WHITLEY CHAPEL CHURCH OF ENGLAND CE FIRST SCHOOL

E-SAFETY POLICY

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, 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 reflects the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including the Acceptable Use policy, ICT, anti bullying, child protection and PSHE.

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

- Responsible ICT use by all staff and pupils: encouraged by education and made explicit through published polices.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the NCC Network including the effective management of filtering.
- Monitoring provided by Central Policy Enterprise, installed on all computers. Termly reports will be reviewed by the headteacher and action taken if necessary.

School e-Safety policy

- The school has appointed a member of staff responsible for e-safety: Miss Jenny Morgan
- The e-safety Policy and its implementation will be reviewed regularly.

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. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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 Head teacher.
- 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 will be updated regularly.

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.
- The forwarding of chain letters is not permitted.
- Pupils have been advised to only open attachments from known and safe sources or to check with an adult if in doubt.

Published content and the school website

- The contact details on the website 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 website or Blog, particularly in association with photographs.
- Long term, written permission will be obtained from parents or carers when children start school to allow photographs of pupils to be published on the school website.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal information of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, e.mail address, names of friends, specific interests and clubs etc.

- Pupils and parents will be advised of the possible risks that the use of social network spaces outside school, primary aged pupils can be exposed to.

Managing filtering

- The school will work with NCC to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to member of staff responsible for e-Safety.

The member of staff responsible for e-Safety will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Learning Platforms – school360

- The member of staff responsible for e-Safety will monitor the usage of school360 by pupils and staff in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised about acceptable conduct and use when using school360
- Only members of the current pupil, parent/carers and staff community will have access to school360
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

Managing mobile phones and personal devices

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.

Use of mobile storage devices (e.g memory sticks)

- Copying of files to non-encrypted USB devices like memory sticks, cameras, external floppy disk drives and external hard drives. Staff will only be able to save files to an authorised and encrypted USB memory stick or an approved device which have been supplied by NCC Information Services.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit before use in school is allowed.

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

- All staff must read and sign the Acceptable ICT Use Policy
- At Foundation Stage and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access will either be supervised by an adult and restricted to websites identified in teachers planning, or internet searches will use a search engine specifically designed for children such as http://kids.yahoo.com www.askkids.com www.bbc.co.uk/cbbc/find
  Image searches http://gallery.nen.gov.uk/gallery-segfl.html
  www.dorlingkindersley-uk.co.uk/static/html/clipart/clipart_home.html

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. Neither the school nor NCC can accept liability for the material accessed, or any consequences of Internet access.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff/head teacher.
- 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 the school child protection procedures.

Communications Policy - Introducing the e-safety policy to all pupils

- E-safety rules will be posted beside computers and discussed with the pupils as appropriate.
- Pupils will be informed that network and Internet use will be monitored.
- E-Safety will be taught to pupils to raise the awareness and importance of safe and responsible internet use.

Useful e–Safety programmes include:

E-safety section in Nortle

- Think U Know: www.thinkuknow.co.uk
- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk

- Safe: www.safesocialnetworking.org

Staff and the e-Safety policy

- All staff will have access to the School e-Safety Policy.
- Staff have signed up to an Acceptable Use Policy.
- Staff should be aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

- Parents attention will be drawn to the School e-Safety policy, for example, in newsletters, the school prospectus and on the school website.
- Adults working with pupils using the Internet will be made aware of the School e-Safety Policy.