly
- Security strategies will be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupil's personal information will not be published.

Publishing photographs, images and work

- Pupils' full names will be avoided on the Website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs or images of pupils are published

- Permission from adults will be obtained before their names, photographs or images of themselves are published

- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

- Staff will not keep images of children on personal devices e.g. memory sticks, or use them for any use other than in school.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords.

- Newsgroups will be blocked unless a specific use is approved.

- All users will be advised never to give out personal details of any kind which may identify them, anybody else or their location.

- Pupils must not place personal photos on any social network space provided in the school learning platform without permission.

Managing filtering

- The school will work in partnership with West Sussex Children's Services to ensure systems to protect pupils are reviewed and improved.

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff.

- The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet **(1)**.

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.

- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Other devices

- Mobile phones and associated cameras will not be used during lessons or formal school time. Taking photographs at any time without the subject's consent is prohibited

- The sending of abusive, offensive or inappropriate material is forbidden.

- Staff should not share personal telephone numbers with pupils and parents. (A school phone will be provided for staff where contact with pupils is required).

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

<u>Policy Decisions</u>

Authorising Internet access

- All staff must read and sign the staff AUP policy before using any school ICT resource (Appendix 1).

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

- Parents will be asked to sign and return a consent form (Appendix 2).

- Any person not employed by the school or West Sussex County Council will be asked to sign an 'acceptable use of school ICT resources' form before being allowed to access the Internet on the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

Neither the school nor West Sussex Children's Services can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective

Handling E-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be referred to the Senior Designated Professional for Safeguarding and dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- All use of the school Internet connection by community and other organisations shall be in accordance with the school E-safety policy.

Data Protection

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 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". (see Privacy Notice section in the appendix)*
- *It has a Data Protection Policy*
- *It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)*
- *Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)*
- *Risk assessments are carried out*
- *It has clear and understood arrangements for the security, storage and transfer of personal data*
- *Data subjects have rights of access and there are clear procedures for this to be obtained*
- *There are clear and understood policies and routines for the deletion and disposal of data*
- *There is a policy for reporting, logging, managing and recovering from information risk incidents*
- *There are clear Data Protection clauses in all contracts where personal data may be passed to third parties*
- *There are clear policies 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, unless permission is agreed in advance by the Head teacher or other senior member of staff, ensuring risks have been identified, discussed and minimised.*

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

- *the data (where possible) must be encrypted and password protected. Where data is not password protected, the portable device itself should be password protected.*
- *the device must be password protected.*
- *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

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff & other adults			Students/Pupils				
	Allowed	Allowed at certain times	Not allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school *Pupils must hand in any mobile phone brought into school to the school's office upon arrival for safe-keeping and return upon exit	X							X *
Use of mobile phones in lessons			X					X
Use of mobile phones in social time	X							X
Taking photos on mobile phones/cameras		X						X
Use of other mobile devices e.g. tablets, ebooks	X						X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails			X					X
Use of messaging apps		X						X
Use of social media			X					X

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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).*
- *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, chat, etc…) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- *Pupils at KS2 will be provided with individual school email addresses for educational use.*
- *Pupils should be taught about e-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.*

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students/Pupils

Incidents:	Refer to class teacher	Refer to technical support staff for action re filtering/security etc	Incident formally logged	Verbal warning	Refer to Headteacher/member of Senior Staff	Inform parents/carers	Further sanction (eg detention/exclusion)	Removal of network/internet access rights	Refer to Police
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	?
Unauthorised use of non-educational sites during lessons	X	X	X	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		X	X		
Unauthorised downloading or uploading of files	X	X	X		X	X	X	X	
Allowing others to access school network by sharing username and passwords	X	X	X	X					
Attempting to access or accessing the school network, using another pupil's account	X	X	X	X	X				
Attempting to access or accessing the school network, using the account of a member of staff	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	?
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	
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	?
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

Incidents: X – Action to be taken ? – Action dependent on severity of incident or whether an additional incident to one previously logged by a staff member	Refer to Technical Support Staff for action re filtering etc	Incident formally logged	E-Safety Co-Ordinator informed of incident	Refer to Headteacher/member of Senior Leadership Team	Refer to Local Authority/HR	Verbal or Written Warning	Disciplinary action	Refer to Police
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	?	?
Inappropriate personal use of the internet/social media/personal email using school IT equipment	X	X	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	?	?	?		
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	X	?	?
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	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	?	?
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils	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 into disrepute or breach the integrity of the ethos of the school	X	X	X	X	X	X	?	?
Using proxy sites or other means to subvert the school's filtering system	X	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	X	X	?	?
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	?

Communications Policy

Introducing the E-safety policy to pupils

- Appropriate elements of the E-safety policy will be shared with pupils
- Pupils will be informed that network and Internet use will be monitored
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils

Staff and the E-safety policy

- All staff will be given the School E-safety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on Esafety.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents and carers will be reminded that they must not publish any images or comments of performances and other community events on social network sites before and after each event.

This policy should be read in conjunction with the Schools Safeguarding Policy.

Reviewed January 2017

To be reviewed: January 2020

Appendix 1 - London Meed Staff Acceptable Use Policy

School networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. If you make a comment about the school or County Council, you must state that it is an expression of your own personal view. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and / or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

CONDITIONS OF USE

Personal Responsibility

Users are responsible for their behaviour and communications. Staff will be expected to use the resources for the purposes for which they are made available. It is the responsibility of the User to take all reasonable steps to ensure compliance with the conditions set out in this Policy, and to ensure that unacceptable use does not occur. Users will accept personal responsibility for reporting any misuse of the network to Mrs K Chalmers, Data Manager.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Below is a set of rules that must be complied with. This is not an exhaustive list and you are reminded that all use should be consistent with the school ethos and code of conduct.

