E – Safety Policy

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 will operate in conjunction with other policies including those for Assertive Discipline, Anti-Bullying, Curriculum, Data Protection and Child Protection.

This e-safety policy provides a school e-safety policy that has been guided and approved by the Children, Families and Education Directorate (CFE).

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 from the East Midlands Broadband Consortium using National Education Network standards and specifications.

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, anti-bullying and for child protection.

- The school has appointed an E-Safety Leader (D. Johnson). This role is shared by the Designated Child Protection Leader (J. Virk – Headteacher; D. Swann – Deputy Headteacher and S. Audley – EYFS Assistant Headteacher) and the Computing Leader (D. Johnson).
- Our e-Safety Policy has been written by the school, building on the Becta e-Safety Policy and government guidance. It has been agreed by Leadership Team and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually using the audit in appendix 2.
- The e-Safety Policy was revised by: D. Johnson (Computing leader) and J. Virk (Head Teacher)

1.2 Teaching and learning

1.2.1 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.

1.2.2 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

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 should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

1.3 Managing Internet Access

1.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with EDISS.

1.3.2 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.
- 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.
- Incidents of 'Cyber-bullying' through e-mails should be passed on to the Head teacher.

1.3.3 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 and business manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

1.3.4 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 on the Website in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.
- Work published on the Website will be carefully selected in order to encourage anonymity.

1.3.5 Use of Twitter, other 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 which 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.

- The school will take action if any of the following actions are committed by pupils or staff.
    - ❖ Offensive language aimed the staff, school, parents, governors or others affiliated with the school.
    - ❖ Unsuitable comments or pictures posted on feeds.
    - ❖ Images or text which infringe upon copyright.
    - ❖ Comments that aim to undermine the school, staff, parents, governors or others affiliated with the school.

1.3.6 Managing filtering

- The school will work with the LA, DfES 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 Leader.
- The E-Safety Leader and technician will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.8 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 allowed in school time and must be handed to the office for safe-keeping. The sending of abusive or inappropriate text messages is forbidden.

1.3.9 Protecting personal data

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

1.4 Policy Decisions

1.4.1 Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- 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.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

- Parents will be asked to sign and return a consent form.

1.4.2 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 nor Leicester City Education Authority 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.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the head teacher.
- Any complaint about staff misuse must be referred to the head teacher.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will be taught about e-safety through specific units of work which form part of the ICT rolling programme.

1.5.2 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.

1.5.3 Enlisting parents' support

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

Reviewed: September 2016

Signed: …… Rev. Clare King (Chair of Governors)

Next review – September 2017

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks National Grid for Learning (
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation.	School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication for websites other than school. Pupils' full names and other personal information should be omitted.	Making the News Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be clearly identified. File names should not refer to the pupil by name.	Making the News Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Skype FlashMeeting
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum

		Imperial War Museum