MAULDETH ROAD PRIMARY SCHOOL

E-SAFETY POLICY

February 2020

E-Safety Policy (Amended Draft)
Date: February 2020
Review Date: February 2021

INTRODUCTION

This policy has been developed to ensure that all adults at Mauldeth Road Primary School are working together to safeguard and promote the welfare of children and young people. This policy applies to all members of the school community (including staff, pupils, governors, parents/carers, visitors and community users) who have access to and are users of the school's ICT systems, both in and out of school. This policy should be used in conjunction with other school polices eg Behaviour, Anti-bullying and Safeguarding. E-safety is a safeguarding issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

This policy will be reviewed annually, or sooner, if significant change requires it.

At Mauldeth Road Primary School we know that the internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide children and young people with quality access as part of their learning experience.

Digital technologies are integral to everyday life. They can develop understanding of the world and communication with others, and can have a positive impact on pupils' engagement and achievement. However we are aware that they can pose risk within and outside the school. All staff are aware that these risks can include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorized access to / loss of / sharing of personal information
- Grooming
- Radicalisation
- Sharing / distribution of personal images without consent or knowledge
- Inappropriate communication with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- Inability to evaluate information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- Excessive use impacting on the social emotional and academic development

Risk cannot be eliminated completely. It is therefore essential to build pupils' resilience to these risks, so that they have the confidence and skills to face and deal with them. Our school must demonstrate the necessary safeguards to manage and reduce these risks. This E-Learning/Safety Policy explains how we intend to do this.

ROLES AND RESPONSIBILITIES

Governors are responsible for the E-Safety Policy and for reviewing its effectiveness. This will be carried out by regular reports to Governors about e-safety training, incidents and monitoring. A nominated E-Safety Governor will:

- Meet with the E-Safety Coordinator
- Monitor E-Safety logs
- Report to Governors' Premises and Safety Committee meetings

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community by

- Ensuring that staff receive suitable CPD
- Ensuring systematic monitoring and support
- Taking a day to day responsibility for e-safety issues
- Ensuring that all staff are aware of e-safety procedures
- Acting as a single point of contact for both Manchester Safeguarding Children's Board (MSCB) and agency staff and service users
- Making appropriate responses to policy breaches including escalating incidents as appropriate
- Ensuring that an e-safety curriculum is being delivered

The ICT coordinator is responsible for assisting the Headteacher in all aspects of E-Safety by

- Providing training and advice for staff
- Receiving, recording, monitoring and reviewing incidents of e-safety
- Meeting regularly with the Headteacher to discuss any issues and review incident logs
- Developing and updating a relevant e-safety curriculum
- Ensuring AU policy is read and signed by staff & reviewed annually
- Overseeing the school's technical support provision.
- Meeting with the E-Safety Governor

Technical Support Staff are responsible for ensuring that:

- The school's technical infrastructure is secure against misuse or malicious attack
- The school meets the Local Authority's online safety technical requirements
- They keep up to date with recent e-safety technical information
- The school's network is monitored and attempted misuse is reported to the headteacher
- Anti-virus, filtering and security software are up to date

Teaching and Support Staff are responsible for supporting E-Safety by

- Having up to date awareness of E-Safety— and of school E-Safety policy and practices.
- Ensuring they have read, understood and signed the school Staff Acceptable Use Policy (AUP) in full.
- Reporting suspected misuse (including accidental incidents) of the school's ICT network or incidents of cyber-bullying to the Headteacher and ICT co-ordinator
- Promoting e-safety issues in all curricular and other school activities
- Ensuring that they read the pupils' AU policy with the children in their class. All children in their class must then sign the contract and it must be displayed in the classroom.
- Monitoring ICT activity in lessons, extra-curricular and extended school activities

- Checking the content of websites and web-based media (downloaded or streamed) before intended for use with pupils to ensure suitability
- Monitoring the use of ICT by classroom visitors to ensure that content is appropriate

Designated safeguarding Lead (DSL) should be trained in e-safety and be aware of child protection issues that could arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming • cyber-bullying

Pupils:

- Must use school ICT systems in accordance with the Pupil AUP Agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and incidents of cyber-bullying and know how to do so
- Should understand the need to adopt good e-safety practice, when using digital technologies out of school, and realise that the school's E-Safety Policy should inform their actions out of school.

