E-safety Policy

Howes Primary School

SEPTEMBER 2018

HOWES PRIMARY E-SAFETY POLICY

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, Howes 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 protect users.

3. INTRODUCTION

3.1
The school has an E-Safety Leader. The E-Safety Leader is also the Computing Leader. The E-Safety Leader works closely with the Designated Officers for Child Protection.
3.2
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.
3.3
The E-Safety Policy will be reviewed every two years.

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?
5.1
Benefits 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 DfE;
• 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 the school E-Safety Leader.

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
Virus protection will be installed and updated regularly.

7.3
Portable media may not used without specific permission and a virus check.

7.4
Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.

7.5
Files held on the school's network will be regularly checked.

7.6

The Computing Leader and Headteacher will review system capacity regularly working with the IT Technician.

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 an 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

Access in school to external personal e-mail accounts may be blocked.

8.5

Excessive social e-mail use can interfere with learning and may be restricted.

8.6

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.

8.7

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.

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 and run from the school website. 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 Coventry LA 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 Leader.
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

Parents and Guardians should agree for their children to take part in videoconferences, probably in the annual return.

13.11

Responsibility for the use of the video-conferencing equipment outside school time needs to be established with care.

13.12

Only key administrators should be given access to the video-conferencing system web or other remote control page available on larger systems.

13.13

Unique log on and password details for the educational video-conferencing services should only be issued to members of staff and kept secure.

13.14

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.

13.15

Recorded material shall be stored securely.

13.16

If third-party materials are to be included, check that recording is acceptable to avoid infringing the owners' Intellectual Property Rights (IPR).

13.17

Video-conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.

13.18

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
15.1
Personal data will be recorded, processed, transferred and made available according to the GDPR 2018.

16. AUTHORISING INTERNET ACCESS
16.1
The 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 CCC 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.
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 CCC procedures.
18.3
Pupils and parents will be informed of the complaints procedure.
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: -
• 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

20.1
Rules 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
Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
21.4
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 the newsletter 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
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:
Safety in Schools and Schools E-Safety Policy
http://www.clusterweb.org.uk?esafety
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/

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/