Mansbridge Primary School

E-safety Policy

Effective Practice in e-Safety
E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from Southampton City Council ;
- A school network that complies with the National Education Network standards and specifications.

School e-safety policy
1.1 E-Safety is a vital and necessary component of a school's health and safety policy.

2.1 Writing and reviewing the e-safety policy

- The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for child protection.
- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

2.2 Teaching and learning

2.2.1 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.

2.2.3 Internet use will enhance learning

The school Internet access will be designed expressly 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 given clear objectives for Internet use.

- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils will be shown how to publish and present information safely to a wider audience.

2.2.4 Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.
- Pupils will be taught how to report unpleasant Internet content e.g. informing teacher

2.3 Managing Internet Access

2.3.1 Information system security

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

2.3.2 E-mail

Pupils may only use approved e-mail accounts on the school system. These will be set up by the ICT technician and monitored by class teachers and e-safety co-ordinator. The email accounts will only be able to send emails internally.

Pupils will be taught that:

- in e-mail communication, pupils must not reveal their personal details or those of others, orarrange to meet anyone without specific permission. Pupils must immediately tell an adult if they receive offensive e-mail.Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

2.3.3 Published content and the school web site

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

2.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consideration will be given to using group photographs rather than full-face photos of individual children.
- Pupils " full names will not be used anywhere on a school Web site or other on-line space, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- Pupil image file names will not refer to the pupil by their full name.

2.3.5 Social networking and personal publishing

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

Newsgroups will be blocked unless a specific use is approved.

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

- Ideally pupils would use only moderated social networking sites, e.g. SuperClubs Plus

- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

- Pupils will be advised to use nicknames and avatars when using social networking sites.

2.3.6 Managing filtering
The school will work with Southampton city council to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator.

2.3.7 Managing emerging technologies

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

The senior leadership team 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.

- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

- The use by pupils of cameras in mobile phones will be kept under review.

- Games machines including the Sony PlayStation, Microsoft XBox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

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

2.4 Policy Decisions
2.4.1 Authorising Internet access
All staff must read and follow the Southampton Acceptable Use of the Internet policy.
The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

2.4.2 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. Neither the school nor SCC can accept liability for any material accessed, or any consequences of Internet access.

The school should 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.

2.4.3 Handling e-safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff.

Any complaint about staff misuse must be referred to the head teacher.

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

2.5 Communications Policy

2.5.1 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.

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.

- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

2.5.2 Staff and the e-Safety policy

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

- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

2.5.3 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 Web site.

The school will regularly update parents/carers regarding issues around e-safety and signpost them to organisations that can support them with use of the internet at home. This will be via school newsletters and/or the school website.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

The e-Safety Policy was approved by the Governors on
Reviewed 24.11.2010
Reviewed 28.09.2011
Reviewed 26.09.2012
Reviewed 25.09.2013
Reviewed April 2015
Reviewed April 2016

Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Kent Learning Zone
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. Ask Jeeves for kids Kidrex CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus Global SchoolNet Kid Safe Mail Cluster blogs
Publishing pupils" work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils" full names and other personal information should be omitted. Pupils" work should only be published on „moderated sites" and by the school administrator.	Making the News 2 SuperClubs Plus Cluster Microsites National Education Network Gallery
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that	Making the News SuperClubs Plus Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art Cluster Microsites National Education Network Gallery

	published images do not breach copyright laws.	
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Plus FlashMeeting
Audio and video conferencing to gather information and share pupils‟ work.	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	FlashMeeting National Archives "On-Line" Global Leap JANET Videoconferencing Advisory Service (JVCS)

Appendix 2: Useful resources for teachers

BBC Stay Safe
http://www.bbc.co.uk/cbbc/curations/stay-safe
Child Exploitation and Online Protection Centre
www.ceop.police.uk/
Childnet
www.childnet.com/
Cyber Café
http://www.thinkuknow.co.uk/8_10/cybercafe/
Digizen
www.digizen.org/
Kent e-Safety Policy and Guidance, Posters etc
http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety
Kidsmart
www.kidsmart.org.uk/
Hampshire Police – e-Safety
http://www.hampshire.police.uk/internet/advice-and-information/general/online-safety
Think U Know
www.thinkuknow.co.uk/
Safer Children in the Digital World
http://www.dfes.gov.uk/byronreview/