Parent/Carers are also responsible in helping to ensure that children understand the need to use the internet and mobile devices in an appropriate way. School will help parents understand these issues through newsletters, letters and information on the school website. Parents will be informed about national/local online safety campaigns.

E-SAFETY CURRICULUM

Whilst regulation and technical solutions are important, they must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is, therefore, an essential part of the school's online safety provision. Children need the school's help to recognise and avoid online safety risks and build their resilience. Staff should reinforce online safety messages across the curriculum. The online safety curriculum includes:

- A planned e-safety programme, provided as part of computing lessons but covering the use of digital technologies in and outside school. It will be based on the SMART internet rules developed by Childnet and resources from CEOP via the thinkuknow website. Children will learn to use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

- Key e-safety messages are embedded into other areas of the curriculum as appropriate

- Children participate in Digi-Fun Week/E-safety day annually

- E-safety issues, including cyber-bullying are addressed in assemblies, year groups or with individual pupils as appropriate

- Teaching the critical appraisal of information found on the internet as appropriate.

- Each pupil signs an E-Safety contract at the beginning of each year. These contracts are discussed with the class teacher and peers and contracts are displayed in classroom. The Key Stage 1 AU policy and Key Stage 2 policy for pupils are displayed in the ICT suite.

- Pupils are encouraged to adopt safe practices adopted in school outside school. in and outside of school

- Acknowledgement of sources of information and respect for copyright

- Staff acting as good role models in their use of ICT, the internet and mobile devices

E-SAFETY TRAINING

All staff will receive e-safety training and should understand their responsibilities, as outlined in this policy. Training will be offered as follows.

- A planned programme of e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly

.

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The DSL will receive regular updates through attendance at MSCB meetings and by reviewing national and local guidance documents.
- This E-Safety policy and its updates will be shared with staff on the intranet and presented to staff in staff meetings.
- Advice/guidance/training will be provided as required to individuals
- Training will be provided for governors.

TECHNICAL INFORMATION

The School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the MSCB E-Safety Guidelines.

- The school will use an approved Internet Service Provider/ filtering system.
- All technologies will be risk-assessed with regard to e-safety
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located with restricted physical access
- All users will have clearly defined access rights to school ICT systems and intranet. Details of the access rights available to groups of users will be recorded by the ICT Coordinator and will be reviewed, at least annually, by governors.
- All staff are provided with an encrypted pen drive. The ICT co-ordinator will keep an up to date list of staff user names and passwords for the pen drives.

- All staff will be provided with a username and password that they must not divulge to others. The ICT co-ordinator will keep an up to date list of staff users names in a secure file. Staff are responsible for notifying the ICT Coordinator if they change their password

- Where pupils (at KS1 and above) are provided with usernames, they will be instructed that they must not share these with other pupils.

- "Master/administrator" passwords for the school ICT system, must always available to the Headteacher and to the ICT co-ordinator.

- Any switching off the filtering for any reason, or user, must be logged and carried out by a process that is agreed by the Headteacher.

- Requests from staff for sites to be removed from the filtered list will be considered by the ICT co-ordinator and Headteacher. If agreed, this action will be recorded and logs of these will be reviewed by the ICT co-ordinator regularly.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy

- An appropriate system is in place for users to report any actual / potential e-safety incident to the ICT co-ordinator and Headteacher

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- Members of staff must only ever use their individual username and password to access the school's network and must log off at the end of their session. Staff must always log out of their google drive when they have finished.

- School hardware must never be connected to any personal device, in school or at home. If documents completed on a personal computer are needed for work purposes they should be emailed to a school address and downloaded on site.

STAFF WIRELESS DEVICES

The wireless devices (laptops, iPads, etc) provided by the school remain the property of the school at all times. As these items are entrusted to certain individuals an additional set of rules govern these items. Any member of staff who has been given a wireless device must sign the wireless device contract.(see AU Policy – Appendix 1)

- The device must always be in school when the associated staff member is in school. The device may be taken off-site for work-related activities.

- The device may be connected to a wireless home network.

- Personal USB based hardware (cameras, pen drives, external hard drives etc.) must not be connected to the device.

