Manor Primary School Policy Document

E-Safety Policy

Written	November 2014
Approved by Governors	
Review date	November 2016

'Our vision is to create a school community where children grow into happy, confident and responsible individuals, who work hard together to achieve their full potential.'

Background

The internet is an essential resource to support teaching and learning and is a part of the statutory curriculum and a necessary tool for staff and pupils.

Computer skills are vital and essential life-skills, and young people have access to the internet from many places - home, school, friends' homes, libraries etc. Teachers need to plan to integrate the use of web-based resources, e-mail and mobile learning, such as phones and touch screen tablet devices.

Schools have a number of services to help ensure that curriculum use is safe and appropriate. However, access out of school does not usually have these services and there are a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line elsewhere.

Internet safety depends on staff, schools, governors, parents and the pupils themselves taking responsibility for the use of the internet and other technologies such as mobile phones. There are no totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Teaching and Learning

Internet use will enhance learning:

- Pupils will be educated in the effective use of the internet for research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright laws.
- Pupils will be taught the importance of cross checking information before accepting its accuracy.
- All forms of bullying, including cyberbullying will be taken seriously, reported to the head teacher and logged in the appropriate file located in the office.

Managing Internet Access

Information system security:
- The schools internet access is provided through the South West Grid for Learning (SWGfL) which is designed for pupil use and includes filtering appropriate to the school.
- School computer system security will be reviewed regularly.
- Virus protection will be updated regularly.
- The school will work in partnership with the LEA on security strategies.
- If staff or pupils discover unsuitable sites, the URL and content will be reported to the computing team who will contact the advisor (K Solomon).

E-mail
- Pupils may only use approved e-mail account on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter on school headed paper.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters is not permitted.

Published content and school website
- Staff or pupil personal contact information will not be published. (The contact details given will be admin@manor.devon.sch.uk)
- Written permission from parents or carers will be obtained before photographs of pupil's are published on the school website. Photographs that include pupils will be selected carefully so that their image cannot be misused.
- Pupils' full names will not be used anywhere on a school website or other on-line space, particularly in association with photographs. Website photographs will be selected carefully to ensure individual pupils cannot be identified by name.
- Work will only be published with the permission of the pupil and parents/ carers.

Social networking and personal publishing
- The school will control access to social networking sites, and will educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social networking spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networks.
- Schools will ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
- Specific lessons will be included to teach all pupils how to read for information from web resources.
- Staff should exercise caution, sound judgement, and common sense when using social media sites.
- Employees of the school should not communicate with students on roll through social media sites and should exercise caution when befriending parents of children enrolled at school.

Managing Filters
- The school will work with SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable material or illegal sites, the URL (address) and content must be reported to the computing team or K.Solomon immediately.
- Computing team will ensure that K. Solomon makes regular checks to ensure that filtering methods selected are appropriate, effective and reasonable.

Managing Videoconferencing and webcam use
- Videoconferencing should use the SWGfL broadband network to ensure quality of service and security.
- Pupils must be accompanied with a member of staff before making or answering a videoconferencing call.

Managing emerging technologies

- Emerging technologies will be examined for educational benefits 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 communication. Our policy is that these devices should be handed in to the office and returned to the pupils at the end of the school day.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files is forbidden.
- Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme
- Staff must not use their own mobile phones in the presence of pupils and they should be turned off during lesson time.
- The appropriate use of our learning platform, as per our platform policy.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the data protection act.

Policy Decisions

Authorising Internet access

- All staff will be provided with the School Internet Policy, and its importance explained.
- All staff must read and sign the "Code of Conduct for Computing" before using the resources.
- All staff will be given the SWGfL Internet Acceptable Usage Policy.
- The school will maintain a current record of all staff and pupils who are granted access to the school computing systems.
- All pupil internet access will be supervised by an adult.
- Parents will be asked to sign and return a consent form.
- Any person not directly employed by the school will be asked to sign the "Code of Conduct for Computing" before being allowed to access the internet from the school site.
- Staff development in safe and responsible internet use and on the school Internet policy will be provided as required.

Assessing risks

The school will take 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 Devon LEA can accept liability for any material accessed, or any consequences of internet access.

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

Handling e-safety complaints
- Complaints of internet misuse will be dealt with by the Designated Safeguarding Officer.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the internet.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Introducing the e-safety policy to pupils
- All children begin the academic year learning abut e-safety and follow the SMART rules (Safe, Meeting, Accepting, Reliable) too keep them safe when using the internet.
- E-Safety rules will be posted in the computer suite and discussed with pupils regularly to remind thee children how to use the nteerneet safely and responsibly. Instruction on responsible and safe use should precede Internet access.
- Pupils will be informed that network and internet use will be monitored and appropriately followed up.
- E-safety training will be embedded (using Rising Stars) within computing and PSHE curriculum, covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.

