Iqra Slough Islamic Primary School

E-Safety Policy 2013 - 2014

"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the Internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."

From: Safeguarding Children in a Digital World. BECTA 2006

E-Safety Policy

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Child Protection and Safeguarding, Behaviour for Learning, Anti-Bullying, Curriculum and Confidentiality.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems

1.0 School e-safety 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 and for child protection.

- The school's e-Safety Coordinator is also the ICT Coordinator (Mr Coleman, Assistant Head). He works in close co-operation with the named Designated Child Protection Officers of the school and with all SLT.
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection, Health and Safety, Anti- Bullying, PSHEC and ICT policies.

2.0 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 students 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 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them 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

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school ICT Coordinator.
- Staff should ensure that the use of Internet derived materials by staff and by 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.

3.0 Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

E-mail

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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 headteacher 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

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

4.0 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- Staff have access to a school phone where contact with pupils is required.

Protecting personal data

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

5.0 Policy Decisions

Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the

acceptable ICT Acceptable User Policy (AUP) before using any school ICT resource.

- At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy.

Assessing risks

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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. The school can accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

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.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Sanctions within the school discipline policy include:
  - interview/counselling by class teacher / headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period.

Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Parents using school ICT equipment must sign an AUP consent form prior to use (eg Family ICT, Numeracy and Literacy).

6.0 Communications Policy

Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness

and importance of safe and responsible internet use.

Staff and the e-Safety policy

- All staff will be given 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.

Enlisting parents' / carers' support

- Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.

Criminal law

Although bullying in itself is not a specific criminal offence in the UK, it is important to bear in mind that some types of harassing or threatening behaviour – or communications – could be a criminal offence, for example under the Protection from Harassment Act 1997, the Malicious Communications Act 1988, the Communications Act 2003, and the Public Order Act 1986.

If school staff feel that an offence may have been committed they should seek assistance from the police. For example, under the Malicious Communications Act 1988, it is an offence for a person to send an electronic communication to another person with the intent to cause distress or anxiety or to send an electronic communication which conveys a message which is indecent or grossly offensive, a threat, or information which is false and known or believed to be false by the sender.

Head Teachers Signature ……..

Approved by the Governing Body on…….…Feb 2014……

Review date:..... Feb 2015.....

Appendix 1:

E-Safety Audit

This quick audit will help the senior management team (SMT) assess whether the basics of e-Safety are in place to support a range of activities.

The school has an e-Safety Policy	**Y/N**
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff	
And for parents	
The Designated Child Protection Coordinator is	
The e-Safety Coordinator is	
How is e-Safety training provided?	
Is the Think U Know training being considered? (available Sept 07)	**Y/N**
All staff sign an Acceptable ICT Use Agreement.	**Y/N**
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	**Y/N**
Rules for Responsible Use have been set for students:	**Y/N**
These Rules are displayed in all rooms with computers.	**Y/N**
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	**Y/N**
The school filtering policy has been approved by SMT.	**Y/N**
An ICT security audit has been initiated by SMT, possibly using external expertise.	**Y/N**
School personal data is collected, stored and used according to the principles of the Data Protection Act.	**Y/N**
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by a member of SMT.	**Y/N**
Have these staff attended training on the filtering and monitoring systems?	**Y/N**