- The associated member of staff is responsible for the use of the device, at all times, while it is off-site.

- Files must be stored on a provided encrypted pen drive. Personal files must not be stored on the device (this includes images and media files).

- Sensitive pupil or staff data must not be stored on any portable memory device.

- The ICT coordinator will keep a record of all encrypted pen-drive passwords. An iPad and Laptop audit is carried out termly by the ICT co-ordinator and school technician.

- Permission from the ICT coordinator must be sought before installing any new software application or apps for the iPad. Updating existing applications (new smart notebook, flash etc) is allowed.

- The device may be used for personal internet use (including forms of internet communication) providing that it does not contradict any of the rules set out in this e-safety document. Any infringements of these rules, regardless of who has carried out the action, must be reported to the school's ICT co-ordinator as soon as possible.

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 they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- When using digital images, staff should educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images, especially when sharing their own images.
- Images should be stored on a password protected drive on the school's network, access to this drive is limited to school staff.
- Digital images must be uploaded and deleted from media cards at the first opportunity.
- Staff are allowed to take digital / video images to support learning, but must follow school policies concerning the sharing, distribution and publication of those images.
- Images should be recorded using school equipment. If not possible, staff may use smartphones but must transfer them to the school's network and deleted from their own device at the earliest opportunity.
- Members of staff must be able to justify the reasons behind taking and storing any digital media file (including image and sound).
- In all digital / video images that pupils must be appropriately dressed and not be participating in activities that might bring disrepute.
- Pupils must not share, publish or distribute images of others.
- Photographs of pupils published on internet-based platforms will be selected carefully, comply with good practice and be accompanied by text that does not name them.
- Written permission from parents/carers to use digital images of their children is obtained at school entry. An up-to-date list is kept on Arbor. It is the responsibility of the person recording the images to check the list.

THE SCHOOL WEBSITE

Mauldeth Road uses its website to celebrate successes, share information and keep parents/carers informed about events taking place. The school will ensure compliance with this policy in the placing of content on the website. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material.

- Photographs of pupils will not be used without the consent of the pupil's parents/carers (see Use of digital and Video images above). Full names of pupils will not be used on the website, particularly in association with any photographs.

- The point of contact on the school website will be the school address, school email and telephone number. Staff or pupil's home information will not be published

- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained.

- Managing Internet Access

MANAGING INTERNET ACCESS

Developing good practice in internet use as a tool for teaching and learning is essential.

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the children and young people.

- Pupils will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupil's age and maturity.

- Pupil's will be taught what to do if they experience material that they may find distasteful, uncomfortable or threatening.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator.

- Pupils will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

The Use of YouTube

The school has unblocked YouTube to allow access to the variety of educational content that it offers. However, the following rules must be adhered to, to help ensure the safety of the pupils and the integrity of the school's network. All staff must be aware of the points below .

- Staff have access to YouTube to support teaching and learning. Personal use of YouTube is allowed before 8.30am and after 3.30pm, but use must be appropriate to the school environment. This rule applies regardless of the device/network used to connect to YouTube.

- Staff must not search for videos in front of the class; all videos must be found prior to the lesson. As YouTube videos do not come with age classification advice, teachers must watch the entire video to assess the suitability of the resource for the pupils they teach.

- Teachers must be aware that YouTube is a commercial site and that videos may contain adverts. If adverts are displayed as part of the video it is suggested that the commercial nature of the site is discussed with the class.

- Pupils are not allowed to use YouTube on their individual devices; any videos that need to be watched should be shown to the entire class through the room's projector.

- If an inappropriate video/image is displayed, the screen should be turned off and the incident reported to the headteacher or ICT Co-ordinator as soon as possible.

USE OF SOCIAL MEDIA

While the school cannot govern the individual's use of internet-based social media outside of the school, it does expect all members of staff to uphold the profession and the institution by using these sites in a responsible manner, exercising common sense at all times. To help do so, staff are advised:

- To use security settings to restrict access to their accounts including view, searching and tagging.

- Not to upload pictures of school events (both official and unofficial).

- Not to post status updates regarding events in school and not to enter into discussions with others regarding school.

