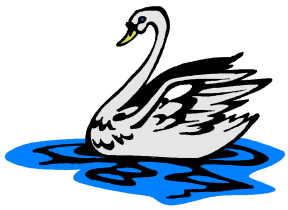

E-Safety Policy

Kingsbury Primary School

1. WHY WRITE AN E-SAFETY POLICY?

1.1 Pupils interact with the Internet and other communications technologies such as mobile phones on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction are both greatly beneficial but can occasionally place young people in danger.

1.2 E-safety comprises all aspects relating to children and young people and their safe use of the Internet, mobile phones and other technologies, both in and out of school. It includes education on risks and responsibilities and is part of the 'Duty of Care' which applies to everyone working with children. A national E-Safety drive is being led by the Child Exploitation and Online Protection Centre (CEOP).

2.WHAT IS E-SAFETY?

2.1 E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children, young people and adults about the benefits, risks and responsibilities of using information technology and provides safeguards and awareness for users to enable them to control their online experiences.

2.2 The Internet is an open communications channel, available to all. Applications such as the Web, e-mail, blogs and social networking all transmit information over the fibres of the Internet to many locations in the world at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

2.3 Some of the material on the Internet is published for an adult audience and is unsuitable for children and young people. For instance, there is information on weapons, crime and racism that would be more restricted elsewhere. It is important that children and young people are made aware of appropriate behaviour in relation to contacting others and they must also understand that publishing personal information could compromise their security.

2.4 As a school we need to protect pupils and staff but also to protect ourselves from legal challenge. The law is catching up with Internet developments: it is an offence to store images showing child abuse and to use Internet communication to 'groom' children. The Computer Misuse Act 1990 (http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm) makes it a criminal offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". We can help protect ourselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, the Shipston Primary is aware that a disclaimer is not sufficient to protect the school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken to

p r o t e c t users.

3. INTRODUCTION

3.1 The school has appointed an E-Safety Co-ordinator. At Kingsbury Primary School the E-Safety Co-ordinator will be the same person as the Designated Child Protection Co-ordinator is also as the roles overlap.
3.2 The ICT Leader will assist the E-Safety Co-ordinator with technical and curriculum matters.
3.3 Our E-Safety Policy has been written by the school, building on the Warwickshire ICT Development Service E-Safety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by Governors and PTA.
3.4 The E-Safety Policy will be reviewed annually.

4. WHY IS INTERNET USE IMPORTANT?

4.1 Internet use is part of the statutory curriculum and a necessary tool for learning.
4.2 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.
4.3 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 information and business administration systems.
4.4 Internet access is an entitlement for students who show a responsible and mature approach to its use.
4.5 Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

5. HOW DOES THE INTERNET ENHANCE LEARNING?

5.1Benefits of using the Internet in education include: -
• Access to world-wide educational resources including museums and art galleries;
• Inclusion in the National Education Network which connects all UK schools;
• Educational and cultural exchanges between pupils world-wide;
• Vocational, social and leisure use in libraries, clubs and at home;
• Access to experts in many fields for pupils and staff;
• Professional development for staff through access to national developments, educational materials and effective curriculum practice;
• Collaboration across support services and professional associations;
• Improved access to technical support including remote management of networks and automatic system updates;
• Exchange of curriculum and administration data with the LA and DCSF;
• Access to learning wherever and whenever convenient.

5.2 The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
5.3 Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
5.4 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.
5.5 Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

5.6 Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6. EVALUATING INTERNET CONTENT

6.1 If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service 01926 414 100, and where appropriate, the school e-safety officer.
6.2 Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
6.3 In Upper Key Stage 2, pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
6.4 Pupils in Key Stage 2 will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

7. MANAGING INTERNET ACCESS

7.1 The security of the school information systems will be reviewed regularly.
7.2 Through Warwickshire ICT Development Service, Virus protection will be installed and updated regularly.
7.3 The school uses the Warwickshire Broadband with its firewall and filters.
7.4 The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Service.
7.5 Portable media may not used without specific permission and a virus check.
7.6 Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
7.7 Files held on the school's network will be regularly checked. Files on the system are checked y WCC and any issues spotted are raised with school.

8. EMAIL

8.1 Pupils may only use approved e-mail accounts on the school system.
8.2 Pupils must immediately tell a teacher if they receive offensive e-mail.
8.3 Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
8.4 Use of words included in the Policy Central 'banned' list will be detected and logged.
8.5 Access in school to external personal e-mail accounts may be blocked.
8.6 Excessive social e-mail use can interfere with learning and may be restricted.
8.7 E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
8.8 The forwarding of chain letters is not permitted.