Appendix 3: Useful resources for parents

Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk
Sure Start
https://www.gov.uk/find-sure-start-childrens-centre

Acceptable Use of the Internet Policy for Mansbridge Primary School

Internet

- Pupils should be supervised at all times when using the Internet. Independent pupil use of telecommunications and electronic information resources is not advised.
- Access to school systems must be with a unique user name and password, which must not be made available to any other staff member or pupil.
- All Internet activity should be appropriate to staff's professional activity or the student's education.
- Users may use their Internet facilities for non-business research or browsing during meal time breaks, or outside of work hours, provided that all other Internet usage policies are adhered to.
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited.
- Copyrights, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The Internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material. Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The Internet must not be used to download entertainment software or games, or play games against other Internet users.
- Uploading materials or files to City Council systems must only be performed on machines that have virus protection to the latest corporate standards and with appropriate authorisation from the relevant departments.
- Downloading of files to school systems using ftp, email and http must be carried out with an appropriate level of care and thought. Problems arising from the installation of files, utilities and software updates obtained by such methods are the school's responsibility unless directed to do so by representatives of the City Council or their agents. Virus infection and subsequent removal caused by such methods on machines without protection to the latest corporate standards will be the school's responsibility.
- The Internet must not be used to engage in any activity for personal gain or personal business transactions.
- The Internet must not be used to conduct or host any on-going non-education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club.
- The Internet must not be used for personal or commercial advertisements, solicitations or promotions.
- The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990.
- To ensure compliance with the acceptable use policy for Web browsing and email

the school reserves the right to monitor and record pupils' activity in these areas. Users should therefore have no expectation of privacy in respect of their web browsing and email activities when using the school's computer facilities.

Email

- Access to email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil.
- Normally, access to another staff user's email account will not be granted to anyone. However, there are occasions when such access may be legitimately needed, e.g. To aid investigation of suspected irregularities; upon summary dismissal of an employee; during suspension or prolonged absence of an employee; where the retrieval of information is necessary to allow continuation of work in hand by the user whose ID/password combination is to be circumvented.
- Attachments from unknown sources should not be opened, but deleted immediately. All attachments should be scanned for viruses.
- Schools are responsible for all email sent and for contacts made that may result in email being received.
- Pupils must not send publish their personal details in an email to an unknown recipient
- Posting anonymous messages and creating or forwarding chain letters is forbidden.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Changes must not be made to other people's messages that are then sent on to others without making it clear where the changes have been made.
- Users must not pretend that they are someone else when sending email, or use someone else's account to send a message.
- Users must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured.
- Standard email addresses in Southampton follow the format of *initial.surname@schooldomain*. Care should be taken when considering the format of individual pupil email addresses, as the recipient would be aware of the sender's name using this format. To address this issue, some schools chosen to use anonymous email addresses for individuals to overcome this e.g. *12345@schooldomain*.

Social Networks, Chat Rooms, Instant and Text Messaging

- Pupils should only be given access to secure, age-appropriate chat rooms and social networks, e.g. GridClub, which are moderated by a teacher, or recognisable, identifiable and approved adult.
- The use of such websites should only be permitted within an educational or professional context.
- Teachers should familiarise themselves with any chat room being used, to ensure that it offers a genuine educational experience.
- Pupils should be supervised at all times when using such websites.
- Pupils should be taught to understand the importance of personal safety on the

Internet, i.e. taught never to give out personal contact information or to arrange to meet someone they have met online.

- Access to internet related services such as instant messaging, chat services and social networks is commonplace outside of the school environment. Many young people own, or have access to a mobile phone which increasingly are providing online access. For this reason, schools will need to ensure that pupils are taught safe and responsible behaviours whenever using ICT.