- Not to accept any pupils (existing or past) or parents as friends.
- To remember comments made in writing are subject to disclosure and could be used as evidence in a court of law

- The school will use Social Media as appropriate to further enhance the reputation of the school, to show case its achievements and as means of communication with parents and carers.

The Use of Twitter

The school uses Twitter as an additional tool to promote parental engagement by sharing photos and information about events, activities and successes of the pupils. Examples of the use so far: pictures of artwork completed by the class; pictures of classroom displays; pictures of children learning to ride bikes. To ensure the staff use of Twitter is appropriate, they must adhere to the rules below.

- The accounts members of staff follow must be appropriate to the environment in which they work.
- Images, including those of pupils, can be tweeted but must adhere to the digital images section of the school's e-safety policy.
- Staff are responsible for checking the content and the appropriateness of any websites they post links to.
- Staff must be aware that all messages/tweets can be seen by anyone accessing the Twitter platform.
- Staff members should not enter into dialogue with anyone through Twitter.

COMMUNICATIONS

A wide range of rapidly developing communications technologies have the potential to enhance learning. This section details the technologies the school currently allows the use of and the manner in which they should be used.

E-Mail

- All staff will be provided with a school email address, which is to be used solely for communication regarding their job. Users need to be aware that email communications may be monitored. You should only use your email address to register to website that are of an educational basis and not for personal social media sites.

- The school regularly communicates with the staff through email. It is therefore expected that staff check their email daily.

- Staff may only access personal email before 8.30am and after 3.30pm or during PPA time. This rule must be adhered to when on the school premises regardless of the device that is being used.

- Emails and attachments: should only be opened if they are from known sources and never on personal email.

- All users must immediately report, to the ICT Coordinator, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

- Parents may use the admin email address to contact members of staff. Parents may contact staff using their school email address if appropriate but staff are under no obligation to reply and should send an out of hours email or request they be contacted through the school admin email address. If the response to the email is presenting simple facts (times of swimming lessons) then an email response is permitted, via the office, but a blind carbon copy (bcc) of the email must be sent to head@mauldethroad.manchester.sch.uk Is this necessary? I'm not sure it is especially if all work emails can be monitored.

- Staff should be aware that under the freedom of information act all emails are subject to disclosure (to any party) and can be used in a court of law if required.

- Any digital communication between staff and pupils must be professional in tone and content. These communications may only take place on official (monitored) school web applications and messages should not be private. The use of any other form of digital communication (including personal accounts) is strictly prohibited.

- Pupils are taught about email safety issues, such as the risks attached to the use of personal details. They are taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

Mobile Phones

Children are prohibited from using mobile phones within school. In exceptional circumstances, the school may allow pupils to bring a mobile phone to school, which needs to be left in the school office. If parents/carers wish their children to bring a mobile phone to school, they must request this in writing and understand that the school accepts no responsibility for any damage that may occur to these phones while in the school's possession.

Although mobile phones are an essential personal communication tool, they also provide a distraction for both staff and pupils. To minimise the disruption to learning, all teaching staff (teachers, teaching assistants) need to follow the rules below.

- Mobile phones should be switched off or to silent and placed out of sight during teaching times, regardless if you are working with pupils or preparing resources.

- Personal phone calls should only be made before school, during PPA, at break and lunchtimes, or after school and should take place in the staffroom or an empty classroom.

- Members of staff should not walk around school using their mobile phone.

- While the use of the mobile internet network is allowed, staff must only access websites, and website-based apps that are consistent with the rules set out in this document. If a member of staff needs to leave his/her mobile phone on because he she is expecting an urgent phone call, he/she must inform their team leader before doing so.

UNSUITABLE/INAPPROPRIATE ACTIVITIES

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyberbullying are also banned and could lead to criminal prosecution.

There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on, materials, remarks, proposals or comments containing or relating to:

- Child sex abuse images
- Promotion or conduct of illegal acts
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminal racist material in the UK
- Terrorists or extremist groups
- Pornography
- Promotion of any kind of discrimination
- Threatening behaviour, including the promotion of physical violence or mental harm
- Any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Running a private business
- Systems, applications, websites or other mechanisms that by pass the filtering or other safeguarding employed by the local authority or the school
- Uploading or downloading or transmitting commercial software or any copyrighted materials belonging to third party, without necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Personal social network sites
- Carrying out sustained downloading or uploading of files that causes network congestion and hinders others in their use of the internet
- Gambling sites
- File sharing

This list must be adhered to regardless of the device used to connect to the internet.

