Becta

becta advice

Signposts to safety
Teaching e-safety at Key Stages 1 and 2

Contents

Introduction

Children and young people have embraced new technologies as a source of information, education and entertainment. A recent report, *Their space: education for a digital generation*,[1] from the think tank Demos found that 'the use of digital technology has been completely normalised by this generation, and it is now fully integrated into their daily lives'.

Children and young people are using technology in new and exciting ways, enhancing and enriching their lives with the many tools on offer. With the advent of Web 2.0 technologies (web-based technologies that emphasize online collaboration and sharing among users), young people are no longer passive recipients of online information, but are increasingly creators of digital content, using social software tools to collaborate within a multimedia landscape. In their exploration of the technologies, young people are not only developing their ICT skills, but also a whole host of 'softer' skills – creativity, communication and networking skills, for example – which will be much in demand by the employers of the future.

Disclaimer

This booklet refers to a selection of websites and resources that may help teachers of Key Stage 1 and Key Stage 2 teach e-safety messages in the classroom. There are other sources available – the number of e-safety websites is growing and their content is developing.

Inclusion of resources within this booklet does not imply endorsement by Becta, nor does exclusion imply the reverse. Becta does not accept any responsibility for, or otherwise endorse, any information contained within the referenced sites, and users should be aware that some linked sites may contain sponsorship information or advertising.

URLs and information given in this booklet were correct at the time of publication, but may be vulnerable to change over time.

Curriculum references apply to the National Curriculum for England only, although it is hoped that the accompanying text will also provide transferable e-safety messages for the other UK countries and beyond.

Some schools, understandably, have found it challenging to keep pace with this technological change, when faced with the inherent safety, security and knowledge issues. The authors of the Demos report state:

> 'Rather than harnessing the technologies that are already fully integrated into young peoples' daily lives, schools primarily have a "battening down the hatches" approach. Responding to concerns about the safety of social networking sites, most schools block MySpace, YouTube and Bebo. Mobiles, iPods and other pieces of equipment are similarly unwelcome in the classroom. Meanwhile, teachers often do not feel confident using hardware or software – many know less than their students.'

Undoubtedly new technologies bring new risks, but the Demos authors found that 'contrary to society's assumptions about safety, this generation is also capable of self-regulation when kept well-informed about levels of risk'. Schools have a duty to help children and young people remain safe when online, whether that use of the internet occurs inside or outside school. Also, as the Demos report states, 'schools need to respond to the way young people are learning outside the classroom' and 'develop strategies to bridge formal and informal learning, home and school'.

Schools will increasingly have more flexibility in the way they deliver the curriculum, embracing these new technologies and recognising that the educational and social opportunities far outweigh the dangers.

Schools can equally become more creative in the way they deliver e-safety messages throughout a child's school life. This booklet aims to help schools in that process. It does not prescribe how schools should deal with the various technologies, but instead aims to assist schools in helping children and young people to acknowledge the opportunities and risks, and develop a set of safe and responsible behaviours to support them whenever they are online. We hope you find it useful.

[1] Green, H and Hannon, C (2007), *Their space: education for a digital generation*, Demos
[http://www.demos.co.uk/files/Their space - web.pdf]

1 The role of ICT in the lives of children today

Children are exposed to ICT at an ever-younger age. Preschool television programmes often have accompanying websites, games consoles offer internet and Wi-Fi connections enabling interaction with other players, and the age of mobile phone ownership is falling, with a number of handsets appearing on the market aimed specifically at the under-10s.

Home access to computers and the internet is also growing. Research conducted by the Office of Communications (Ofcom)[2] found that by the first quarter of 2006, internet connections had reached 60 per cent of households in the UK, and 67 per cent of households had a personal computer. Growth in broadband connections has similarly risen, with seven in 10 internet-connected homes (41 per cent of all UK homes) using a broadband connection in the first quarter of 2006.

The same report found that young people (aged 16–24) are typically moving away from old, traditional media, favouring digital television and radio over analogue and local commercial services. These young people also favour mobile voice and text calls over fixed-line telephony, spend more time online, and expect 'on demand' delivery of services. These trends are probably reflected in the younger population.

Technology has not just permeated the social aspects of life, but is evident in the classroom too. ICT is embedded in reception classrooms and is a constant and prevalent feature of school life.

Children and young people are increasingly referred to as 'digital natives'[3]: citizens born into a digital world, who grow up surrounded by and emerged in the technology and tools of the digital age. Their confidence in using the technologies is typically high, but their knowledge and awareness of the inherent issues, risks and dangers may be low. It makes sense, therefore, that children should be taught responsible use of these technologies as soon as they start to use them, and certainly when they start school.

Education about how to use the technologies safely should be appropriate to the children's age and level of skill and understanding, and should not detract from the fun and educational aspects of ICT. By instilling within children a set of core principles to support them in their use of technology, they will be better able to become safe and discriminating users of new technologies as they grow older and their experiences and exposure to technology widens.

