E-Safety Policy

issued by the Governors of Milton Mount Primary School

Effective from: March 2018

Signed by: Lesley King

Next review date: March 2019

The E-Safety Policy reflects the UN Convention on The Rights of the Child (CRC) by supporting these Articles:

Article 13: Children have the right to get and to share information
Article 17: Children have the right to reliable information from the mass media

1. **Rationale**
   - Internet use is a key part of life in the 21st Century. In Milton Mount Primary School, we aim to keep children safe when they use the internet and to teach them how to keep themselves safe.
   - Children are taught about safe and responsible use of technologies when online. They are taught about appropriate online behaviour and what to do if they feel worried about something online.

2. **Internet access**
   - Children in the school have a year group log in to access the school network, which in turn provides filtered access to the internet. The children have their own password to access Purple Mash (our computing software) and they are taught to keep passwords private and to understand that sharing a password can result in someone using their access inappropriately.
   - Children and parents are encouraged to use the educational links on the school website.
   - Nobody is permitted to access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; lifestyle websites e.g. that promote anorexia or self-harm; any other information which may be illegal or offensive to colleagues.
   - It is recognised that under certain circumstances inadvertent access may happen. For example, a school researching the holocaust may produce results with Nazi propaganda. Should a pupil or member of staff access any of these sites unintentionally they should report the matter to the Headteacher so that it can be logged. We encourage the children to turn the screen off if they see anything that they don't think is appropriate so that the teacher can log the website in order for it to be blocked.
   - Access to any of the following should be reported to West Sussex Police: images of child abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

3. **Social networking**
   - School has a Twitter account which is monitored by the teachers. It is used to share children's achievements and other items of educational value.
   - Children's photographs will only be included in tweets if parents have signed permission forms for the images to be used on the internet.
   - School will remove a photograph of a child as soon as possible if their parents request this.
   - Individual teaching staff who also use a Twitter account for school should ensure that their tweets are in-line

with the school policy and any photographs taken of school children, using their personal phones or cameras, are removed from these devices routinely.

- We acknowledge that staff might use social networking sites for personal use out of school. We advise that they bear in mind security of personal details, rather than relying on the default settings. Staff should fully acquaint themselves with the privacy settings that are available on any social networking profile in order that personal profiles are not publicly available. They should not post about school in any negative way or in any way that would bring the school into disrepute.
- Using personal accounts, members of staff, student teachers, work experience students and volunteer helpers should never knowingly become "friends" with pupils on any social networking site or engage with pupils on internet chat.
- Children are taught that there are minimum age limits to sign up for social networking accounts and that this is for their safety.

4. Use of Email –

- All members of staff should use their professional email address for conducting school business with outside agencies.
- Parents use teacher@miltonmount.co.uk to email teachers. These emails are checked before being passed onto staff.

5. Unwanted contact

- Children are taught that sometimes people adopt a false identify or profile on the internet e.g. in chat rooms or social network sites. They are taught that they should not share any personal information with people that they don't know in real life, even if their profiles say they are friends of their friends.
- Children are taught that they have the right to block contacts and that they should tell a trusted adult about any unwanted contact.

6. Passwords

- Staff should keep school passwords private. Passwords are confidential and individualised to each person.
- On no account should a member of staff allow a pupil to use a staff login.
- We recognise that at times people without logins will need them. New staff awaiting a login should use one of the supply teacher logins.

7. Data Protection

- Where a member of staff has to take home sensitive or confidential information sufficient safeguards should be in place to prevent loss or misuse, i.e. Staff should log in to the secure remote access to the school network from home, rather than carry unencrypted personal data.
- All personal data will be handled according to the Data Protection Act 1998

8. Personal Use

Staff are permitted to use school ICT equipment for personal use as long as the use complies with all other points of this policy.

9. Images and Videos

Staff and pupils should not upload onto any internet site (including social media sites) images or videos of themselves or other staff or pupils without consent, including photos of staff which may cause embarrassment or bring the school into disrepute.

10. Use of Personal ICT

Use of personal ICT equipment, including cameras on mobile phones, is at the discretion of the school. Any such use requires the explicit permission of the Headteacher.

11. Viruses and other malware

Any suspected virus outbreaks should be reported to the Senior Leadership Team, who will ensure that JSPC

(the school network manager) is informed as soon as possible.

