Michaelchurch Escley Primary School

E-Safety Policy **March 2016**

Our e-Safety Policy has been written by the school, drawing on current government guidance. It has been agreed by senior management and approved by the governors. The e-Safety Policy and its implementation will be reviewed annually.

The e-Safety Policy was revised by: Mr Gary Crocker
It was approved by the Governors on: March 2016
The next review date is: March 2018

1. 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.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and effective curriculum practice;
- communication and collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and DCSF;
- access to learning wherever and whenever convenient.

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 to a wider audience.

Evaluation of 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 internet content they find unpleasant

2. Managing Internet Access

Information system security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.

E-mail

The government encourages the use of e-mail as an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional school boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

- 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.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- Individual school e-mail addresses are used at Key Stage 2
- Pupils may not access personal email accounts in school.
- E-mail sent to an external organisation is written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The sending of abusive or inappropriate email messages is forbidden.

Published content and the school website

The school web site – www.michaelchurchprimary.co.uk - displays the rich diversity of opportunities available to pupils at Michaelchurch, as well as celebrating the achievement of pupils and sharing of information.

The point of contact on the Website is the school address, school e-mail and telephone number. Staff or pupils' personal information is not published.

- The headteachers and ICT Co-ordinator take overall editorial responsibility and try to ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils are selected carefully so that their image cannot be misused.
- Pupils' full names are not used anywhere on the Website or other online space, particularly in association with photographs, without express parental permissions.
- Written permission from parents or carers is obtained before photographs of pupils are electronically published.
- The copyright of all material is held by the school, or is attributed to the owner where permission to reproduce has been obtained.
- Parents will be clearly informed of the school policy on image taking.

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 will only use moderated social networking sites, eg. LA Learning Platforms.
- 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.

Managing filtering

- The school works in partnership with parents, the LA and DCSF to ensure that systems to protect pupils are reviewed and improved.
- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- It is the responsibility of all staff to ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies.

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 e.g. Smart Phones
- The senior management 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.

- If children need to bring a mobile phone to school, the phone will be deposited at the school office in the morning for collection at the end of the day.

Protecting personal data

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

3. Policy Decisions

Authorising Internet access

- The school allocates Internet access for staff and pupils on the basis of educational need. Parental permission is required for each pupil.
- The school maintains a current record of all staff and pupils who are granted access to the school's ICT systems.
- Pupils accessing the internet are directly supervised by a member of staff.
- Parents are informed that pupils will be provided with supervised Internet access and are asked to return a consent form.

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 HCC can accept liability for any material accessed, or any consequences of Internet access.

Methods to identify, assess and minimise risks will be reviewed regularly. The headteachers will ensure that the e-Safety policy is implemented and compliance with the policy monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Complaints procedures

- Prompt action is required if a complaint regarding the inappropriate use of the Internet is made. The facts of the case need to be established, for instance whether the Internet use was within or outside school.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be referred the school Designated Child Protection Coordinator and dealt with in accordance to school child protection procedures
- Pupils and parents will be informed of consequences for pupils misusing the Internet. A minor transgression of the rules may be dealt with by the teacher as

part of normal class discipline. Other situations could potentially be serious and a range of sanctions are in place, linked to the school's behaviour policy.

- Sanctions available include:
    - interview/counselling by Headteacher
    - informing parents or carers
    - removal of internet or computer access for a period.
- Pupils and parents will be informed of the complaints procedure (see school complaints policy)
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with other safeguarding issues, there may be occasions when the police must be contacted.

4. Communications Policy

Introducing the e-Safety policy to pupils

- E-Safety rules will be posted in rooms where computers are used and discussed with the pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Instruction in responsible and safe use will precede Internet access.
- e-Safety training will be embedded within the ICT scheme of work or the PSHCE curriculum.

Staff and the e-Safety policy

- All staff will have access the e-Safety policy and its application and importance explained.
- Staff should be aware that network and Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will use a child friendly safe search engine when accessing the web with pupils.

Enlisting parent/carer support

The majority of pupils have access to the internet at home. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet. The school may be able to help parents plan appropriate, supervised use of the Internet at home. Parents are also advised to check if pupils' use elsewhere, such as libraries, is covered by an appropriate use policy.

- Parents'/Carers' attention will be drawn to the school's e-safety Policy in newsletters, the school handbook and on the school website.
- Internet issues will be handled sensitively, and parents/carers will be advised accordingly.
- A partnership approach with parents will be encouraged.
- The school will ask new parents to sign the parent/pupil agreement when they register their child within the school.