Staff and the e-safety policy

- All staff will be given the 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.
- Staff will use a child friendly search engine when accessing the web with Foundation and KS1 children, however those children in KS2 will be taught how to safely search the internet using engines such as Google.
- Children must be monitored by staff at all times, and never left alone when using the internet.

Enlisting parent's and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school website.
- Information will be provided to parents about how to ensure they can work with the school to ensure e-safety is used appropriately both within school and home.
- Internet issues will be handled sensitively without undue alarm.
- A partnership approach with parents will be encouraged.
- The school will maintain a list of e-safety resources for parents/carers.
- New parents will be asked to sign the internet permission form.

Code of Conduct for Computing at Manor Primary School

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- ➢ I understand that it is a criminal offence to use a school computing system for a purpose not permitted by its owner.

- ➢ I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.

- ➢ I understand that my use of school information systems, internet and email may be monitored and recorded to ensure policy compliance.

- ➢ I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

- ➢ I will not install any software or hardware without permission.

- ➢ I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.

- ➢ I will respect copyright and intellectual property rights.

- ➢ I will report any incidents of concern regarding children's safety to the Designated Child Protection Coordinator or Headteacher.

- ➢ I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- ➢ I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for Computing.

Signed: ……………………………………………… Capitals: …………………………………….Date: ……………

Accepted for school: ……………………………. ……………………… Capitals: …………………………. ……………

Agreed by Governors and SMT – November 2014

<h1 align="center">Pupil Acceptable Use Agreement/e-Safety Rules</h1>

Dear Parent/Carer

Computing has become an important part of learning in our school. We expect all children to be safe and responsible when using any equipment or resources.
Please discuss these e-safety rules with your child. If you have any concerns, please contact the school which holds a Code of Conduct for Computing policy and an e-Safety policy.

- ❖ I will only use computing in school for school purposes.
- ❖ I will only use my class email address.
- ❖ I will make sure that all contacts with other children and adults are responsible.
- ❖ I will not deliberately look for, save or send anything that could be unpleasant or hurtful. If I accidentally find anything like this I will turn off my monitor and tell my teacher immediately.
- ❖ I will not send to children or adults anything that could be considered unpleasant or hurtful.
- ❖ I will not give out my own details such as my name, phone number or home address.
- ❖ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ❖ I will be responsible for my behaviour when using computing because I know that these rules are to keep me safe.
- ❖ I know that my use of computing can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-safety.

E-Safety Agreement

Name of child

……………………………………………………………………Class…………………………………………………

We have discussed this and my child agrees to follow the e-Safety rules and to support the safe use of computing at Manor Primary School.

Parent/ Carer Signature ………………………………………………………..……

Date……………………………….

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of their Computing skills, Manor Primary School provides supervised access to the internet. We believe it is an effective, worthwhile essential skill for children as they grow up in the world.

All children begin the academic year learning about e-safety and follow the SMART rules to keep them safe when using the internet. These are displayed in the computer suite to remind the children how to use the internet safely and responsibly.

Our school internet provider is the SWGfL, which operates a filtering system that restricts access to inappropriate materials. However, whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the internet. The school will not be liable for any damages arising from your child's use of the internet facilities.

Please would you read the attached Acceptable Use agreement and sign and return the consent form so that your child may use the Internet at school.

Should you wish to discuss any aspect of internet use please contact the school.

Yours sincerely

Policy for responsible e-mail, network and internet use for
Manor Primary School

- ❖ I will use all computing equipment issued to me in an appropriate way. I will not:
- Access offensive websites or download offensive material.
- Make excessive personal use of the internet or e-mail.
- Copy information from the internet that is copyright or without the owner's permission.
- Place inappropriate material onto the internet.
- Will not send e-mails that are offensive or otherwise inappropriate.
- Disregard my responsibilities for security and confidentiality.
- Download files that will adversely affect the security of the laptop and school network.
- Access the files of others or attempt to alter the computer settings.
- Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Manor Primary School.

- ❖ I will inform the School's Technician as soon as possible if I know my password is no longer secret.
- ❖ I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the internet sites I visit.
- ❖ If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
- ❖ I will not open e-mail attachments unless they come from a recognised and reputable source.
- ❖ I will bring any other attachments to the attention of the technician.
- ❖ I will report immediately to the **Headteacher** any unpleasant material or messages sent to me.
- ❖ I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
- ❖ Use for personal financial gain, gambling, political purposes or advertising is forbidden.
- ❖ Activity that threatens the integrity of the school system, or activity that attacks or corrupts other systems, is forbidden.

I understand that if I do not adhere to these rules, my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Name...

Signature: ....

Date: ....