12. Reporting a Problem

- Children are taught to turn the screen off immediately if they inadvertently come across inappropriate content or a contacted inappropriately.
- They should then report the incident immediately to a member of staff who will inform a member of the Senior Leadership Team.
- The Senior Leadership Team will contact JSPC to block the website or will report the incident to the police if deemed serious enough.

13. Staff should note that internet use and email may be subject to monitoring

This policy has been circulated to all staff and it is expected that full compliance will be given. All staff and children will sign an appendix to the policy to that effect (see appendix 1), which will be kept in the policy file in the school office.

During the updating of this policy, Safeguarding was taken account of.
Approved by the Governing Body

Signed (Chair of Governors) _____

Date March 2018

Review Date March 2019

Appendix 1

Staff Acceptable Use Policy
issued by the Governors of Milton Mount Primary School

Effective from: March 2018

Signed by: Lesley King

Next review date: March 2019

The Staff Acceptable Use Policy reflects the UN Convention on The Rights of the Child (CRC) by supporting these Articles:

Article 3: The best interests of the child must be a top priority in all things that affect children

Article 16: Every child has the right to privacy

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 user's 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 the Head Teacher or a member of the Headship team.

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.

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 the Head Teacher or a member of the Headship team.
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 usernames 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 Head Teacher or a member of the Headship 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 the Head Teacher or a member of the Headship team.

15	I will not use “USB drives”, portable hard-drives, tablets or personal laptops on the network without having them “approved” by the school and 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 as 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 the Data Protection Act or breaching the security this act requires for personal data, including data held in SIMS.
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 (or taken offsite in any other way) will be encrypted or otherwise secured.

Additional guidelines

- 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 the Head Teacher or a member of the Headship team 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 a person authorised by the Head Teacher. 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 may 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 5 of the WSSS Schools Acceptable Use Policy - http://wsgfl.westsussex.gov.uk/AUP

Staff User Agreement Form for the Staff Acceptable Use Policy

As a school user of the network resources, I agree to follow the school rules (set out above) on its use. I will use the network in a responsible way and observe all the restrictions explained in the school acceptable use policy. If I am in any doubt I will consult the Head Teacher or a member of the Headship team.

I agree to report any misuse of the network to the Head Teacher or a member of the Headship team.
I also agree to report any websites that are available on the school Internet that contain inappropriate material to a member of the Headship team.
Lastly I agree to ensure that portable equipment such as cameras or laptops will be kept secured when not in use and to report any lapses in physical security to a member of the Headship team.
If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

Staff Name:

Staff Signature (if appropriate):

Date: _ _ /_ _ /_ _ _ _

During the updating of this policy, Safeguarding was taken account of.
Approved by the Governing Body

Signed (Chair of Governors) _____

Date March 2018

Review Date March 2019

Computing Charter: Reception & KS1

S

I will only click on icons and links when I know they are **safe**.

A

I will only use the Internet and email with an **adult** present.

F

I will only send **friendly** and polite messages to people I know.

E

If I see something with my **eyes** that I don't like, I will tell an adult.

I have read and understood that if the Computing Charter is broken in any way, my teachers have the right to remove my use and privileges for an agreed period of time. This is to keep me safe.

Computing Charter: KS2

This Computing Charter will keep me safe and help me to be fair to others.

☺ I will sign in and log off properly and put the technology back carefully.

☺ I will keep my logins and passwords to myself.

☺ I will check with an adult if I want to bring files into school.

☺ I will only edit or delete my own files and not look at, or change, other people's files without their permission.

☺ I will not open an attachment, or download a file, unless I know and trust the person who has sent it and have checked with an adult.

☺ I will ask an adult before I print or delete my own work.

☺ I am aware that some websites and social networks have age restrictions and I should respect this.

☺ I will not attempt to visit Internet sites that I know are banned by the school and will click on icons and links only if I know they are safe.

☺ I will communicate in a polite, respectful and sensible manner.

☺ I will not share my personal details or send a photograph or video that could be used to identify me, my family or my friends.

☺ I will never arrange to meet someone I have only ever previously met on the Internet.

☺ I will tell an adult straight away if I find or see anything inappropriate and will not respond to it.

I have read and understood that if the Computing Charter is broken in any way, my teachers have the right to remove my use and privileges for an agreed period of time. This is to keep me safe.