9. PUBLISHED CONTENT AND THE SCHOOL WEBSITE

9.1 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.
9.2 Email addresses should be published carefully, to avoid spam harvesting.
9.3 The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
9.4 The Website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

10. PUBLISHING STAFF AND PUPIL'S IMAGES AND WORK

10.1 Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name.

10.2 Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
10.3 Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.

10.4 Images of staff and governors should not be published without consent.

11. SOCIAL NETWORKING AND PERSONAL PUBLISHING
11.1 Social networking sites and newsgroups will be blocked unless a specific use is approved.
11.2 Pupils are advised never to give out personal details of any kind which may identify
them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, email address, names of friends, specific interests and clubs etc.
11.3 Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school or shopping centre.
11.4 Teachers' official blogs or wikis should be password protected. Teachers should be advised not to run social network spaces for pupils on a personal basis.
11.5 Staff and pupils should be advised on security and encouraged to set passwords,
Deny access to unknown individuals and instructed how to block unwanted communications. They should be encouraged to invite known friends only and deny access to others.
11.6 Pupils should be advised not to publish specific and detailed private thoughts.
11.7 Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
12.MANAGING FILTERING
12.1 The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.
12.2 If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety Co-ordinator.
12.3 Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
13. MANAGING VIDEO-CONFERENCING
13.1 All video-conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
13.2 IP video-conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
13.3 Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
13.4 External IP addresses should not be made available to other sites.
13.5 Video-conferencing contact information should not be put on the school website.
13.6 The equipment must be secure and if necessary locked away when not in use.
13.7 School video-conferencing equipment should not be taken off school premises

without permission. Use over the non-educational network cannot be monitored or controlled.
13.8 Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
13.9 Video-conferencing should be supervised appropriately for the pupils' age.
13.10 Responsibility for the use of the video-conferencing equipment outside school time needs to be established with care.
13.11 Only key administrators should be given access to the video-conferencing system web or other remote control page available on larger systems.
13.12 Unique log on and password details for the educational video-conferencing services should only be issued to members of staff and kept secure.
13.13 When recording a lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of video-conference should be clear to all parties at the start of the conference.
13.14 Recorded material shall be stored securely.
13.15 If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).
13.16 Video-conferencing is a challenging activity with a wide range of learning benefits.
Preparation and evaluation are essential to the whole activity.
13.17 Establish dialogue with other conference participants before taking part in a video-conference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.

14. MANAGING EMERGING TECHNOLOGIES

14.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
14.2 Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
14.3 The school should investigate cellular wireless, infra-red and Bluetooth communication and decide a policy on phone use in school.

15. PROTECTING PERSONAL DATA

15.1Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

16.AUTHORISING INTERNET ACCESS

16.1The school will maintain a current record of all staff and pupils who are granted Internet access.
16.2 All users must read and abide by the 'Acceptable ICT Use Policy' before using any school ICT resource.
16.3 At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
16.4 Parents will be informed that pupils will be provided with supervised Internet access.
16.5 Parents will be asked to read and acknowledge the school's 'Acceptable ICT Use Policy'.

17. ASSESSING RISKS

17.1 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 WCC can accept liability for the material accessed, or any consequences of Internet access.
17.2 The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy monitored. WCC liaise with headteacher re any issues. Staff and pupils will raise any concerns which are recorded in school and the Headteacher monitors this. Policy will be amended if issues are raised.
17.3 The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
17.4 Methods to identify, assess and minimise risks will be reviewed regularly.

18. HANDLING E-SAFETY COMPLAINTS

18.1 Complaints of Internet misuse will be dealt with by a senior member of staff.
18.2 Any complaint about staff misuse must be referred to the Headteacher who should use the agreed WCC procedures. We will follow the flow diagram attached at the end of this policy.
18.3 Any issues for parents, children or staff should be brought to the attention of the headteacher who will follow the flow diagram at the end of this policy.
18.4 Parents and pupils will need to work in partnership with staff to resolve issues.
18.5 Sanctions within the school discipline policy include: -

- pupil interview;
- informing parents or carers;
- detentions;
- removal of Internet or computer access for a period.

