Howes Primary School

E-Safety Policy

Contents

1 Why Write an E-Safety Policy?

Pupils interact with the Internet and other communication 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.

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). The annually updated Government document 'Keeping Children Safe in Education' provides information about organisations who can offer support and provides advice about online safety remote learning procedures.

2 Why is E-Safety Important?

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.

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, however, also poses potential risks.

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, sex, 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.

As a school, we need to protect pupils and staff but also to protect ourselves from legal challenge. 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 School 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

The school has an E-Safety Leader. The E-Safety Leader is also the Computing Leader, Mrs Townsend. The E-Safety Leader works closely with the Designated Safeguarding Leaders (DSLs).

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.

The E-Safety Policy will be reviewed every two years.

The E-Safety Policy has been written in conjunction with our: Child Protection and Safeguarding Policy, Positive Behaviour Policy and Acceptable Use of IT policy.

4 Why is Internet Use Important?

Internet use is part of the statutory curriculum and a necessary tool for learning.

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.

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.

Internet access is an entitlement for students who show a responsible and mature approach to its use.

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, both now and in the future.

5 How Does the Internet Enhance Learning?

Benefits of using the Internet in education include: -

- Access to world-wide educational resources including museums and art Galleries, organisations and online events;
- 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.

The school Internet access will be designed 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 boundaries and expectations 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 to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.

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

If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported, by the staff member, to the school E-Safety Leader, IT technician and, if necessary, the DSL.

Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

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.

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. They will also learn about plagiarism.

Pupils will be provided with access to appropriate websites to use. These will be carefully chosen by the teacher to match learning outcomes. Pupils in lower year groups will not be required to conduct their own internet searches.

7 Managing Internet Access

The security of the school information systems will be reviewed regularly. Virus protection will be installed and updated regularly throughout the year.

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

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

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

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

8 Email

Pupils may only use approved e-mail accounts on the school system.
Pupils must immediately tell a teacher if they receive an offensive e-mail or an e-mail that contains any other information which concerns them.
Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

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

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

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 would be.

The forwarding of chain letters is not permitted.

9 Published Content and the School Website

The contact details on the Website should be the school address, admin e-mail and telephone number. Staff or pupils' personal information will not be published.

Email addresses should be published carefully, to avoid spam harvesting.

The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

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

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, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

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

11 Social Networking and Personal Publishing

Social networking sites and newsgroups will be blocked unless a specific use is required and has been approved prior to use.

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.

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.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers must not run social network spaces for pupils on a personal/individual basis.

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.

Pupils should be advised not to publish specific and detailed private thoughts.

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 comments.

Pupils should be made aware of the age restrictions associated with social networking sites and apps.

12 Managing Filtering

The school will work in partnership with the Coventry LA and LinkIT to ensure filtering systems are as effective as possible.

If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety Leader, IT technician the DSL.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.

13 Managing Video-Conferencing (Microsoft Teams)

All video-conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

Secure software, such as Microsoft TEAMs will be used for video-conferencing and a secure, password protected connection should be used.

External IP addresses should not be made available to other sites.

Video-conferencing contact information should not be put on the school website.

Pupils should ask permission from the supervising teacher before making or answering a video-conference call.
Video-conferencing should be supervised at all times.
Parents and Guardians should agree for their children to take part in videoconferences, probably in the annual return.
Unique log on and password details for video-conferencing services should only be issued to members of staff and kept secure.

When recording a video-conference session, 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.

Recorded material shall be stored securely.

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

Video-conferencing is a challenging activity with a wide range of learning benefits.

Preparation and evaluation are essential to the whole activity.

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.

Use of video-conferencing for home/school learning activities is sometimes a necessary tool to deliver learning to pupils and further detail is provided in the school's remote learning policy.

14 Managing Emerging Technologies

Emerging technologies will be examined for educational benefit prior to classroom use and potential risks will be assessed before use in school is allowed.

Although many new technologies are available on mobile phones and other hand-held devices, personal mobile devices will not be used during lessons or formal school time. For older pupils, who have mobile phones and walk to or from school alone, their device must be handed to the office at the beginning of the school day, to keep it secure.

15 Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to GDPR 2018 (see relevant policies).

16 Authorising Internet Access

The school will maintain a current record of all staff and pupils who are granted Internet access.
All users must read and abide by the Acceptable ICT Use Policy before using any school ICT resource.
At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be informed that pupils will be provided with supervised Internet access.

17 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. Although we operate a filtering system and take all due precautions for such incidents, 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 Coventry City Council can accept liability for the material accessed, or any consequences of Internet access.

The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Methods to identify, assess and minimise risks will be reviewed regularly throughout the year.

18 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 who should use the agreed Coventry City Council procedures.
Pupils and parents will be informed of the complaint's procedure.
Parents and pupils will need to work in partnership with staff to resolve issues.

The school's Positive Behaviour Policy would be followed if misuse of IT equipment occurs.

19 Community Use of the Internet

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 and will aim to provide support where necessary.

20 Introducing the E-Safety Policy to Pupils

Rules for Internet access will be posted in all networked areas.
Pupils will be informed that Internet use will be monitored.
E-Safety lessons will be covered to all year groups every half term to raise the awareness and importance of safe and responsible Internet use.
Instruction in responsible and safe use should precede Internet access.
Pupils will also take part in annual E-Safety weeks linked to Safer Internet Day.

21 Staff and the E-Safety Policy

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

Staff have all signed the Staff code of conduct policy and follow guidance in the staff handbook.

22 Enlisting Parents' Support

Parents' attention will be drawn to the School E-Safety Policy in the newsletter and on the school website.
Internet issues will be handled sensitively to inform parents without alarm.
A partnership approach with parents will be encouraged. This could include parents' evenings with demonstrations and suggestions for safe home Internet use.
Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
Interested parents will be referred to organisations listed in section 3 E-Safety Contacts and References.

Policy Reviewed – May 2023

To be reviewed – May 2025

Appendix 1

Web Links

Useful E-safety programmes include:

- Think U Know (CEOP) www.thinkuknow.co.uk
- Childnet www.childnet.com
- Project Evolve https://projectevolve.co.uk/
- UK Safer Internet Centre https://saferinternet.org.uk/
- Google Family Safety Centre https://safety.google/families/

E-Safety Contacts and References:

- 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 https://www.iwf.org.uk/
- NSPCC https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- Childline http://www.childline.org.uk/