Moss Park Junior School

E-Safety Policy

Consulted on: Oct –Feb 2009

Ratified: March 2009

To be reviewed: Summer 2012

Ratified: Dec 3rd 2012

To be Reviewed Autumn 2015

Ratified: February 2016

To be reviewed: Spring 2017

To be read in conjunction with the following policies:

Behaviour Policy

Child Protection Policy

Computing/ ICT Policy

Data Protection Policy

Safeguarding Policy

***This policy has been reviewed with regard to the Disability and Safeguarding policy, and in l*ight of the Prevent and CHANNEL guidance and school's Safeguarding Policy.**

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

Websites

E-mail and Instant Messaging

Social Media

Mobile/ Smart phones with text, video and/ or web functionality

Other mobile devices with web functionality

Gaming, especially online

Learning Platforms and Virtual Learning Environments

Blogs and Wikis

Podcasting

Video Broadcasting

Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At Moss Park Junior School we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and

pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please speak to the Head Teacher.

All internet activity is logged by the school's internet provider. These logs may be monitored by authorised Trafford Council staff.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Behaviour Policy and where appropriate, the Trafford LA Disciplinary Procedure or Probationary Service Policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's Head Teacher. Additionally, all security breaches, lost/stolen equipment or data (including USB pens), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head Teacher.

Please refer to the section Incident Reporting, E-Safety Incident Log & Infringements.

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick, must be checked for any viruses using school provided anti-virus software before being used. Please see the ICT coordinator to do this.

Never interfere with any anti-virus software installed on school ICT equipment that you use.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately (via a ticketing system). The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Email

The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, pupil email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette; 'netiquette'.

Managing e-Mail

- The school has one central email account to use for all school business. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. The Head Teacher and Computing teacher also have their own school email account.

- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school office email account should be the account that is used for all school business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses, unless discussed with the Head Teacher.

- Staff sending emails to external organisations, parents or pupils should send this from the main admin email account.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes

- Emails created or received as part of your school job (in the office) will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account as follows:

  - Delete all emails of short-term value
  - Organise email into folders and carry out frequent house-keeping on all folders and archives

- All pupil email users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail

- Staff must inform the Head Teacher if they receive an offensive e-mail

- Pupils are introduced to email as part of the Computing Programme of Study

- However you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply

Sending e-Mails

- If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to 'Managing Email' section above. This must **only** be sent via the admin email account to allow encryption.

- Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate

- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments

Receiving e-Mails

- Never open attachments from an untrusted source; Consult your network manager first if unsure

- Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder

Emailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using email - emailing confidential data is not recommended and should be avoided where possible.

Where your conclusion is that email must be used to transmit such data:

Exercise caution when sending the email and always follow these checks before releasing the email:

- Verify the details, including accurate email address, of any intended recipient of the information

- Verify (by phoning) the details of a requestor before responding to email requests for information

- Do not copy or forward the email to any more recipients than is absolutely necessary

Equal Opportunities

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' E-Safety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

E-Safety

E-Safety - Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-Safety co-ordinator in this school is Mrs Stallman who has been designated this role as Head Teacher. All members of the school community have been made aware of who holds this post. It is the role of the E-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as Trafford LA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and governors are updated by the Head/ E-Safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHCE.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the E-Safety curriculum

- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum (such as Year 3 Roman research topic)

E-Safety Skills Development for Staff

- Our staff receive regular information and training on E-Safety and how they can promote the 'Stay Safe' online messages in the form of INSET training and updates, and the e-safety policy

- New staff receive information on the school's acceptable use policy as part of their induction

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community

- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas

Managing the School E-Safety Messages

- We endeavour to embed E-Safety messages across the curriculum whenever the internet and/or related technologies are used

- The E-Safety policy will be introduced to the pupils at the start of each school year

- E-Safety posters will be prominently displayed

- The key E-Safety advice will be promoted widely through class activities

Incident Reporting, E-Safety Incident Log & Infringements

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Head Teacher. Additionally, all security breaches, lost/stolen equipment or data (including USB pens), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Head Teacher.

Misuse and Infringements

Complaints
Complaints and/ or issues relating to E-Safety should be made to Head Teacher. Incidents should be logged in the school's E-Safety Incidents Log.