19. COMMUNITY USE OF THE INTERNET

19.1 The school will liaise with local organisations to establish a common approach to E-safety.
19.2 The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

20. INTRODUCING THE E-SAFETY POLICY TO PUPILS

20.1Rules for Internet access will be posted in all networked rooms.
20.2 Pupils will be informed that Internet use will be monitored.
20.3 An E-Safety training programme will be introduced to raise the awareness and importance of safe and responsible Internet use.
20.4 Instruction in responsible and safe use should precede Internet access.
20.5 A module on responsible Internet use will be included in the PSHE and ICT programmes of learning covering both school and home use.

21. STAFF AND THE E-SAFETY POLICY

21.1 All staff will be given the School E-Safety Policy and its importance explained.
21.2 Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
21.3 All staff should read and sign the Warwickshire Acceptable ICT Use Policy.
21.4 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
21.5 Staff development in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

22. ENLISTING PARENTS SUPPORT

22.1 Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Website.
22.2 Internet issues will be handled sensitively to inform parents without alarm.
22.3 A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.

22.4 Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
22.5 Interested parents will be referred to organisations listed in section 3 E-Safety Contacts and References.

Appendix 1
Web Links
Becta has produced these booklets that are essential reading:
• Safeguarding children in a digital world (Feb 2006) Ref: BEC1-15401
• E-safety: Developing whole-school policies to support effective practice (revised Feb
2006) Ref: BEC1-15402
• Signposts to safety at KS1 and KS2 (April 2007) Ref: BEC1-15488
• Signposts to safety at KS3 and KS4 (April 2007) Ref: BEC1-15489
• Using technology safely in schools – an essential guide (April 2007) Ref: BEC1-15461
• AUPs in context: Establishing safe and responsible online behaviours (February 2009)
Ref: BEC1-15648
Useful E-safety programmes include:
• Think U Know
www.thinkuknow.co.uk
• Childnet
www.childnet-int.org/kia
• Kid Smart
www.kidsmart.org.uk/
• The BBC's Chat Guide
www.bbc.co.uk/onlinesafety/
• CBBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/
E-Safety Contacts and References:
Warwickshire ICT Development Service Desk
01926 414100
Safety in Schools and Schools E-Safety Policy
http://www.clusterweb.org.uk?esafety
WMNet E-Safety Pledge
http://www.wmnet.org.uk/esafetypledge/
Schools E-Safety Blog
http://www.clusterweb.org.uk?esafetyblog
Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk/contact_us.html
Virtual Global Taskforce – Report Abuse
http://www.virtualglobaltaskforce.com/
Think U Know website
http://www.thinkuknow.co.uk/
Becta
http://www.becta.org.uk/schools/safety
Internet Watch Foundation
http://www.iwf.org.uk/
Internet Safety Zone
http://www.Internetsafetyzone.org.uk/
KidSMART
http://www.kidsmart.org.uk/
NSPCC
http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Childline
http://www.childline.org.uk/
NCH – The Children's Charity
http://www.nch.org.uk/stories/index.php?i=324
NCH – Digital Manifesto
http://www.actionforchildren.org.uk/uploads/media/29/5706.pdf
CBBC Safe Surfing including the Chat Guide
http://www.bbc.co.uk/cbbc/help/safesurfing/
Parents' Centre
http://www.parentscentre.gov.uk/usingcomputersandtheInternet/
The Warwickshire Safeguarding Children Board have provided guidance and contacts in their publication, *Keeping Children Safe and Healthy* ('The Blue Book'), should you be concerned about the Internet usage of a child, young person or member of staff.
http://www.warwickshire.gov.uk/Web/corporate/pages.nsf/Links/D45A0720FD40CFC580256EE4004C6C70

Blogging Policy Kingsbury Primary

1. AIMS AND OBJECTIVES

1.1 Whilst blogging has been around for 10+ years, more and more schools are now giving their pupils a voice and an audience through blogging. These are mainly in the form of class blogs but can also be in the form of project blogs or individual pupil blogs.

1.2 This policy will outline the safe management of setting up and running a blogging platform. A successful blog can:

- Safely give your pupils a wider audience for their learning
- Encourage reluctant learners to participate and succeed
- Allow pupils to receive feedback safely from many different people
- Allow your pupils to peer assess each other's learning
- Encourage parental engagement
- Provide a platform that you can embed Web2.0/3.0 tools into
- Promote your pupils' learning across the globe

2 E-SAFETY

2.1 Blogging involves pupils working on a blog whilst in school and also at home. To be able to post, pupils need to log into the blog either using an individual sign in or a class sign in. The advantages of individual sign in is that this gives more ownership to each pupil. Most blog platforms allow accounts to have different permissions. Contributor is the lowest level that allows a user to post. A contributor can submit a post for review, however, this will need to be authorised by the admin before it appears on the blog. The 'Contributor' permission level is recommended for Primary School. Any other permission level above that of 'Contributor' will allow posts to be viewable as soon as the pupil clicks 'Submit'.

