**Hope Primary School**
**E-Safety Policy**

This E-Safety Policy is part of the School Improvement Plan and relates to other policies including those for Computing, Anti-bullying and Child Protection.

## 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 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 systems to support safe use. 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.

### 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 and clarification / advice will be sought as necessary.

**E-mail** (for example as a means of communication between schools in neighbouring villages and in different continents)

Pupils may only use approved e-mail accounts on the school system and email usage should be supervised and monitored by a staff member. Alternatively, whole class or group email addresses may be used for communication outside school. Pupils must immediately tell a teacher offensive e-mail is received. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. E-mails 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. Attachments to emails may not be opened unless the author is known.

### Published content and the school web site

The contact details on the Web site should be the school address, e-mails and telephone numbers. 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. No content should be added to the site without the head teacher's approval.

**Publishing pupil's images and work**
Photographs that include pupils will be selected carefully. 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.

**Social networking and personal publishing**
The school will educate older pupils in the safe use of age appropriate social networking sites or mobile sharing apps. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give 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 brings a range of dangers for primary aged pupils and should be carefully monitored. Staff will be asked to refrain from communicating with pupils via social networking sites and also parents/carers where it can compromise the professional relationship between both parties.

**Managing filtering**
The school will work to ensure systems to protect pupils are reviewed and improved. If staff or pupils come across unsuitable on-line materials, it must be reported to the head teacher or E-Safety Coordinator. Staff will ensure that regular 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 by pupils during lessons or formal school time. Parents wishing their child to have a mobile phone in school need to write a letter to the Head teacher. Mobile phones need to be handed in at the office at the start of the day and collected at home time. If a mobile phone is found in school it will be confiscated and arrangements made for collection by a parent. The sending of abusive or inappropriate text messages is forbidden. The appropriate use of Learning Platforms will be discussed at the time of their implementing within the school.

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

**Policy Decisions**

**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 connected to the school network. Neither the school nor DCC can accept liability for any 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 posted around the school and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored. Training in E-Safety will be based on the materials from CEOP and embedded within the school Curriculum maps and/or the Personal Social and Health Education (PHSE) curriculum. Pupils will be asked to sign an acceptable use agreement.

**Staff and the e-Safety policy**
All staff will be given the School E-Safety Policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Staff will be asked to sign an acceptable use agreement.

**Enlisting parents' support**
Parents' and carers' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Web site. Parents will receive a copy of their child's cceptable use agreement and will be asked to go through it with their child. Parents will sign an agreement to confirm they understand the school's procedures on acceptable use of the Internet and will support the school's E-Safety policy. This will go out with the Home School Agreement, Photo Permission and Low Risk Day visits forms in September each year.

**Failure to Comply**
Failure to comply in any way with the policy will be considered as a serious risk to children's wellbeing and safety and all incidents of non-compliance will be investigated by a senior member of staff.

**Monitoring/review of ICT and E-Safety policy**
This policy will be regularly evaluated and updated in accordance with the School Development Plan to ensure that:
All new staff are aware of the current practice in ICT.
New developments and initiatives are taken into account.
Ideas of new staff are incorporated.
Policy and practice are matched.

**Date:** 22.5.15

**Next Review Date:** July 2016

**Signed _____ Head Teacher**

**Signed _____ Chair of Governors**

**This policy will be reviewed annually from date of approval from governing body**