Inappropriate Material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety co-ordinator
- Deliberate access to inappropriate materials by any user will lead to the incident being logged in the class teacher's Concerns File, depending on the seriousness of the offence; investigation by the Head Teacher/ LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Users are made aware of sanctions relating to the misuse or misconduct through teaching in lessons involving ICT

Internet Access

The internet is an open worldwide communication medium, available to everyone at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity

- Staff will preview any recommended sites before use

- Raw image searches are not allowed for Lower School (Year 3 and 4). Google Custom Search can be used to minimise risk of unsuitable material for these year groups. Year 5 and 6 may search for images, however, search terms should always be discussed with the children, as well as behaviour if something undesirable is found.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

Internet Use

You must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience

Do not reveal names of colleagues, pupils, others or any other confidential information acquired through your job on any social networking site or other online application.

On-line gambling or gaming is not allowed in school or on school equipment

Infrastructure

- Trafford Local Authority has a monitoring solution where web-based activity is monitored and recorded

- School internet access is controlled through the LA's web filtering service.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required

- The school does not allow pupils access to internet logs

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed, the incident reported immediately to the class teacher, and the Head Teacher must be informed immediately.

- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines

- Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems.

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT coordinator or technician

- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the school's 'ticketing system' immediately (see ICT Policy).

Managing Other Web Technologies

Online technologies including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities, for example YouTube. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny individual access to social networking and online games websites (non educational) to pupils within school
- All pupils are taught to be cautious about the information given by others on such websites, for example users not being who they say they are
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests)
- If applicable, our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals
- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online
- Our pupils are asked to report any incidents of Cyberbullying to their parents/ carers. This can also be reported to school
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school blog site or other systems approved by the Head Teacher
- Parental Involvement - We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities.
- Parents/carers are asked to read through and countersign acceptable use agreements on admission of their child to the school
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school blog)
- Parents/carers are expected to sign a Home-School agreement
- The school disseminates information to parents relating to E-Safety where appropriate in the form of;

- Posters
- School website
- Newsletter items

Radicalisation and Extremism

Safeguarding against radicalisation and extremism is part of schools existing Safeguarding Policy.

We understand that parental attitude can influence child behaviour and we have support structures in place to allow for non-confrontational supportive discussions with individual parents relating to any particular issues e.g Parents' Information Meeting on Keeping Children Safe on-line, Parents' Evening, Drop-Ins.

Staff and pupils are encouraged to use critical thinking with all online content and are taught these skills through the wider curriculum and Staff Training.

Staff, pupils and parents are involved in monitoring of online content e.g. school Blog Site

Staff and pupils know how to raise concerns and be sensitive in their own on-line conduct and discussion around radicalisation and extremism have been incorporated into the PSHE curriculum and provision for Fundamental British Values as appropriate.

All school policies will be reviewed on an on-going basis and Prevent actions included where considered appropriate.

Passwords and Password Security

Passwords

Always use your own personal passwords where applicable

Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures

Staff should change temporary passwords at first logon

Change passwords whenever there is any indication of possible system or password compromise or approximately every 6 weeks if sooner.

Do not record passwords or encryption keys on paper or in an unprotected file

Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished

Never tell a child or colleague your password

If you are aware of a breach of security with your password or account inform the ICT Coordinator immediately

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT Coordinator

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords for their individual log ins which are not shared with anyone. Staff are regularly reminded of the need for password security.

- All pupils, staff and visitors read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's E-Safety Policy and Data Security

- Staff are provided with an individual blog log-in username and separate username to access the school network. They are expected to use a personal password and keep it private

- Pupils are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others unless specified by a teacher

- Upon entry to the school, pupils will be given their own log on to the school system. Passwords should be recorded and help by the class teacher and pupils should keep these private. The technician should be informed via ticketing if the password needs to be replaced.

- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and blog site, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

- In our school, all ICT password policies are the responsibility of the ICT coordinator or ICT technician and all staff and pupils are expected to comply with the policies at all times

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with **school** equipment

Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Head Teacher.

Upon leaving Moss Park Junior School, teachers should permanently delete images of pupils no longer attending this school.

Publishing Pupil's Images and Work

On a child's entry to Moss Park Juniors and subsequent years, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school blog site
- on the school Twitter account
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas
- in display material that may be used in external areas, ie exhibition promoting the school
- general media appearances, eg local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

- This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, eg divorce of parents, custody issues, etc.
- Parents or carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be published alongside their image and vice versa. Email and postal addresses of pupils will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/ films of children are stored on the school's network in the 'Media' drive with is securely stored on our school network.