2.2 Each child has access to a blog through the safe and secure Welearn365 learning portal provided by the Warwickshire Local Authority ICT Development Service.

2.3 First names only are used for pupils on photos

2.4 Each pupil with a unique log in has been told to keep this private. If a pupil or parent thinks their log in needs changing, this can be done in the 'profile' setting on the dashboard. Parents and pupils are to contact the ICT Leader should this need clarifying.

3. BLOG RULES

3.1 Using a blog safely is the most important thing about being a blogger. The following rules, if followed, will minimise any risks and will ensure that you will stay safe whilstblogging:

3.2 **Don’ts**

1. Never give away any personal information about your location or identity.
2. Don't post pictures of yourself without specific permission from your teacher or parents.
3. Never give out your log in details to anyone.
4. Don't use text language in your posts.

3.3 **Do’s**

1. Post about whatever you like.
2. If you receive a comment, it is polite to respond, say thank you and reply to a question if they have left one.
3. Comment on other people's posts too. Blogging is about commenting and posting!
4. If your post doesn't appear straight away, you teacher might be busy, do be patient.
5. Try to post about things that your audience would like to read.
6. If you see anything that shouldn't be on your screen, do tell your teacher or parents immediately.
7. Do visit other class blogs regularly to read and comment. This helps people come back to your blog.
8. Try to show off your best work/writing whilst blogging and use the tips people suggest to you to improve.
9. Always tag your posts with your first name and include key words specific to your post.

4. THE ROLE OF THE BLOG ADMINISTRATOR

4.1 The blog admin normally is the class teacher. This responsibility as gatekeeper is key to ensuring safety for the pupils using the blog. The following guidelines should be followed if a successful flowing blog is to be achieved:

• Visit the blog regularly. It is better to visit short and often than catching up once a week. Your bloggers will appreciate comments and posts being approved quickly!
• If you use a shared computer, log out at the end of each session.
• Promote the links on the class blog to the parents and the wider community. Twitter is a great way to promote a blog.
• A blog can take a while to gather momentum and an audience. Be patient... the audience will come!
• Your users will need to log in. For a quick solution, you can have one Username and Password for your class to get posts on the blog. However, for older pupils of 7+ they are more than capable of having their own log in.
• The safest permission setting for your blogger is 'Contributor'. This will allow them to log in and post but the blog admin will need to approve each post.
• Mention the blog in assemblies and have it on display at parent evenings or school events, a blogging culture will soon be established!
• Make sure each blog looks different in your school. This will help keep the interest high for the pupils from year to year.
• Visit other blogs regularly and promote these to your class through links on your blog. What goes around comes around with blogging and strong loyal communities will form quickly.

Kingsbury Primary School
Mobile Phone Policy

Rationale

Mobile phones are now a feature of modern society and an increasing number of our staff and pupils own one.

Increasing sophistication of mobile phone technology presents a number of issues for schools:

• The high value of many phones

• The integration of cameras into phones leading to potential child protection and data protection issues.

• The potential to use the phone eg for texting whilst on silent mode.

Children:

Pupils are not permitted to have mobile phones at school or on trips during school time, including clubs

If in the rare event of a parent wishing for his/her child to bring a mobile phone to school to contact the parent after school: the parent must speak to the headteacher/deputy and the phone must be handed in , switched off, to the secretary's office first thing in the morning and collected from the office by the child at home time(the phone is left at the owner's own risk). It can be collected by the child at hometime.

If a child breaches these rules the phone will be confiscated and given in to the main office. It will be returned to the child after a discussion with parents.

This policy should be read in conjunction with the school's other policies in particular the Behaviour Policy.

Staff:

Phones must not be used for any purpose (eg phoning, texting, surfing the internet, taking photos, checking the time, taking videos) during lesson time. . If there are extreme circumstances (eg. acutely sick relative) the member of staff will have made the principal aware of this and can have their phone incase of having to receive an emergency call. If possible they will leave their phone with the office staff.

Phones must be stored out of sight during lesson time.

Phones must always be switched off or on silent mode during class time and meeting time unless permission has been granted in advance by senior staff..

Phones will never be used to take photographs of children or to store their personal data.

. K Hanson

Review date Autumn 2017