



Hazelwood Schools

E-Safety Policy

To be reviewed March 2012

Hazelwood Schools

E-Safety Policy

1. What is E-Safety?

E-Safety reflects the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

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 and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally 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.

Much of the material on the Internet is published for an adult audience and some is unsuitable for children and young people. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is an offence to store images showing child abuse and to use e-mail, text or Instant Messaging (IM) to 'groom' children.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

2. Teaching and learning

2.1 Why is Internet use important?

- 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.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.
- 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.

2.2 How does Internet use benefit education?

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 LBE and DCSF;
- access to learning wherever and whenever convenient.

2.3 How can Internet use enhance learning?

- The school Internet access will be designed expressly 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 objectives 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 in 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.

2.4 How will pupils learn how to evaluate Internet content?

- The school will ensure that the copying and subsequent 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.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

3. Managing Information Systems

3.1 How will information systems security be maintained?

- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed.
- Portable media may not be used by children and non-staff members without specific permission followed by a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly virus-checked.
- The ICT co-ordinator / network manager will review system capacity regularly.

3.2 How will e-mail be managed?

- Pupils may only use approved e-mail accounts.
- 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.
- For external e-mail linked to class work, when contacting other schools and outside agencies, whole-class or group e-mail addresses will be used.
- Where practicable, access in school to external personal e-mail accounts, including webmail accounts, will 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.
- The forwarding of chain letters is not permitted.

3.3 How will published content be managed?

- The contact details on the website will be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- E-mail addresses will be published carefully, to avoid spam harvesting.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

3.4 Can pupil's images or work be published?

- Images that include pupils will be selected carefully and will not be identified by name.
- Pupils' full names will not be used anywhere on the website in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Work can only be published with the permission of the pupil and parents.

3.5 How will social networking and personal publishing be managed?

- Where feasible the school will endeavour to block access to social networking sites.
- Newsgroups will be blocked to children and non-staff members unless a specific use is approved by a member of staff.
- 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 e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will 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 will be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- If applicable, teachers' official blogs or wikis should be password protected and run from the school website. Teachers will be advised not to run social network spaces for student use on a personal basis.
- Pupils will be advised on security and encouraged to set secure passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students will be encouraged to invite known friends only and deny access to others.
- Students will be advised not to publish specific and detailed private thoughts.

3.6 How will filtering be managed?

- If staff or pupils discover unsuitable sites, the URL must be reported to the appropriate member of staff in the school.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be reported to appropriate agencies such as Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP) (addresses later).

3.7 How will videoconferencing be managed?

The equipment and network

- IP videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment will be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.
- Parents and guardians should agree for their children to take part in videoconferences.
- Responsibility for the use of the videoconferencing equipment outside school time needs to be established with care.
- Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference 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 third party intellectual property rights.
- Videoconferencing 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 videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

3.8 How can emerging technologies be 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 will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils is required.

3.9 How should personal data be protected?

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

4. Policy Decisions

4.1 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 must read and sign the appropriate Code of Conduct before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the Internet will be with adult-supervised access to specific, approved on-line materials
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access

4.2 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 Enfield 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.
- 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.

4.3 How will E-Safety complaints be handled?

- 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.
- Any complaint about misuse by a headteacher must be referred to the Chair of the board of governors.
- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the local Police to establish procedures for handling potentially illegal issues.
- Sanctions within the school discipline policy include:
 - interview/counselling by the headteacher;
 - informing parents or carers;
 - removal of Internet or computer access for a period.

4.4 How is the Internet used across the community?

- The school may 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.

5. Communications Policy

5.1 How will the policy be introduced to pupils?

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- An e-safety training programme will be introduced to

6. Legal Framework

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice.

Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

- ⊙ The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;
- ⊙ The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and
- ⊙ The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of “*Children & Families: Safer from Sexual Crime*” document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.

This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to:

- ⊙ gain access to computer files or software without permission (for example using someone else's password to access files);
- ⊙ gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- ⊙ impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her “work” without permission.

The material to which copyright may attach (known in the business as “work”) must be the author’s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.

It is an infringement of copyright to copy all or a substantial part of anyone’s work without obtaining the author’s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else’s material.

It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

7. Notes

Using the Internet to support learning

Most Internet use in primary schools is safe, purposeful and beneficial to learners. There is always an element of risk: even an innocent search can occasionally turn up links to adult content or violent imagery. Risks are magnified by the upsurge in schools' Internet access. However, many teachers feel that there is a far greater problem in the amount of irrelevant, incomprehensible material typically yielded by Internet searches.

