Reviewed January 2017

Believe to achieve

Whitley Memorial First School

E-SAFETY POLICY

School Name: Whitley Memorial First School
Date of policy implementation: November 2014
Date of next review: November 2016

(This E-Safety policy has been based on the model policy approved by Kent County Council Children, Families and Education Directorate and recommended by Northumberland and North Tyneside ICT Consultants as being appropriate for use by Northumberland schools for a basis for establishing their own policies)

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective eSafety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our e-Safety Policy, as part of the wider safeguarding agenda, outlines how Whitley Memorial First School will ensure our school community is prepared to deal with the safety challenges that the use of technology brings.

What is E-Safety?

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, iPads, 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 Computing, Behaviour, Bullying, Curriculum, Data Protection and Security.

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 connections including filtering.
- National Education Network standards and specifications.

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 across the school.
- The filters are very strict and controlled by the LA.
- Staff and pupils have different access rights to the Internet in school, for example pupil logins are automatically blocked for sites such as You Tube but staff logins have access.
- 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 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 will be updated regularly by Northumberland NCC
- Security strategies will be discussed with the Northumberland ICT Team

E-mail

- Pupils only learn about e-mail through using internal software within the school network.
- 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.

Published content and the school web site

- 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 Headteacher and Computing Co-ordinator 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** include pupils whose parents have not given permission
- Pupils' names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

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 and explicitly taught 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.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Facebook page.

Managing filtering

- PCE Monitoring is used across the county network and NCC uses a strict filtering system.
- The school will work with the LA, DfE 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 Co-ordinator.
- Any breaches of e-safety will follow the *Responding to e-Safety Incident/ Escalation Procedures* (Appendix 1)
- The e-Safety Co-ordinator and computer technician, in conjunction with the Northumberland ICT Team 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 during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff phones may be used on a school visit in an emergency but the 'Acceptable User Policy' must be adhered to.
- Staff are not permitted to use their own mobile phones at any time during school hours (see *Mobile Phone Policy*) except when accompanying children on a school trip.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Where ever possible personal data will be stored only on encrypted storage devices and on password protected hardware.
- On-line back up to 'cloud storage' must be UK based as part of the NCC *Disaster Recovery Plan*.

Policy Decisions

Authorising Internet access

- All staff must read and sign the '*ICT Acceptable Use Policy*' before using any school ICT resource, including PCs, iPads and laptops.
- At Whitley Memorial First School any access to the Internet will be closely supervised by teaching staff.
- Children have directly supervised access to specific, approved on-line sites and materials eg Education City, NorTLE, School360.
- Visitors to the school have no access to the computer system or Internet unless we provide them with login details.

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 NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

- In the event of an e-safety issue all staff will refer to *Responding to e-Safety Incident/ Escalation Procedures* (Appendix 1)
- E-safety incidents will be recorded in the *e-Safety Incident Log* (Appendix 2)

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 Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Parents will be informed of the complaints procedure (available on Website)

Communications Policy

Introducing the e-safety policy to pupils

- E-safety will be taught across all year groups (Reception – Year 4) at the beginning of each year.
- E-safety rules will be posted in the Computer Suite and discussed with the pupils at the start of each year.
- Pupils will be given age appropriate information, linked to their e-safety teaching, to take home and share with parents.
- All pupils (Year 1- Year 4) must log on to the computers and network using their own login name and password.
- Pupils will be informed that Internet use will be monitored.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- All teaching staff will be expected to sign the school's *AUP*.
- Staff should be aware that Internet traffic can be monitored and 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 in newsletters and on the school website.
- Parents will be invited to attend an e-safety information meeting in early 2015.
- Information about e-safety will be sent home to parents and be made available on the school website.

Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for Computing, Behaviour, Bullying and for Child Protection.

- The school's e-Safety Co-ordinators are Miss Abigail Evans, Computing Co-ordinator and Mrs Sally Hobson, Headteacher.
- The school governor with specific responsibility for computing and e-safety is Mrs Rachel Crawford.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.

