MANOR FARM
COMMUNITY JUNIOR SCHOOL

E-SAFETY POLICY

Date of last review: **September 2014**

Due for Review: **September 2017**

Manor Farm Community Junior School

E-SAFETY POLICY

Policy for E-Safety and Acceptable Usage

At Manor Farm Community Junior School, we recognise the importance of using, and developing a good understanding of new technologies to enhance learning. Moreover we are aware that the technology will play a fundamental part in the present and future lives of our children and that ICT in our schools should reflect ICT in society.

The school is committed to the developing our ICT in order to create ICT users with the skills necessary to quickly adapt to new technologies, as well as creating effective communication between pupils, staff, parents and the wider community to share our school news.

However, as in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Additionally, some young people may find themselves involved in activities which are inappropriate, or possibly illegal. E-safety seeks to address the issues around using these technologies safely and promote an awareness of the benefits and the risks.

Network Safety:

All users need to log on using their username, this is specific to them. The children are taught from Year 3 that they should only log on using their own username. Children have a generic password.

On the network there is an 'ICT share area' where children may save work. Pupils are taught how to access the shared resource area and to save their work there. We expect pupils to be respectful of other people's work and not to delete anything without permission.

Pupils are only allowed to print their work under the instruction of an adult. Work prints to the networked printer.

Children must be taught not to change or alter any settings. Although children are unable to access a large part of the network, they still need to be taught the importance of this.

Only the network administrators are permitted to install software on to computers. Staff requiring additional software must raise an issue in the ICT issues book to be dealt with by the ICT administrator. If apps are required for the tablets, staff need to ask the Computing coordinator; if these are paid apps, permission must be sort from the subject specific budget holder, for example maths**.**

All users of the network can be monitored remotely by the network administrators. *Pupils are taught that their use of the network can be monitored.*

Internet Safety:

The school system is filtered by the internet provider for the safety of the children. These filters are designed to protect the children and staff from accidental or deliberate access of unsuitable materials. The network administrators can manually add site address which are considered unacceptable, or those sites which are acceptable and have been incorrectly blocked.

However, no system is 100% safe and we expect users to behave responsibly. Pupils are taught that the Internet contains many websites that are useful but that there are also websites that are unpleasant, offensive, not child-friendly or can damage your computer. Children are also taught that whilst the internet is useful, not everything on the internet is true and that children need to use trustworthy sources and websites.

Staff are expected to have watched any online videos, being used in their teaching, all the way through before presenting them to the children. Staff must never carry out video or image searches in front of the children.

Children are expected to report to the nearest adult, immediately, anything that they see which they find upsetting, inappropriate, or which they believe should have been blocked by the filtering system. All reports of this nature will be logged by Teachers and passed on to the Computing coordinator and person responsible for Child Protection, as appropriate.

We expect pupils to make no attempt to access a website that they know to be unsuitable for children and/or containing offensive language, images, games, other media or social networking sites.

Pupils accessing the Internet at home are subject to the controls placed upon them by their parents. However, any home use of the Internet made in connection with the school or school activities; any of its staff, pupils and governors or any partnership organisation will be subject to this policy and any breach dealt with as if the event took place at school. We expect all members of our school community to behave as positive ambassadors of the school in all school related activities made through the Internet.

The school website contains school policies, newsletters and other information. **We expect all persons accessing the school web site to treat the content with respect and make no attempt to reproduce, use or alter any part in any way with malicious intent. No part can be reproduced for commercial reasons without written permission from the school.**

Email safety:

Some pupils will have their own webmail accounts at home. As these are independent of the school they do not necessarily come with the safeguards that we set for email usage. Therefore we do not permit the use of personalised email accounts by pupils at school or at home for school purposes. We remind children that when setting up an email account, the email account provider has terms and conditions which should be read and adhered to. Many email account providers set a minimum age limit of 11 years.

Website safety:

Websites accessed out of school do not come within the safeguards that we set within school. However, the children are taught that they need to also be very careful when using online sites. They should **never give their real name, school, age or location.** Children need to be taught the dangers of giving out personal information to strangers on the internet and should always use a nickname rather than their real name. Children should never put a photo of themselves online wearing their school uniform as it makes them easily identifiable and gives a stranger information about where they live. Children should also know that the people that they are talking may not be who they think they are.

Digital Images:

- Digital still and video cameras are used for recording events as well as being essential tools for everyday learning experiences across the curriculum. When children arrive at Manor Farm Community Junior School, all parents have the opportunity to opt out of their child's image being used by the school. Some images celebrating the work of pupils involved in everyday and special event activities may be selected to be shown on the school website or on our display screens. On the website we never state a child's full name with their image. The school will happily remove any image of a child on the school website at their parent's request.
- Digital images may be shared with partner schools and organisations as part of collaborative learning projects. This can include live video conferencing. All such use is monitored and supervised by staff. Pupils are taught to seek permission before copying, moving, deleting or sending any images taken within school. We expect all pupils to seek permission from staff before sharing images outside of the school environment.
- Staff may use their own personal phones, cameras and recording equipment with the permission of the Head Teacher to enhance learning. However, any images must be transferred to a school computer at the earliest opportunity and deleted from the device as soon as possible. Photos should not be stored on personal computers, only the school devices or the school network. Photos should never be passed on to a third party without permission from a senior leader. **Staff may not take photos of the children in any state of undress or in swimwear.**

Cyber Bullying:

- The school takes all forms of bullying very seriously. Cyber-bullying is the use of any communication medium to offend, threaten, exclude or deride another person or their friends, family, gender, race, culture, ability, disability, age or religion. Pupils are taught about bullying as part of the PSHE curriculum. We expect all members of our community to communicate with each other with respect and courtesy. Bullying of any type will not be tolerated by the school and will be dealt with under the procedures within the Whole School Policy on Behaviour, including bullying**.** All incidences of cyber bullying are recorded by the e-safety coordinator. Cyber bullying which takes place outside of school hours, if reported by a pupil or parent, will be dealt with as far as is reasonably possible by school staff.

Mobile Phones:

- Pupils should not bring mobile phones in to school. In exceptional circumstances, children may be permitted to bring phones into school but these must be switched off and handed into the school office before school and collected when school finishes.
- Pupils shouldn't have a mobile phone on their person in school. If a phone is brought into school without permission, it will be confiscated by a member of staff and only returned to an adult.

Data Protection Act:

- The Data Protection Act 1998 gives you the right to access information held about you or your child by the school. The school has the right to charge for supplying this information. Further information on the Data Protection Act can be obtained from the Department of Constitutional Affairs – www.justice.gov.uk

Child protection

- Any e-safety incident which raises concerns about a child protection issue will be reported to the school designated person and referred to Social Care as appropriate.

Glossary of terms
Email Text based messages sent through the Internet
Internet A global network of computers which allow efficient communication from any point to any point
Network A group of computers linked together and often managed by a server
Podcast One of a series of sound files uploaded on to the Internet and download by subscribers
Server A computer that controls access to a network of computers and usually stores data for all users
Webmail Email service which is held on a secure website and can be accessed anywhere on the Internet

E-Safety Rules for Pupils

Think then Click
E-safety Rules for Key Stage 2
· We ask permission before using the Internet. · We only use websites that an adult has chosen. · We tell an adult if we see anything we are uncomfortable with. · We immediately close any web page we not sure about. · We only e-mail people an adult has approved. · We send e-mails that are polite and friendly. · We never give out personal information or passwords. -We never use our real name · We never arrange to meet anyone we don't know. · We do not open e-mails sent by anyone we don't know. · We do not use Internet chat rooms. - We never put pictures of us on the Internet in our school uniform.