St. Michael & All Angels Primary School

E-safety Policy

This policy was adopted on	**Date:**
By Name:	
Position:	
Signature:	**on behalf of St. Michael & All Angels Primary School**
This Policy was updated in September 2012 & will be reviewed or replaced no later than December 2013 Version 1.1	

St. Michael & All Angels Primary School
E-safety policy Policy

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 Safeguarding Pupils. The school's Safeguarding Officer & Network Manager will also act as the E-Safety Coordinator.

Our e-Safety Policy has been written by the school, building on CEOP & Government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

Teaching and Learning

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children 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.

Internet use will enhance learning

The school Internet access is designed expressly for pupil use and includes 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 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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Managing Internet Access

- Information system security
- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Advice on security strategies will be monitored on the School's ICT web page and clarification sought as necessary.

E-mail

Staff & Pupils may only use approved e-mail accounts on the school system and email usage by pupils should be supervised and monitored by a staff member.

- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be 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.

Published content and the school web site

The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, 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's work can only be published with the permission of the pupil and parents.
- Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- YouTube is currently blocked in school to prevent the viewing of inappropriate material.

Managing filtering

- The school will work with the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Managing videoconferencing
- When this becomes available within the school, videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils will be required to gain permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Protecting personal data
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Policy Decisions

- Authorising Internet access

Acceptable ICT Use Agreement

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. Staff will be regularly reminded of the schools Acceptable Use Policy which they will have to agree to before using the schools computers. Clicking on agree is deemed as you agreeing and signing the policy.

- All Pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource. Parents must also sign the same Acceptable use policy.

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance, a member of staff may leave or a pupil's access be withdrawn.

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

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school or Knowsley Council can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

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 or Deputy Head Teacher in the Head Teachers absence.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

Communications Policy

Introducing the e-safety policy to pupils
E-safety rules will be discussed with the pupils at the start of each year.
Pupils will be informed that network and Internet use will be monitored.
At the start of each school year the Acceptable Use Policy will be sent home for parents and pupils to sign. Parents are advised to discuss the content of the AUP with their child before signining.

Staff and the e-Safety policy

All staff will be emailed the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.