Pupils are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher. Staff should only do so if using a school encrypted USB drive and has been approved by the Head Teacher.

Rights of access to this material are restricted to the teaching staff and teaching assistants within the confines of the school network.

Webcams and CCTV

We do not use publicly accessible webcams in school

Webcams in school are only ever used for specific learning purposes, eg. Interaction with a class abroad or monitoring a bird's nest

Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document)

- Webcams can be provided by the ICT coordinator
- Consent is sought from parents/carers and staff on joining the school, in the same way as for all images

Video Conferencing

Permission is sought from parents and carers if their children are involved in video conferences

Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school

All pupils are supervised by a member of staff when video conferencing

All pupils are supervised by a member of staff when video conferencing with end-points beyond the school

The school keeps a record of video conferences, including date, time and participants.

Approval from the Headteacher is sought prior to all video conferences within school

The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

Additional points to consider:

Participants in conferences offered by 3rd party organisations may not be CRB checked

Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

School ICT Equipment including Portable & Mobile ICT

Equipment & Removable Media

School ICT Equipment

As a user of the school ICT equipment, you are responsible for your activity.

School log serial numbers as part of the inventory and cameras, microphones and laptops are monitored through a log book/ timetable.

Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.

Ensure that all ICT equipment that you use is kept physically secure and locked in the ICT store cupboard when not in use.

Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

It is imperative that you save your data on a frequent basis to the school network. You are also responsible for the backup and restoration of any of your data to password protected portable media devices provided by school.

Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick, or other portable device.

Privately owned ICT equipment should not be used on a school network.

On termination of employment, resignation or transfer, return all ICT equipment to your Head Teacher.

It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person or saved on this equipment.

All ICT equipment allocated to staff must be authorised by the ICT coordinator or Head Teacher. Teaching Staff are responsible for returning equipment when no longer needed.

All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

Staff must ensure that all school data is stored on the school network, and not kept

solely on the laptop.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. Staff should not have any ICT equipment belonging to school at home unless approved by the Head Teacher.

Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

Portable equipment must be transported in its protective case.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as, Smartphones, Blackberries, iPads, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.

Pupils are not allowed to bring personal mobile devices/phones to school unless permission is given by the Head Teacher.

The school is not responsible for the loss, damage or theft of any personal mobile device.

School Provided Mobile Devices (including phones)

Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

Ensure that any School information accessed from your own PC or removable media equipment is kept secure.

Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared photocopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.

You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information

Using Removable Media

Store all removable media securely.

Securely dispose of removable media that may hold personal data.

Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

Social Media, including Facebook and Twitter

- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- Pupils are not permitted to access their social media accounts whilst at school.

- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law.

Writing and Reviewing this Policy

Review Procedure

There will be on-going opportunities for staff to discuss with the E-Safety Leader any E-Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the SIRO/AIO any issue of data security that concerns them.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended and approved by the staff, head teacher and governors in Autumn 2015.

APPENDIX 1:

Pupil Acceptable Use – Year 3 and Year 4
Agreement / E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address when the teacher says, (only accessible within school)
- ✓ I will only open/delete my own files.
- ✓ I will keep my usernames and passwords secure.
- ✓ I will make sure that I am responsible, polite and sensible when contacting people on electronic devices.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately and turn my screen off.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my E-Safety.
- ✓ I will report anything that I think is wrong or has upset or worried me, to a member of staff, Mrs Stallman, a friend or family member. I also know I can report any bad behaviour or thing that upsets me to the Police, CEOP website or by pressing the report button on the school blog site.

Pupil Signature:

I have read the Internet guidelines and promise to follow these, to make sure ICT use is safe and secure throughout Moss Park Junior School:

Full Name ……..…….…… Date …… Class……..

Counter Signature:

I have discussed these guidelines with the pupil named above and will work with the school to adhere to these guidelines in order to ensure safety online and correct use of ICT equipment:

……..Date……

Relationship to Child……

Pupil Acceptable Use – Year 5 and Year 6
Agreement / E-Safety Rules

- ✓ I will only use ICT in school for school purposes.
- ✓ I will only use my class email address when the teacher says, (only accessible within school)
- ✓ I will only open/delete my own files.
- ✓ I will keep my usernames and passwords secure.
- ✓ I will make sure that I am responsible, polite and sensible when contacting people on electronic devices.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately and turn my screen off.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community.
- ✓ I know that my use of ICT can be checked and that my parent/ carer will be contacted if a member of school staff is concerned about my E-Safety.
- ✓ I will report anything that I think is wrong or has upset or worried me, to a member of staff, Mrs Stallman, a friend or family member. I also know I can report any bad behaviour or thing that upsets me to the Police, CEOP website or by pressing the report button on the school blog site.