For the youngest pupils, the greatest risk is through inadvertent access. Fast broadband means that inappropriate images can appear almost instantaneously. Children can innocently follow a series of links to undesirable content. A procedure should be agreed with all staff on what to do, and how to handle the situation with pupils. For example:

Close or minimise the image or window immediately. Don't try to navigate away. If pupils saw the page, talk to them about what has happened, and reassure them. Later, investigate the history of visited sites and how the pupil got there.

In view of the risks, we advise that primary pupils are supervised at all times when using the Internet.

Search engines

We urge teachers to think very carefully about allowing primary pupils to use Internet-wide search engines such as Google. If Google is to be used at all, you must make sure that strict filtering is applied. Go to www.google.co.uk and click *Preferences*.

The BBC search engine is a safer approach for children: <http://search.bbc.co.uk/>

Image searches are especially risky. There may be no need for pupils to download them, as long as an adult downloads the images before the lessons and stores them in a shared folder. Alternatively, teachers may use Microsoft's clipart library, which automatically adds downloaded images to Clipart: <http://office.microsoft.com/clipart/>

Tagged image browsers are fun to explore. An example is www.airtightinteractive.com/projects/related_tag_browser/. The danger is that this will accept inappropriate keywords. While useful to teachers, we can no longer recommend it for use by pupils. Links such as this must not be stored in the 'Favourites' folder accessible to pupils.

For most curriculum-related research, there is no need to use an unfenced search engine. **Yahooligans**, although US centric, does offer a range of

selected sites which are relevant to the UK curriculum. For details, see Yahoo!igans UK: <http://uk.docs.yahoo.com/yahooligans/parents.html>

There is excellent advice on safe searching at The Guardian's NetClass: <http://education.guardian.co.uk/netclass> (click on 'I can't find what I want').

http://www.wisekids.org.uk/Kids_safe_search_engines.htm

However, please note that NO filter-based search engine is completely safe.

Curriculum planning

Good planning and preparation is critical in ensuring a safe starting point for the development of Web search skills and strategies. Tasks can be planned that do not require an Internet-wide search engine.

If the aim is to teach search skills, **BBC Schools** offers a safe environment. The search box automatically restricts the search to the BBC Schools site. There is no indication of age range, but pupils can judge readability from the example retrieved by the search www.bbc.co.uk/schools. Importantly, primary pupils can learn skills such as keyword selection to narrow down searches, and evaluating quality and relevance. This will prepare them for efficient, productive Internet research in the secondary phase.

Webquests contain direct links to support research. There is no need to use a search engine. Some webquests simply consist of a list of questions. The questions are linked directly to text sources and offer a motivating means of engaging reluctant readers in 'finding out'.

Others are designed to support collaborative group activity. They encourage pupils to apply what they have found, leading to more effective learning. The webquests at WebQuestUK are linked to National Curriculum topics and QCA schemes of work. They offer a self-contained set of learning tasks with a defined outcome, such as recording a WWII evacuee's diary or writing a Victorian school's handbook. <http://www.webquestuk.org.uk/>

A list of webquests is at: <http://ecs.lewisham.gov.uk/youthspace/quests/>

The Dragonfly Challenges at Naturegrid draw on the natural habitat 'Explorer' themes and are a useful introduction for Key Stage 2:

www.naturegrid.org.uk/e-mail/enquiry.html

Any teacher able to produce a document in Word can create his/her own webquest. To place an active web link on the page, simply select and copy from the address bar in Internet Explorer, and paste into Word. To follow the link, press and hold the Ctrl key while you click on the link.

Primary school learners need not be exposed to the risks of the unfenced Internet!

8. E-Safety Contacts and References

BBC Chat Guide

<http://www.bbc.co.uk/chatguide/>

Becta

<http://www.becta.org.uk/schools/esafety>

Childline

<http://www.childline.org.uk/>

Child Exploitation & Online Protection Centre

<http://www.ceop.gov.uk>

Grid Club and the Cyber Cafe

<http://www.gridclub.com>

Internet Watch Foundation

<http://www.iwf.org.uk/>

Internet Safety Zone

<http://www.internetsafetyzone.com/>

Kidsmart

<http://www.kidsmart.org.uk/>

NCH – The Children's Charity

<http://www.nch.org.uk/information/index.php?i=209>

NSPCC

<http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm>

Stop Text Bully

www.stoptextbully.com

Think U Know website

<http://www.thinkuknow.co.uk/>

Virtual Global Taskforce – Report Abuse

<http://www.virtualglobaltaskforce.com/>

Click Clever Click Safe

<http://clickcleverclicksafe.direct.gov.uk/>

UK Council for Child Internet Safety (UKCCIS)

<http://www.dcsf.gov.uk/ukccis/>

9. Acknowledgements

We acknowledge the extensive, pioneering work undertaken in Kent and in other areas, and by BECTA (British Educational Communications and Technology Agency) as source materials in producing this document. This guidance is based on the results of others' development work.

<http://www.becta.org.uk/>