Policy approved and adopted:

Due for review: November 2016 Reviewed - January 2017

Signed: Abigail Evans

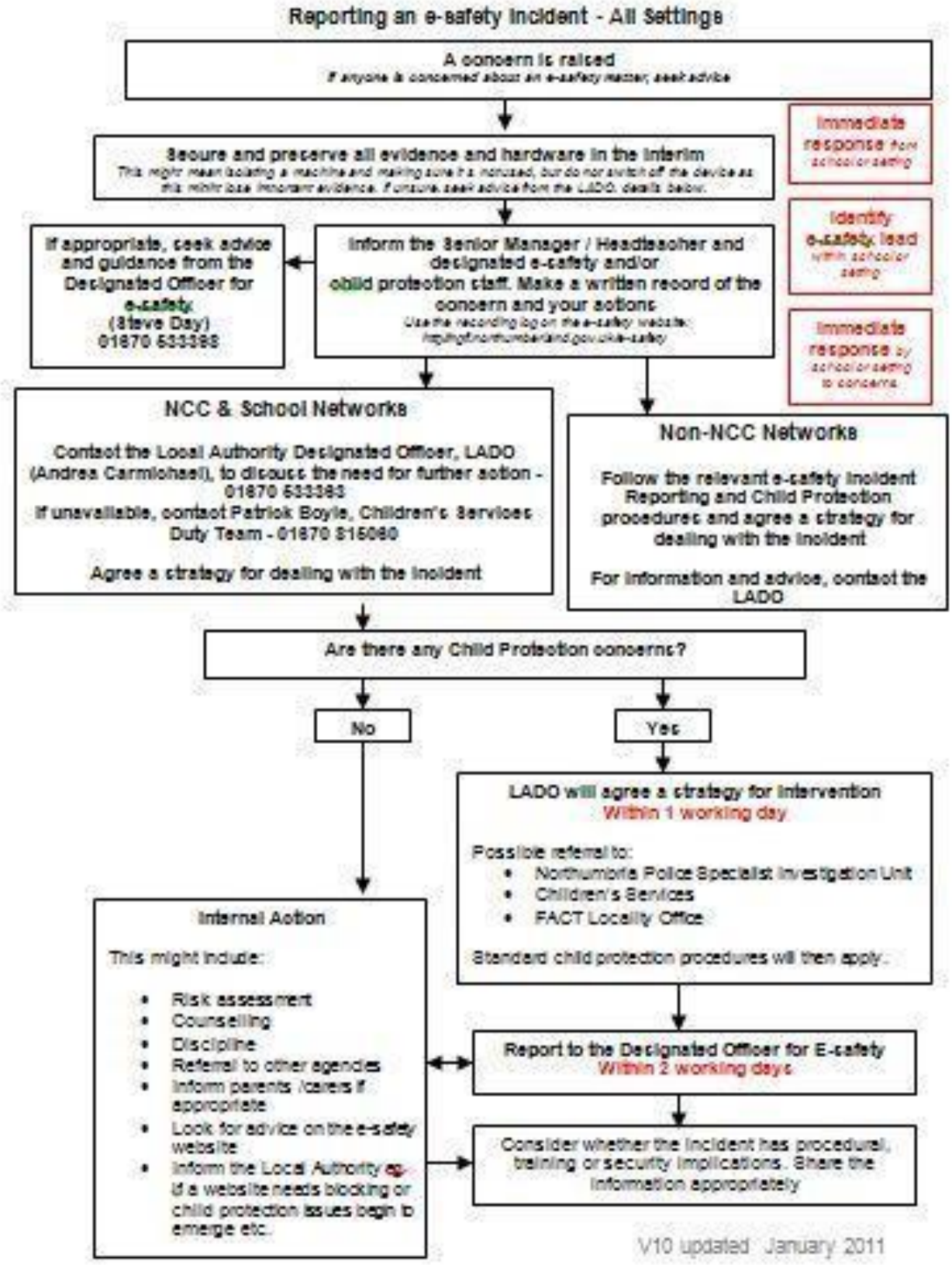
Head Teacher: Sally Hobson

Chair of governors: Pam Lee 6.3.17

This policy should be read in conjunction with:

Behaviour
Child protection
Staff Code of Conduct
Whistleblowing Anti-bullying
Health & Safety
Allegations against staff Attendance
PSHE
Administration of medicines Drug Education
Sex and Relationships Education
Physical intervention
Social networking Policy
Cameras and mobile phone usage IT Security Policy
Recruitment and Selection
Child Sexual Exploitation
Safeguarding

Appendix 1: Responding to e-Safety Incident/ Escalation Procedures



Appendix 2: e-Safety Incident Log

Northumberland County Council

Information Security Event Report

This Event Report Form Compiled By: Name Title Date	
This Event Report Form Managed By: Name Title Date	
Nature of Event (Violation, Breach, Weakness, Other)	
Date of Report	
Time of Report	
Reported To:	
Person Making Report Position/Role/Status Name of Line Manager Title	
Individuals/Teams/Systems/ Applications/Equipment/Locations Involved	
Event Witnessed/Experienced:	
Incident Ref Number	

Initial Response by ISO	
Other Officers Involved in Response/s	
Follow up Action	
Evidence Collected (and where retained)	
Referral to Internal Audit Required Y/N? Date Referred Internal Audit Officer	
Closure Action	
Review Date if required	