St Michael and St John’s R.C. Primary School

E-Safety Policy

2014-15

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 Designated Child Protection Coordinator as the roles overlap. It is not a technical role.

Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance.

It has been agreed by senior management and approved by governors.

The e-Safety Policy was revised by ICT Subject Leader

It was approved by the Governors on:14/10/14

The next review date is: October 2015

1.2 Teaching and learning

1.2.1 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 provides pupils quality access as part of their learning experience.

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

1.2.2 Internet use will enhance learning

The school Internet access is designed expressly for pupils use and will include filtering by the Internet provider, CLEO. On the occasion any unsuitable material appears, it is reported to ***One Connect*** who manages the school Internet system.

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 to a wider audience.

1.2.3 **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 how to report unpleasant Internet content e.g. by informing an adult, using the CEOP Report Abuse icon or Hector Protector.

2. **Managing Internet Access**

2.1 **Information system security**

School ICT systems security will be reviewed regularly.

Virus protection, **SOPHOS** provided by LCC is constantly being updated.

Security strategies will be discussed with the Local Authority.

2.2 E-mail

Pupils may only use approved e-mail accounts on the school system

Pupils must immediately tell a teacher if they receive offensive e-mail.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Any pupil who breaches the e-mail protocol will have their account barred.

2.3 Published content and the school website

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

2.3.1 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. We will consider using group photographs rather than full face photos of individual children.

Pupils’ full names will not be used any where on a school website or other on-line space, particularly in association with photographs.

Written permission from parents and carers is obtained at the beginning of the school year regarding the use and publication of children’s images.

Work can only be published with the permission of pupil and parents/carers.

2.3.2 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.

2.3.3 Managing filtering

The school will work with CLEO and One Connect 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.

2.3.4 Managing videoconferencing & webcam use

Video conferencing should use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

2.3.5 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.

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.

Children are not allowed to have mobile phones in school. Any that are brought into school will be given to their teacher for safe keeping until the end of the day.

The appropriate use of learning platforms will be discussed as the technology becomes available.

2.3.6 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 sign the ‘Staff Code of Conduct for ICT’ before using any of the school ICT resources.

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 LCC can accept liability for any material accessed, or any consequences of Internet access (not sure about this sentence)***

The school should audit ICT use to establish if the e-safety policy is adequate and 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 complaints about staff misuse must be referred to the headteacher.

2.4.4 Community use of the Internet

The school will liaise with parents and local organisations to establish a common approach to e-safety.

2.5 Community 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.

Precautions to stop Pupils breaching e-safety rules…

Key Stage 1

a. The children search the internet using websites saved in My Favourites.
b. Children search the internet using Espresso search facility.

c. In the event of any unpleasant material the children are instructed to do the following.

(i) Turn off the monitor.
(ii) Tell supervising adult.
(iii) Establish who else has seen the image etc.

Key Stage 2

a. The children will only access search engines under adult supervision.
b.Children search the internet using Espresso search facility.
c.In the event of any unpleasant material the children are instructed to do the following.

(i) Turn off the monitor.
(ii) Tell supervising adult.
(iii) Establish who else has seen the image etc.

d. Any incidences will be recorded in an ICT incident book stored in a secure place in the ICT Suite.

<u>Sanctions</u> if Pupils breach safety rules..

a. Establish if the breach was accidental or on purpose.
b. Accidental breaches will be recorded and parents informed in case the child is traumatised.
c. If it was intentional, parents would be notified and a contract of responsible use will be signed.
d. Subsequent breaches will result in 1:1 supervision (either through peer or adult).

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, initially based on the materials from CEOP and thinkuknow.co.uk .

E-safety training will be embedded within the ICT scheme of work and linked to the PSHE curriculum and SEAL.

2.5.2 Staff and the e-safety policy

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

2.5.3 Enlisting parents' and carers' support

Parents and carers attention will be drawn to the School e-Safety Policy in newsletters and in the school brochure.

The school will maintain a list of e-safety resources for parents/carers. See appendices.

St Michael and St John’s R.C. Primary School, Clitheroe.

E-Safety Policy 2014