MONITORING AND REPORTING

In accordance with MSCB policy, the school will monitor its network regularly and consistently. All users will be made aware of this through the AUP. The ICT co-ordinator will maintain an incident log of e-safety incidents, including cyber-bullying that include:

- A description of the event
- Details of people involved
- How the incident was identified
- What actions were taken
- Conclusion of the incident

RESPONDING TO INCIDENTS OF MIS-USE

All members of the school community should be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

Any breach of the E-Safety policy will be responded to in accordance with the Incident Response Form and will be recorded in the school's e-safety log. In situations where the pupils have been the perpetrators, the school will use the consequences set out in its behaviour policy in addition to any other sanctions. In the event of a serious breach of the E-Safety policy, a full review of the E-Safety and Acceptable Use policies and procedures will be conducted as soon as possible by the headteacher and ICT co-ordinator.

Appendix A

Mauldeth Road Primary School

ICT Acceptable use policy

Introduction

Mauldeth Road Primary School recognises the importance of ICT in education and the needs of pupils to access the computing facilities available within school for their studies. This policy outlines our purpose in providing e-mail facilities and access to the internet and explains how our school is seeking to avoid the potential problems that unrestricted internet access could give rise to.

- This policy has been developed to ensure that all adults in Mauldeth Road Primary School are working together to safeguard and promote the welfare of children and young people.
- E Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of E safety at all times, to know the procedures and to act on them.
- When new technologies are brought into the school we will consider any dangers or concerns to the children and act accordingly.

Ethos

It is the duty of the school to ensure that every child and young person in its care is safe. The same staying safe outcomes and principles outlined in 'Every Child Matters' apply equally to the digital and virtual world.

All staff have a responsibility to support E safe practices in school and all pupils need to understand their responsibilities in the event of deliberate attempts to breach e safety protocols.

E safety is a partnership concern and is not limited to school premises, school equipment or the school day.

Teaching and Learning

Internet access in school

The purpose of Internet access in schools is to raise educational standards, support work of staff and enhance the school's management, information and business administration systems.

Teachers and pupils will have access to web sites worldwide (including museums and art galleries) offering educational resources, news and current events.

In addition, staff will have the opportunity to access educational materials and good curriculum practice; to communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the Lea and DfEE and receive up to date information to aid their teaching.

Parents' attention will be drawn to the rules for internet safety by letter and will be able to access this on the school website thereafter.

Ensuring Internet use is appropriate and safe

In common with other media such as magazines, books and video, some material available on the Internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter, upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- **Our internet access has a filtering system which prevents access to material inappropriate for children.**
- **Children using the internet will be working in the classroom or computer suite and will be under the supervision of an adult at all times.**
- **Staff will use their professional judgement and check that sites pre-selected for pupil use are appropriate to the age and maturity of pupils.**
- **Our rules for Responsible Internet Use are posted near all computers with Internet access.**
- **The ICT coordinator will ensure that occasional checks are made on files to monitor compliance with the school's Acceptable Use Policy.**
- **Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice for the Lea, our internet provider and the DfEE.**

A most important element of our Rules of Responsible Internet Use is that pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving the children is taken by the ICT coordinator and the Child Protection Officer in consultation with the Head Teacher and the pupil's class teacher. All teaching staff will be made aware of the incident at a Staff meeting if appropriate.

- **If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school has aims to work with parents/ carers to resolve any issue.**
- **If staff or pupils discover any unsuitable sites the ICT coordinator will be informed. The ICT coordinator will report the URL and content to the Internet Service provider. If it thought that the material is illegal, the site will be referred to the Internet Watch Foundation and the police.**

Maintaining the security of the school ICT network

Security is maintained by separate teacher/student log on and by updating virus protection.

Using the Internet to enhance learning

Access to the Internet is a planned part of the curriculum that enriches and extends learning activities and is integrated into the class schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

I have read the school's E-Safety policy and understand the terms on which I am able to use You Tube with my class and on the school premises.

