Rush Green Primary School E-Safety Policy

January 2015

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. Examples of e-Safety issues include:

- exposure to inappropriate material
- bullying via websites and mobile phones
- the threat of danger from making contact with a criminal minority via chat rooms and social networking sites

Writing and reviewing the E-safety policy

The E-Safety Policy relates to the Acceptable User Agreements signed by pupils, staff and other adults working in the school and other policies including those for Safe Guarding, Child Protection and Anti-bullying.

The school's ICT Co-ordinator will also act as E-Safety Coordinator. Our e-Safety Policy has been written by the school in conjunction with guidance from LGFL. 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

School Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils through RM Safety Net. Pupils will be taught about acceptable and non-acceptable internet use and they will be given clear objectives for safe internet use. Pupils will be educated in the safe use of the internet in research, including skills of 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.

Parents will be made aware of the 'Acceptable User Agreements' for KS1 and KS2 pupils which are available to view on the school's MLE.

Children are made aware of the internet safety steps that are to be taken prior to internet use:

- Keep your password protected at all times.
- Only access websites which you have been told/have permission to do so.
- Never pass on personal information about yourself over the internet.
- Always tell an adult if you come across something inappropriate on the internet so that it can be recorded and acted upon.

E-mail and text messaging

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

Pupils must immediately tell a teacher if they receive an offensive e-mail or other electronic message.

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

Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

General written permission from parents or carers will be obtained before photographs of pupils are published on the school web site or MLE. More specific permission will be obtained before photos or videos are uploaded to public domains.

Staff may not use their mobile phones to take photos of pupils.

Social networking and personal publishing

The school will block/filter access to social networking sites.

Pupils will be advised never to give out personal details of any kind that may identify them or their location.

Pupils will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the Internet Service Provider and Barking and Dagenham LA 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 emerging technologies

Pupils' mobile phones are not allowed in school.

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

For Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised

access to specific, approved on-line materials.

For Key Stage 2, children are made aware of the internet safety steps that are to be taken prior to internet use and that children never access the internet without a suitable adult present.

Parents will be asked to sign and return an acknowledgement form.

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. The school cannot 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.

Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communications Policy

Introducing the e-safety policy to pupils

E-safety rules will be discussed with pupils at the start of each year.

Pupils will be informed that network and internet use will be monitored.

Each year, pupils will participate in a range of activities about how to stay safe on the inetrnet

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained. All adults working in the school will sign an 'Acceptable User Agreement' form to be kept by the head teacher.

Staff should be aware that internet traffic can be monitored. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters (as and when appropriate), the school brochure and the school web site.

To be reviewed: January 2017

Governing Body Approval _____ Date _____