1. I will not create, transmit, display or publish any material that is likely to: harass, cause offence, inconvenience or needless anxiety to any other person or bring the school (or West Sussex County Council) into disrepute.

2. I will use appropriate language –I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.

3. I will not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.

4. I understand that staff under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

5. Privacy – I will not reveal any personal information (e.g. home address, telephone number, social networking details) of other users to any unauthorised person (see 21). I will not reveal any of my personal information to students.

6. I will not trespass into other users' files or folders.

7. I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself. Likewise, I will not share those of other users.

8. I will ensure that if I think someone has learned my password then I will change it immediately and/or contact Mrs K Chalmers

9. I will ensure that I log off after my network session has finished.

10. If I find an unattended machine logged on under other users username I will not continuing using the machine – I will log it off immediately.

11. I will not use personal digital cameras or camera phones for creating or transferring images of children and young people without the express permission of the school leadership team.

12. I am aware that e-mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.

13. I will not use the network in any way that would disrupt use of the network by others.

14. I will report any accidental access, receipt of inappropriate materials or filtering breaches/ unsuitable websites to JSPC.

15. I will not use “USB drives”, portable hard-drives, “floppy disks” or personal laptops on the network without having them “approved” by the school checked for viruses,

16. I will not attempt to visit websites that might be considered inappropriate or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.

17. I will not download any unapproved software, system utilities or resources from the Internet that might compromise the network or are not adequately licensed.

18. I will not accept invitations from children and young people to add me as a friend to their social networking sites, nor will I invite them to be friends on mine. As damage to professional reputations can inadvertently be caused by quite innocent postings or images - I will also be careful with who has access to my pages through friends and friends of friends. Especially with those connected with my professional duties, such a school parents and their children.

19. I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to, are not confused with my professional role in any way.

20. I will support and promote the school’s e-safety and Data Security policies and help students be safe and responsible in their use of the Internet and related technologies.

21. I will not send or publish material that violates Data Protection Act or breaching the security this act requires for personal data, including data held on the SIMS Learning Gateway.

22. I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.

23. I will not attempt to harm or destroy any equipment or data of another user or network connected to the school system.

24. I will ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used.

25. I will ensure that any Personal Data (where the Data Protection Act applies) that is sent over the Internet will be encrypted or otherwise secured.

 Staff must comply with the acceptable use policy of any other networks that they access.

 Staff will follow the “Safer Use Of The Internet By Staff Working With Young People” published within the West Sussex Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform Mrs K Chalmers who will inform JSPC immediately if a security problem is identified and should not demonstrate this problem to other users. Files held on the school's network will be regularly checked by JSPC. Users identified as a security risk will be denied access to the network.

MEDIA PUBLICATIONS

Written permission from parents or carers must be obtained before photographs of or named photographs of students are published. Also, examples of students' work must only be published (e.g. photographs, videos, TV presentations, web pages etc) if written parental consent has been given.

Further guidance can be found in the "Model Policy for schools regarding photographic images of children" August 2010.

Copies can be obtained from section 6 of the WSSS Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

Appendix 2:

London Meed Primary School

Pupil Acceptable Use Policy

All pupils must follow the rules in this policy when using school computers, and the school learning platform.

Pupils that do not follow these rules may find:

- They are not allowed to use the computers,
- They can only use the computers if they are more closely watched.

Their teachers will show pupils how to use the computers.

Computer Rules

1. I will only use polite language when using the computers
2. I must not write anything that might: upset someone or give the school a bad name.
3. I know that my teacher will regularly check what I have done on the school computers.
4. I know that if my teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5. I must not tell anyone my name, where I live, or my telephone number – over the internet.
6. I must not tell my username and passwords to anyone else but my parents.
7. I must never use other people's usernames and passwords or computers left logged in by them.
8. If I think someone has learned my password then I will tell my teacher.
9. I must log off after I have finished my computer.
10. I know that e-mail is not guaranteed to be private. I must not send unnamed e-mails.
11. I must not use the computers in any way that stops other people using them.
12. I will report any websites that make me feel uncomfortable to my teacher or a member of staff.
13. I will tell my teacher or a member of staff straight away if I am sent any messages that make me feel uncomfortable.
14. I will not try to harm any equipment or the work of another person on a computer.
15. If I find something that I think I should not be able to see, I must tell my teacher straight away and not show it to other pupils.

Unacceptable Use

Examples of unacceptable use include, but are not limited to:

- Using a computer with another person's username and password.
- Creating or sending on the Internet any messages that might upset other people.
- Looking at, or changing work that belongs to other people.
- Waste time or resources on school computers.

Student User Agreement Form for the Student Acceptable Form for the Student Acceptable Use Policy

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all rules explained by my teacher or member of staff. I agree to report anyone not using the computers sensibly to my teacher or member of staff. I also agree to tell my teacher or another member of staff if I see any websites that make me feel unhappy or uncomfortable. If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Student Name:_____

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers may have their use stopped, more closely monitored or past use investigated.

Parent/Carers/Guardians Name:_____

Parent/Carers/Guardians Signature:_____

Date:_____