School Websites

-
- The production and publication of any unofficial websites is strictly forbidden and, if undertaken will be actively pursued by the City Council for removal on behalf of the school.
- A hyperlink will link the official home page to the school website, whether it is hosted with the City Council or externally.
- Only the designated staff member(s) within the school may upload material to the school website and all material for the website must be monitored and approved by the person(s) responsible. The user name and password must not be given to any other members of staff or pupils. If other people know this information, the school should immediately change the password.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore, using such images for school publicity purposes, i.e. school web site will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photographs, full names, addresses, telephone numbers and email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website, where possible the school details should be given as the main point of contact.
- Southampton City Council reserves the right to remove any material from school websites if it is considered to be unsuitable or if it poses a threat to the safety of a school or pupil. Individual support and guidance on developing a school website is available from CSL ICT Strategy telephone 023 8083 2111 or email csl.ict@southampton.gov.uk

References

Acceptable Use of the Internet Policy for Schools (CSL ICT Strategy 2008)
http://intranet.southampton.gov.uk/csl-esafety

E-safety – developing whole school policies to support effective practice (Becta 2005)
http://publications.becta.org.uk/display.cfm?resID=25934&page=1835

Safeguarding Children in a Digital World – developing a strategic approach to e-safety (Becta 2006)

http://publications.becta.org.uk/display.cfm?resID=25933&page=1835
Safeguarding Children Online – a checklist for Local Authorities and Local Safeguarding Children Boards (Becta 2007)
http://publications.becta.org.uk/display.cfm?resID=31051
Safeguarding Children in a Digital World – developing a LSCB e-safety strategy (Becta 2008)
available to view at the CSL ICT Strategy & Training Centre
Schools' e-Safety Policy Guidance 2007 (Kent County Council, 2007)
http://www.kenttrustweb.org.uk/kcn/e-safety_home.cfm
Signposts to safety – Teaching e-safety at Key Stages 1 and 2 (Becta, 2007)
http://publications.becta.org.uk/display.cfm?resID=32422&page=1835
Signposts to safety – Teaching e-safety at Key Stages 3 and 4 (Becta, 2007)
http://publications.becta.org.uk/display.cfm?resID=32424&page=1835
SCC Internet and Email Standards
http://intranet.southampton.gov.uk/corporatestandards/

i Becta was the Government's lead agency for Information and Communications Technology (ICT) in education, covering the United Kingdom. Becta lead the national drive to improve learning through technology.
ii The Child Exploitation and Online Protection (CEOP) Centre is part of UK law enforcement and as such can apply the full range of policing powers in tackling the sexual abuse of children. The organisation is very different in its set up not least because of the high volume of specialists who work alongside police officers but also because of the faculty approach that underpins their structure. In addition to the Intelligence and Operations Faculty, CEOP has a Harm Reduction Faculty which has a multi-faceted approach. It works to deliver market intelligence, liaising with the technological industry and fine-tuning guidelines that look to minimise the possibility of present and future technology increasing the risk of sexual abuse to children. At the same time, training, education and public awareness specialists work together to raise the knowledge, skills and understanding of parents, children, young people and a wide and diverse stakeholder community including dedicated skills training for those working with sex offenders.
iii For the blocking or unblocking of a website address please contact the IT Service desk on 023 8083 2333
iv If you are concerned or offended by the content of an email it can be forwarded to junkmail@southampton.gov.uk for further investigation.

E-Safety Audit – Primary / Special

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Network Manager and Headteacher.

Has the school an e-Safety Policy that complies with current guidance? **Y/N**

Date of latest update (at least annual):

The school e-safety policy was agreed by governors on:

The policy is available for staff at:

The policy is available for parents/carers at:

The responsible member of the Senior Leadership Team is:

The responsible member of the Governing Body is:

The Designated Child Protection Coordinator is:

The e-Safety Coordinator is:

Has e-safety training been provided for both pupils and staff? **Y/N**

Is there a clear procedure for a response to an incident of concern? **Y/N**

Have e-safety materials from CEOP and Becta been obtained? **Y/N**

Do all staff sign a Code of Conduct for ICT on appointment? **Y/N**

Are all pupils aware of the School's e-Safety Rules? **Y/N**

Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils? **Y/N**

Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules? **Y/N**

Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced? **Y/N**

Has an ICT security audit been initiated by SLT, possibly using external expertise? **Y/N**

Is personal data collected, stored and used according to the principles of the Data Protection Act? **Y/N**

Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements **Y/N**

Has the school-level filtering been designed to reflect educational objectives and approved by SLT? **Y/N**