Different ways of accessing information from the Internet are used depending upon the nature of the material being accessed and the age of the pupils:

- **Access to the internet may be by teacher (or other adult) demonstration**
- **Pupils may access teacher prepared materials, rather than open an internet site.**
- **Pupils may be given a suitable internet page or single web site to access.**
- **Pupils may be provided with lists of relevant and suitable web sites which they may access.**
- **Pupils are expected to observe the rules of responsible Internet use (Think then click) and are informed that checks can and will be made of files held on the computer and sites they access.**
- **Pupils will be educated in taking responsibility for their own Internet access.**

Using information from the Internet

- Pupils are taught to expect and wider range of context, both in level and in audience, than is found in the school library or on TV.
- Teachers ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that it is even more important when considering information from the Internet.
- When copying things from the Web, pupils are taught to observe copyright.
- Pupils are made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Using e-mail

Pupils learn how to use an e-mail application and are taught e-mail conventions. Staff and pupils use e-mail to communicate with others, to request information and to share information.

- Pupils are only allowed to use e-mail once they have been taught the rules of responsible internet use and the reason for these rules.
- Teachers endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail.
- Pupils may send e-mail as part of a planned lesson, but will not be given individual e-mail accounts unless it is part of a taught topic. They will not have access to these email accounts outside school.
- Incoming e-mail to pupils will not be regarded as private and should not be opened unless the author is known.
- Children will have the e-mail messages they send checked by a member of staff before they send them.
- The forwarding of chain letters will not be permitted.
- Pupils are not permitted to use e-mail at school to arrange to meet someone outside school hours.
- Personal email or messaging between staff and pupils should not take place.

Mobile phones and notebooks

Pupils are not permitted to use mobile phones or other personal mobile technologies in school. If a pupil brings a mobile phone into school it must be handed to a member of staff immediately. If inappropriate material is sent to a pupil, it must be reported immediately to a member of staff within the school.

Staff mobile phones should be switched off or to silent and placed out of sight during teaching times, regardless if you are working with pupils or preparing resources.

Personal phone calls should only be made before school, during PPA, at break and lunchtimes, or after school and should take place in the staffroom or an empty classroom.

Members of staff should not walk around school using their mobile phone.

While the use of the mobile internet network is allowed, staff must only access websites, and website-based apps that are consistent with the rules set out in this document. If a member of staff needs to leave his/her mobile phone on because he she is expecting an urgent phone call, he/she must inform their team leader before doing so.

Social networking

Pupils will not be allowed access to any social networking sites within school. They will be given guidance as to the problems and dangers of these sites when and if they use them outside school time. Staff are strongly advised that they should not accept direct requests from pupils or parents to join them on social networks and should avoid any direct internet-based or social networking contact with children outside of school.

The school strongly discourages parents from allowing their children to fabricate their birthdates in order to join age restricted social media sites as this poses a serious safeguarding risk.

The school uses Twitter as an additional tool to promote parental engagement by sharing photos and information about events, activities and successes of the pupils. Examples of the use so far: pictures of artwork completed by the class; pictures of classroom displays; pictures of children learning to ride bikes. I have read the school's E-Safety policy and understand the terms on which I am able to use Twitter for school use.

The Mauldeth Road Website

Our school Website is intended to:

- Provide accurate up to date information about our school
- Promote the school
- Allow current and prospective parents to view the school ethos, curriculum and staff.

The point of contact on the web site will be the school address and telephone number and e-mail address. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from any individual before they are referred to by name on any pages we publish on our website.

Internet access and home/school links

Parents will be informed that children are provided with supervised Internet access as part of their lessons. We will keep parents in touch with future ICT developments by letter and newsletter.

Photographic, video and audio technologies.

Staff may use photographic or video technologies to capture and support school trips and appropriate curriculum activities. A record of pupils who are to be excluded from photographs and videos is kept in the school office.

Only school issue equipment may be used for taking photos or videos of the school children; staff should not use their own personal devices under any circumstances.

Introducing the policy to pupils

Responsible Internet use, covering both school and home use will be included in the ICT and PSHE curriculum. Pupils will be instructed in responsible and safe use before allowed access to the internet and will be reminded of the rules and risks before any lesson using the internet. Pupils will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately. Every child in school will watch an e-safety presentation with their class and teacher and then sign an e-safety contract. These are displayed in every classroom. **Please note that children new to the school who arrive half-way through the year should also watch this presentation**. These presentations are displayed clearly in the ICT suite.

