THE FEDERATION OF

LOWER HALSTOW & NEWINGTON CEP SCHOOLS

E-Safety Policy

Approved	Co-Ordinator	Review Date
	T. Godfrey	Autumn 2013
Nov 13		Autumn 2014
30.09.14		Autumn 2015

Lower Halstow and Newington E-safety Policy

Who will write and review the policy?

Across the Federation the schools each have an e-safety coordinator, Mrs Cathy Walker for Lower Halstow and Trudi Godfrey for Newington. The e-safety coordinator will help to promote the awareness of e-safety to both staff and children.

Our e-safety policy has been written by staff across the federation, building on the KCC e-safety policy and government guidance and linking with the schools safeguarding, behaviour and anti-bullying policies. It has been agreed by the Senior Leadership Team and approved by the Governors.

An e-safety Governor has been appointed:

The e-safety policy and its implementation will be reviewed annually.

Why is the Internet Important?

The Internet is an essential element in the 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. Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

How does Internet use benefit education and enhance learning?

He school Internet access will be designed to enhance and extend education. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet Use.

It is sometimes used for collaboration across networks of schools, support services and professional associations.

The schools will ensure that the copying and subsequent use of Internet-derived materials by staff and pupils complies with copyright law. Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils. Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Pupils will use age-appropriate tools to research Internet content.

Managing Information Systems

How will information systems security be maintained?

The security of the school information systems and users will be reviewed regularly. Virus protection will be updated regularly by EIS. The use of user logins and passwords to access the school network will be enforced.

How will email be managed?

Pupils may only use approved email accounts for school purposes. Pupils must immediately tell a designated member of staff if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult. Whole -class or group email addresses will be used in primary schools for communication outside of the school. Staff will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team. Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be. Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published. The website should comply with school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupils' images or work be published?

Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before images of pupils are electronically published. Pupils work can only be published with their permission or their parents/ carers. Pupils work can only be published with their permission or their parents / carers.

How will social networking, social media and personal publishing be managed?

The school will control access to social media and social networking sites. Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.

Staff wishing to use Social Media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.

Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupil will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.

Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.

How will filtering be managed?

The school works with the LA, DCSF and EIS to ensure systems to protect pupils are reviewed and improved. Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day but is carried out by EIS. This will include filtering appropriate to the age of the pupils.

If staff or pupils discover an unsuitable site, the URL should be reported to the e-safety co-ordinator. The ICT technician will then be told and contact made with EIS.

How will videoconferencing be managed?

We are still developing work within videoconferencing. At present we have only used secure networks to link with other schools. As we develop this are we will:

- Ensure all videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Ensure pupils ask permission from a teacher before making or answering a videoconference call.
- Ensure that videoconferencing will be supervised appropriately for the pupils' age and ability.
- Ensure parents and carers consent should be obtained prior to children taking part in videoconferences.

How are emerging technologies managed?

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Mobile phones are not allowed in school and if children do bring in mobile phones, they will be kept safe in the office.

Staff use the school phone when contact with pupils and parents is required. They are not to use their own mobiles.

How should personal data be protected?

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

How will Internet access be authorised?

The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.

All staff will read and sign the School Acceptable Use Policy before using any school ICT resources.

At Key Stage 1, access to the Internet is by adult demonstration with occasional directly supervised access to specific, approved, online materials.

At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Appropriate search engines include: - http://www.askkids.com/

How will risks be assessed?

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

How will the school respond to any incidents of concern?

All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc). The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log. The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately. The school will manage e-Safety incidents in accordance with the school discipline/ behaviour policy where appropriate. The school will inform parents/carers of any incidents of concerns as and when required. After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required. Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police. The school will contact to the Area Children's Officer or the County e-Safety Officer if we are unsure how to proceed with any incidents of concern.

How will e–Safety complaints be handled?

Complaints about Internet misuse will be dealt with under the School's complaints procedure. Any complaint about staff misuse will be referred to the Executive Head teacher / Head of School.

All e–Safety complaints and incidents will be recorded by the school, including any actions taken. Parents and pupils will need to work in partnership with the school to resolve issues.

All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community.

How is the Internet used across the community?

The school will liaise with local organisations to establish a common approach to e–Safety. The school will be sensitive to Internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice. The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

How will Cyberbullying be managed?

Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour. There are clear procedures in place to support anyone in the school community affected by cyberbullying. All incidents of cyberbullying reported to the school will be recorded. There will be clear procedures in place to investigate incidents or allegations of Cyberbullying. Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos. Advice from the local PCSO or police office will be sort if required.

Sanctions for those involved in cyberbullying may include:

The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to delete content.

Internet access may be suspended at school for the user for a period of time. Other sanctions for pupils and staff may also be used in accordance to the schools anti-bullying, behaviour policy or Acceptable Use Policy. Parent/carers of pupils will be informed. The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms / Network Areas be managed?

SLT and staff will regularly monitor the usage of the LP 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 the LP / Network Areas. Only members of the current pupil, parent/carers and staff community will have access to the LP. All users will be mindful of copyright issues and will only upload appropriate content onto the LP. When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

How will mobile phones and personal devices be managed?

The use of mobile phones and other personal devices by staff in school will be decided by the school and covered in the school Code of Conduct. Mobile phones are not allowed in school and if children do bring in mobile phones, they will be kept safe in the office.

The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

Children should not bring camera phones to School. Children on discussion with the Executive Head Teacher/Head of School may bring a phone to School in extreme circumstances, but this must be kept locked away in the School Office.

School staff may confiscate a phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device might be searched by the Senior Leadership team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

Communication Policy

How will the policy be introduced to pupils?

All users will be informed that network and Internet use will be monitored. An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils. The schools will take part in Safer Internet Day in February each year. E-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access. Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas. Particular attention to e-Safety education will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

The e–Safety Policy will be formally provided to and discussed with all members of staff. Staff training on e-safety will be linked to Safeguarding and updated regularly. To protect all staff and pupils, the school will implement Acceptable Use Policies. Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

How will parents' support be enlisted?

Parents' attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website. A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use, or highlighting e–Safety at other attended events e.g. parent evenings and sports days. Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement. Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it's implications with their children.

Advice on useful resources and websites, and educational and leisure activities which include responsible use of the Internet will be made available to parents.

Useful e–Safety programmes include:

- Think U Know: www.thinkuknow.co.uk

- Childnet: www.childnet.com
- Kidsmart: www.kidsmart.org.uk
- Orange Education: www.orange.co.uk/education
- Safe: www.safesocialnetworking.org