Pupil Signature:

I have read the Internet guidelines and promise to follow these, to make sure ICT use is safe and secure throughout Moss Park Junior School:

Full Name ……..…….…… Date …… Class……..

Counter Signature:

I have discussed these guidelines with the pupil named above and will work with the school to adhere to these guidelines in order to ensure safety online and correct use of ICT equipment:

…….Date……

Relationship to Child……

APPENDIX 2: Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the ICT co-ordinator or Head Teacher.

- I will only use the school's email / Internet / Intranet / Blog and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will only use encrypted USB devices purchased by school when transferring data.
- I will not install any hardware of software without permission of the ICT Co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I understand that all my use of the Internet and other related technologies can be monitored and logged by the Local Authority and can be made available, on request, to the Head Teacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school:

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

APPENDIX 3: BLOG, DIGITAL IMAGE AND INTERNET PERMISSION FORM

Moss Park Junior School
Moss Park Road
Stretford
Manchester
M32 9HR
Tel: 0161 864 1710
Fax: 0161 864 1723
Email: mossparkjun.admin@trafford.gov.uk
Website: www.mossparkjun.net
Twitter: @MossParkJnrs

Head Teacher: Mrs. K. Stallman, B.Ed.(Hons), NPQH, LLE

Dear Parents/ Carers,

Please find attached a number of permission sheets for you to read, sign and return to school as soon as possible.

Photographs and Videos

During the school year there are occasions where photographs of your child may be taken by staff at Moss Park Junior School and other educational visitors. These photographs enable us to showcase the many exciting activities that take place within school. Photographs are displayed around school, in Moss Park Junior School publications, the School website and on the School Twitter account. We are very careful of what we display, never using the child's full name. We are also very grateful to the sensible way in which photos are used when taken by parents in school.

In order for us to use these photographs we request your permission. We will, of course, respect the wishes of any parent who does not give consent and a meeting with me will be necessary to discuss the child appearing on class photographs etc.

School Website

Our school website is a popular place where children, teachers, parents and the wider community can leave their comments and interact with each other. It is a great way for us all to communicate and provides an excellent opportunity for parents to see what is happening in school. All comments go to teachers who read and vet each one first. Nobody can leave a comment directly on the site without this taking place.

School has many procedures in place to ensure the safety of our pupils. We ask that you discuss the attached User Agreement with your child and for you both to sign the form to acknowledge these guidelines have been shared.

Internet Use

Accessing specific learning materials and learning about the Internet is now a statutory requirement and part of the National Curriculum. We have Local Authority firewalls, prohibited sites and school security settings in place. Facebook, YouTube and other sites are prohibited and cannot be accessed by the children. No child is allowed to use a computer unsupervised and we have everything in place with regard to the Internet and its use in school. Obviously, nothing is 100% guaranteed but we have real trust in our security systems and replicate what any reasonable, caring parent would do at home.

If you have any concerns, please do not hesitate to contact me.

Yours sincerely,

Mrs K. Stallman

Images and Video Permission Form

These forms will cover the period that your child attends our school.
Please complete each section and return to your child's class teacher.

The School will:

- Use any images that have been taken in the appropriate manner.
- Not give full names on photographs
- Ensure that images are securely stored in school and used only by those authorised to do so.
- Permanently delete these images when they are no longer required.

Please delete the appropriate paragraph:

I DO CONSENT to digital images and videos of my child being dispayed in Moss Park Junior School publications, such as the school prospectus or website. I understand that the images will be used for educational purposes only.

I DO NOT CONSENT to digital images and videos of my child being dispayed in Moss Park Junior School publications, such as the school prospectus or website.

Pupil's Name:

Parent/ Carers Signature:	Date:

Current Legislation

Acts Relating to Monitoring of Staff eMail

Data Protection Act 1998

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice)

(Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

Other Acts Relating to E-Safety

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

access to computer files or software without permission (for example using another persons password to access files)

unauthorised access, as above, in order to commit a further criminal act (such as fraud)

impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Acts Relating to the Protection of Personal Data

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 200

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx