MEON INFANT SCHOOL

E-SAFETY POLICY

This policy replaces the previous 'Internet Access Policy'. It has been developed to cover aspects of internet usage (as the previous policy did) but also to cover aspects of modern technology and ICT guidance which have been introduced since the previous policy was developed (access to social networking sites, guidance on storage of pupil information etc).

1. INTRODUCTION

The school makes widespread use of modern technology in the belief and understanding that it can develop and enhance many aspects of teaching and learning, as well as providing a preparation for life in a society where the use of ICT is widespread.

The statutory curriculum expects pupils to learn how to locate, retrieve and exchange information using ICT.

This policy:

- applies to all users of ICT equipment, in its widest sense, whilst on school premises. It also applies to anyone who uses school ICT equipment, software or electronic data whilst off the premises.
- forms part of the school's ICT subject policy.
- relates to other school policies including, child protection, behaviour and bullying.

2. E-SAFETY

The increased use of technology at work and at home exposes people to a number of risks and dangers. In its simplest form e-safety is about ensuring that adults and children use electronic technologies in a way which will keep them safe without limiting their opportunities for creation and innovation.

The Internet is a wonderful resource but it can also be dangerous. It is important to protect people through the access that they are given but it is also vital to equip them with the skills to handle this technology safely.

E-safety is also about protecting the hardware and software we use from attack by unscrupulous people, who may wish to cause disruption or commit illegal acts.

E-safety is also about protecting electronic data, our private, personal data and that of other people.

3. RESPONSIBILITIES

Everyone who uses ICT connected with the school has a responsibility to have a regard for e-safety. It is NOT just the remit of the Head teacher and ICT/E safety Coordinator.

The Government has placed a responsibility on the Governors and Management of the school to ensure that all employees and pupils are aware of e-safety concerns and procedures, and that they receive training to raise their awareness of the issues involved.

The teaching staff have a responsibility, as part of the statutory requirements of the curriculum, to teach e-safety.

3.1. The E-Safety / ICT Coordinator will

- oversee the development/review of this policy
- oversee the implementation of this policy
- advise the school management on e-safety issues
- advise staff on e-safety teaching and learning resources
- be a point of contact for anyone connected with the school who has questions or concerns about e-safety issues
- be available to deal with general issues of e-safety that are not specific complaints concerning individuals
- be available to deal with minor infringements of the e-safety policy and rules, including accidental infringements
- pass on to the Headteacher any complaint or evidence received concerning individual pupils or staff misuse of ICT

Staff who manage the filtering systems or monitor ICT use will be supervised by a member of the senior management team and work to clear procedures for reporting issues, testing filtering restrictions and checking security systems.

4. TEACHING AND LEARNING

Why the Internet and Digital Communications are important:

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use enhances children's learning

The school Internet access will be specifically tailored for pupil use and will include filtering appropriate to the age of pupils.

Pupils will be taught what Internet use is acceptable and what is not and they will be given clear rules for internet use.

5. EQUAL OPPORTUNITIES

The school believes that it is essential that opportunities are provided for everyone to access ICT, regardless of gender, race, religion, culture, ethnic group, physical ability or mental ability.

6. SPECIAL NEEDS

ICT can be a positive tool for children with Special Educational Needs. Access to the Internet is, therefore, a vital link with which communication to the outside world can be achieved. Access to the Internet can also stimulate children to develop their ideas independently.

The school will endeavour to ensure that children with Special Educational Needs are made aware of the risks and dangers of using ICT, within their understanding and abilities. The ICT Co-ordinator will make appropriate resources available to facilitate this.

7. MANAGING SCHOOL NETWORK ACCESS

The school will maintain two network systems under the control of two separate file Servers - admin (school administration network) - curriculum.

The E safety Co-ordinator/Headteacher will oversee the use of the admin network.

The ICT Co-ordinator will have responsibility for the administration of the curriculum network with help and guidance from the ICT technician.

Security strategies will be implemented according to guidance from PCC.

Full access to the admin network will be restricted to senior management and office staff. Other employees may be allowed limited access to this network for specific tasks, at the discretion of the Headteacher.

Levels of access to the admin network will be enforced through unique usernames and passwords.

The admin network will be the only network to contain the full details of all employees and pupils. SIMs etc.

All staff and pupils of the school will be allowed access to the curriculum network.

Staff will have their own username and unique password in order to use the curriculum network. They will be allocated their own file space and have access to a shared “staff only” area of the network, which the pupils will not be able to access. Staff will also be able to access all pupil folders.

Children will not be allowed access to computer equipment at playtimes and lunchtimes unless a member of staff is present in the room.

Parents, visitors, guests and supply staff may be granted restricted access to the curriculum network, with permission from the Headteacher or ICT Co-ordinator, through the use of special usernames and passwords.

Contracted I.C.T. technicians may be given full access to either network, at the discretion of the Headteacher.

Only the ICT Co-ordinator, computer technicians, or other persons nominated by the Headteacher, may install software on any school workstation or server.

8. MANAGING INTERNET ACCESS

The Internet Service Provider for the school will be PCC.

Staff must adhere to the school’s ‘Acceptable Use Policy – staff’ when accessing the internet. (Appendix A)

Foundation and key stage 1 pupils’ access to the Internet will be by adult demonstration with directly supervised access to specific, approved, on-line materials.

Foundation and key stage 1 pupils will be closely supervised by an adult when accessing materials using the Internet.

Pupils will adhere to the school’s document ‘Rules for using the internet’ whilst accessing materials online.

Pupils will not be allowed to access the internet other than through the school website pupil zones.

9. MANAGING ACCESS TO E-MAIL

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Teachers should consider how e-mail from pupils to external bodies is to be presented and controlled before allowing it.

The forwarding of chain letters or anonymous mail is not permitted.

Staff will have access to e-mail through their Google Meon Infant account.

Staff may only access a private or home e-mail account on school premises outside normal timetabled hours. However, this should be kept to a minimum and staff should follow the school's 'Acceptable Use of ICT – Staff' document when doing so. The Headteacher reserves the right to withdraw this arrangement at any time.

Staff should inform the Headteacher if they receive an offensive e-mail.

Pupils will not be allowed access to individual e-mail accounts on school premises. The only email that children will encounter will be directly related to curriculum activities and operated with complete supervision of a member of staff i.e. sending a class email to a different school in order to share or gather information.

10. MANAGING OTHER TECHNOLOGIES

Published content and the School Website

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or Headteacher.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

All material published on the school website must be the author's own work. If material from other sources is included credit should be given to the original author, stating clearly the source of such work and must not break copyright laws.

Pupils 'full' names will not be used anywhere on the school website, particularly in association with photographs.

Pupil image file names will not refer to the pupil by name.

Written permission from parents or carers will be obtained before photographs of individual pupils are published on the school website.

Parents will be clearly informed of the school policy on image taking and publishing.

Social Networking and Personal Publishing

Pupils will not be allowed to access social networking sites, instant messaging sites or chat rooms, on school premises.

Pupils will not be allowed access to YouTube or similar websites on school premises apart from those found and shown by a member of staff in order to support the curriculum.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Members of staff must not access social networking sites during normal timetabled hours.

Staff will not allow pupils to name them in any “friends” or contacts list on a social networking site, unless they are actually a relation of the pupil.

Staff will not add pupils to their own “friends” or contacts list on a social networking site, unless they are actually a relation of the pupil.

See also Staff/Governors Confidentiality Statement (Appendix B)

Webcam will only be used under the direct supervision of a member of staff.

Mobile Phones

All staff should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Pupils are not allowed to use mobile phones, or technologies built in to a mobile phone, on school premises or during school activities off-site.

Staff should not use their own mobile phone to capture photographs of pupils.

Staff should not use their mobile phones during their working hours. In case of emergency permission should be gained from the Headteacher. If contact is required the school’s main line system should be used.

Digital Cameras

It should be noted that there are risks to allowing the capturing digital images on the school premises. It is easy for anyone to manipulate digital images, using modern software, and put them to inappropriate uses.

It should be noted that digital cameras can be used to spread computer viruses, in a similar way to memory sticks.

Staff and pupils may use digital cameras belonging to the school, as part of the curriculum, to provide evidence or as a record of work.

Staff should not capture images of pupils on personal digital cameras. Staff who do so would put themselves at risk should a pupil or parent bring a complaint against them. It would be harder to prove that the images were taken for school purposes, especially if the images were taken home on the camera.

Digital copies of images of staff or pupils must not be e-mailed or given to someone outside the school premises without permission from the Headteacher.

Images taken with a school digital camera should be kept in the cameras memory, or on the memory card, for as short a time as possible and then be deleted. Images should not be stored on a camera for long periods and certainly not indefinitely.

Pupils should not be allowed to use personal digital cameras on the school premises unless permission is granted by the Headteacher for a specific use, and only then under close supervision and with great care.

If sanctioned by the Headteacher, pupils will be allowed to use personal cameras on a school activity off the premises. Close supervision would be essential and limits should be explained to the pupils.

Laptops

When on the school premises, pupils may only use laptops provided by the school. They are not allowed to bring personal laptops on to school premises.

Staff provided with a laptop purchased by the school can only use it for private purposes at the discretion of the Headteacher. Such laptops remain the property of the school and are open to scrutiny by senior management, contracted technicians and the ICT Co-ordinator.

Staff intending to bring personal/private laptops on to the school premises should consider very carefully if it is appropriate. There are security risks and also risks associated with any private content on the laptop.

Staff must not attach a personal/private laptop to an interactive whiteboard when children are present.

The security of school laptops is of prime importance due to their portable nature and their being liable to theft.

Wi Fi

There may be devices on the premises that use Wi Fi or other wireless connection. It is extremely important that such connections have the maximum possible security levels activated.

Staff should note that Wi Fi connections can be intercepted by unauthorized persons, depending on the range of the transmission and what security systems are activated.

Interactive Whiteboards (IWB)

Anyone using an IWB in school must follow the current guidelines for their safe use.

Emerging Technologies

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

Technologies not specifically covered by this policy can only be used on school premises at the discretion of the Headteacher.

AUTHORISING ACCESS

The final decision as to who can be granted access to school ICT equipment and facilities will rest with the Headteacher.

A nominated member of the senior management will be responsible for supervising access to the admin network.

The ICT Co-ordinator will be responsible for supervising access to the curriculum network and classroom ICT equipment.

All staff must read and sign the "Acceptable Use of ICT - Staff" document before using any school ICT resource.

Temporary staff and supply staff regularly used by the school will be granted access to the curriculum network, through being allocated their own username and password, and will read and sign the "Acceptable Use of ICT - Staff" document before using any school ICT resource.

Parents will be asked to sign and return a consent form concerning their child's use of the Internet as part of the 'Home School Agreement' when their children first start in Foundation Stage. (Appendix C)

PROTECTING PERSONAL DATA

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

Every member of staff must take all reasonable steps to securely protect all data concerning pupils and others.

Any data taken off the school premises should be kept to a minimum and if no longer required, deleted or destroyed in an appropriate manner, or returned to school for destruction.

All printed copies of personal data must be shredded before disposal as waste material.

There is a security/data protection risk when computer equipment is taken out of use and disposed of. Hard disks from computers should be adequately erased before machines are recycled, especially if being taken off the premises. Hard disks that have contained sensitive data (such as those from the admin network) should be destroyed rather than recycled.

Staff must take all reasonable care when using, storing and transporting memory sticks, CDs or DVDs containing school data.

Memory sticks provided by school must not be used for private purposes and remain open to scrutiny by senior management, contracted technicians and the ICT Co-ordinator.

Anyone transferring personal data from school sources to their own personal computer or memory stick is personally liable for the security of the data and for any legal consequences.

ASSESSING RISKS

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

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

The final decision when assessing risks will rest with the Headteacher.

HANDLING E-SAFETY COMPLAINTS

Complaints of ICT/Internet misuse will be dealt with by a senior member of staff, who will decide if any sanctions are to be imposed.

Any complaint about staff misuse must be referred to the Headteacher, who will decide if any sanctions are to be imposed.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Any complaint about illegal misuse must be referred to the Headteacher, who will decide if a referral to the police or other relevant authority is necessary, following any guidelines issued by Portsmouth City Council.

Sanctions for minor incidents could include:

- informing parents or carers, when a pupil is involved
- receiving a verbal warning, of which a record is kept
- receiving a formal written warning
- having network access denied for a specified period

Sanctions for other incidents, especially after warnings have been given, could include:

- informing parents or carers, when a pupil is involved
- having network access permanently revoked
- formal disciplinary action being taken against an employee

Staff should note that copies of illegal material they find should not be sent /forwarded to anyone else, even as evidence, as this could also be seen an committing an illegal act.

Do not e-mail copies of illegal material to the Headteacher, E-Safety Co-ordinator, Child Protection Co-ordinator, as receiving such material could also be seen as the committing of an illegal act on their part.