Consulting Staff

It is essential that teachers and learning support staff are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies.

- All staff are governed by the school's Acceptable use statement and will have access to the School's ICT Acceptable use policy.
- All new staff will be made aware of the importance of the ICT Acceptable use policy.
- Staff development in safe and responsible use of the internet will be provided as required.
- Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential.
- Staff understand that use of the internet is for professional and not personal use.

iPads/Laptops/Cameras

Users Responsibilities

Users must use the protective covers/cases provided.

Users should not expose the devices to extreme heat or cold.

Do not store or leave unattended in vehicles.

It is a User's responsibility to keep their iPad, LapTop or camera safe and secure

The whereabouts of the devices should be known at all times.

Users may not photograph any other person without that persons' consent.

Please ensure that your device is used only by yourself and not by friends or members of your family.

These devices are subject to routine monitoring by Mauldeth Road Primary School. Devices must be surrendered immediately upon request by any member of staff.

iPads/Laptops and cameras should be used for **Education** purposes only.

Staff should set their own four digit security password on their iPads to protect confidentiality.

Free apps for the iPad may be downloaded, but should be educational in nature or for appropriate reinforcement, and only ever by staff.

Paid apps for the iPad may only be downloaded and administered by the school technician, with prior agreement from the head or co-ordinator.

If an iPad, LapTop or Camera is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen device

If an iPad, LapTop or Camera is lost, stolen or damaged the ICT co-ordinator must be notified immediately. The ICT co-ordinator will then notify the Head Teacher.

Prohibited Uses

Users are not allowed to send, access, upload download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

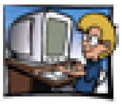
Inappropriate media may not be used as a screensaver or background photo.

Use school email addresses and school itunes accounts – do not use personal email or personal itunes accounts on your devices.

Appendix B

Internet Safety Agreement
For KS1 pupils

I will not give out my name, address, telephone number, email address or school to anyone online without first checking with a grown up.



I will tell a grown up straight away if I see or hear anything which makes me feel uncomfortable when online.

I will never agree to get together with someone I 'meet' online.

I will only go on websites that my teacher, parent or carer have agreed to.

I know that not everything I see online is true!

I will not give out any passwords to anyone (even my best friend) except my parents or carers.

Appendix C

Internet Safety Agreement
For KS2 pupils

I will not give out my name, address, telephone number, email address or school to anyone online without first checking with an adult.

I will tell my teacher, parent or carer straight away if I see or hear anything which makes me feel uncomfortable when online.

I will never send a person my picture or anything else without checking with an adult first.

essential e-safety

I will never agree to get together with someone I 'meet' online.

I will not respond to any messages which are mean or in any way make me feel uncomfortable. It is not my fault if I get messages like that. I will tell an adult straightaway.

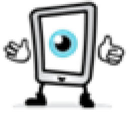
THINK U KNOW

I will only go on websites that my teacher, parent or carer have agreed to and understand that rules should be in place to limit the amount of time I spend on the computer/tablet or using my mobile phone.

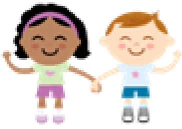
I will not give out any passwords to anyone (even my best friend) except my parents or carers.

I understand what it means to be a good online citizen and I will not do anything that could hurt other people and their feelings or break the law.

I will check with an adult before downloading or installing software which could possibly hurt our computer or mobile device.

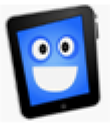


I am aware that the recommended age to be using social networking sites is at least 13 years of age.



When I am using the iPads, I will only use apps and websites that my teacher has asked me to.

I will never change the settings on the iPad unless my teacher asks me to.



I understand that 'Copyright' is a form of protection given to the authors or creators of photos, pictures, literary or dramatic works. What that means is that the author of the work has the right to do any of the following, make copies of that work, distribute copies of that work, perform that work or display that work publicly.

© All Rights Reserved

..... But you I don't necessarily have that right!

I will help my parents understand how to have fun and learn things online and teach them new things I have learned about the internet, computers and other technologies.