COMMUNICATING POLICY

Introducing the E-Safety Policy to Pupils

E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.

A programme of training in e-Safety will be developed, based on the materials from Childnet “Captain Kara”.

E-Safety training will be embedded within the ICT scheme of work.

Staff and the E-Safety Policy

All staff will be given the School E-Safety Policy and its importance explained.

Appropriate training will be arranged for all staff.

All temporary staff and supply staff used regularly by the school will be given the School E-Safety Policy and its importance explained.

Every member of staff, whether permanent, temporary or supply staff regularly used by the school, must be informed that network and Internet traffic will be monitored and can be traced to the individual user.

Enlisting Parents' and Carers' Support

Parents and carers attention will be drawn to the School E-Safety Policy in newsletters, the school brochure and on the school website.

Visitors and the E-Safety Policy

Not all visitors will need to use school ICT but those which do will need to be informed that the school does have an E-Safety policy and they should be given the opportunity to read it, if the Headteacher thinks that it would be appropriate.

Visitors using school ICT must be informed that network and Internet traffic will be monitored and can be traced to the individual user.

Should be reviewed annually.

A full copy of this policy will be given to:

- each member of the teaching staff/each member of the administrative staff/each member of the support staff

A copy will also be available

- to other interested parties, by request to the Headteacher or ICT Coordinator
- as a MSWord file in the staff section of the curriculum network.
- On the school's website

NOMINATED PERSONS

The following persons are nominated until further notice:

The nominated member of the senior management team with responsibility for e-safety is **Mrs Morey.**

The nominated E-Safety Co-ordinator is **Mrs Simmons**.

The nominated Governor with responsibility for e-safety is **Mrs. Lyuda Wade**

KM – reviewed Sep. 17

MEON INFANT SCHOOL

Acceptable Internet Use Statement

For Staff

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties - the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access must only be made via the authorised account and password, which must not be made available to any other person;
- All Internet use should be appropriate to staff professional activity or student's education;
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden;
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for e-mail they send and for contacts made that may result in e-mail being received;
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded;
- Posting anonymous messages and forwarding chain letters is forbidden;
- Copyright of materials and intellectual property rights must be respected;
- Legitimate private interests may be followed, providing school use is not compromised;
- Use for personal financial gain, gambling, political purposes or advertising is forbidden;
- Occasionally it may be necessary to investigate links to undesirable sites in order to prevent future access. Written permission will be sought from the Headteacher before undertaking such investigations.

Staff should respect the school's Confidentiality Policy when using social networking sites and should not include references to school life as these could be misconstrued in the local community.

Staff requesting Internet access should sign a copy of this Acceptable Internet Use Statement and return it to the ICT Manager for approval.

Full name ……. … … … … … … … … form/post … … … … … …… … …

Signed ……. … … … … … … … date … … … … … … … … … … … … …

Access granted … … …… … … … date … … … … … … … … … … … … …

STAFF /GOVERNORS/ VOLUNTEER HELPERS CONFIDENTIALITY STATEMENT

Meon Infant School takes confidentiality of information very seriously. It is a requirement of the school that all Staff/Governors/volunteer helpers read, understand and sign this document.

1. All staff/Governors/volunteer helpers are to respect the confidentiality of all parents, children, other professionals and each other. This means that privileged information *(this means any information relating to a child or their family that is obtained by virtue of being a staff member/Governor/volunteer that would not have been known otherwise)* relating to children/their families/staff will not be discussed with anyone outside of the staff body/management committee.

2. All business relating to Meon Infant School will be treated in the strictest confidence and not repeated outside of the school. This includes financial, staffing, management and any other business in connection with the Infant School.

3. If staff have family or personal connection with a child or family of a child in attendance at the school they must maintain the strictest professional relationship with the family whilst the child attends the school.

4. All staff/governors/volunteers and students will not attribute any comments on the internet (including social networking sites such as Facebook, Twitter etc.) to Meon Infant School without prior written agreement from the Headteacher. Staff must not add parents of children in the school as friends/contacts on these sites except where they are previously known or are themselves a staff member/governor. In these circumstances it is advisable to inform the Headteacher of those parents you are "friends" with.

The breaking of this agreement may result in disciplinary action for any staff member.

I have read and understand this confidentiality statement and agree to abide by it at all times.

Name .....

Signed .....

Date .....

All signed documents will be kept on file by the Headteacher