This booklet gives an overview of the technologies that children and young people may encounter, and describes some of the associated risks and issues. It identifies appropriate curriculum links for teaching e-safety at Key Stage 1 and Key Stage 2, along with some useful resources.

---

[2] Ofcom (2006), *The communications market 2006*
[**http://www.ofcom.org.uk/research/cm/cm06/cmr06_print/main.pdf**].

[3] Prensky, M (2001), 'Digital natives, digital immigrants' in *On the horizon* 9(5), October, NCM University Press
[**http://www.marcprensky.com/writing/Prensky - Digital Natives, Digital Immigrants - Part1.pdf**].

2   Evidence of ICT use among children

The UK Children Go Online (UKCGO)[4] study offered a rigorous and timely investigation of 9 to 19-year-olds' use of the internet between 2003 and 2005. The project assessed online risks and opportunities in order to contribute to academic debates and developing frameworks for children's and young people's internet use. Factors such as access to the internet, the nature of internet use, inequalities and the digital divide, education and literacy, and communications and participation were considered.

The study found the following:

- Home access to the internet is growing (75 per cent), and school access is nearly universal (92 per cent). Two-thirds of children and young people (64 per cent) have accessed the internet outside school or home – for example, in someone else's house or a public library.
- Access platforms are diversifying (71 per cent of children and young people have internet access via a computer, 38 per cent via a mobile phone, 17 per cent via a digital television and eight per cent via a games console).
- Most children and young people use the internet daily (41 per cent) or weekly (43 per cent), with many children using the internet for searching and homework (90 per cent).
- Contrary to public perception, there is little reported interest in contacting strangers online, and most online communication is with existing friends. Generally, mobile phones are used in preference to email or instant messaging.

However, the study also found that:

- Children lack key skills in evaluating online content (38 per cent of pupils aged between 9 and 19 trust most of the information online, and only 33 per

cent of daily and weekly users have been taught how to judge the reliability of online information).
- Many children (30 per cent) have not received lessons on using the internet.
- Children divulge personal information online (46 per cent).
- More than half (57 per cent) of daily and weekly internet users have come into contact with online pornography.
- One-third of daily and weekly internet users have received unwanted sexual comments (31 per cent) or nasty comments (33 per cent) online or by text message.

The authors of the study conclude that:

'...the risks do not warrant a moral panic, and nor do they warrant seriously restricting children's internet use because this would deny them the many benefits of the internet. Indeed, there are real costs to lacking internet access or sufficient skills to use it.

However, the risks are nonetheless widespread, they are experienced by many children as worrying or problematic, and they do warrant serious intervention by government, educators, industry and parents.'

Looking specifically at mobile technologies, the *Mobile life youth report 2006*[5] surveyed 1,256 young people (aged 11–17) in the UK to consider the impact of the mobile phone on daily life, family, relationships and school. Although not surveying primary-age pupils as such, the report found that more than half of 10-year-olds own a mobile phone (51 per cent), and by the age of 12, 91 per cent own a mobile phone.

This research demonstrates that technology is now a huge part of young people's lives – it provides them with a source of communication, education and entertainment at an ever-younger age. Now, more than ever, children need to know how to stay safe when using technology, and schools have a role to play in providing e-safety education and supporting parents in providing a safe home environment.

[4] Livingstone, S and Bober, M (2005), *UK children go online*, The London School of Economics and Political Science [**http://personal.lse.ac.uk/bober/UKCGOfinalReport.pdf**].

[5] The Carphone Warehouse and The London School of Economics and Political Science (2006), *The mobile life youth report 2006: the impact of the mobile phone on the lives of young people* [**http://www.yougov.com/archives/pdf/CPW060101004_2.pdf**].

3 E-safety and whole-school issues

As seen from the evidence, children are using technology at an ever-younger age, and so their e-safety education should start as soon as technologies are introduced.

Teachers are bound by a wider duty of care to raise awareness of e-safety issues among children and young people. However, the development of effective e-safety strategies should involve all stakeholders in a child's education, from the headteacher and governors to the senior management team, classroom teachers, support staff, pupils and parents.

Headteachers, with the support of governors, should take a lead in embedding safe internet practices into the culture of the primary school, perhaps designating a member of the senior management team with responsibility for e-safety. This member of staff should act as the central point of contact for all safety issues within the school, ensuring that policies are current and adhered to, any breaches or abuse are monitored and reported to the headteacher and governors, and that all staff receive relevant information about emerging issues. Someone other than the ICT co-ordinator or network manager can take responsibility for e-safety, but all three roles should work closely to ensure that technological solutions to e-safety support classroom practice.

It is recommended that, as a minimum, schools have an acceptable use policy in place to protect the interests of both pupils and staff, and that this is at the heart of practice. This should be linked to other school policies, as appropriate, such as child protection and anti-bullying policies, and guidance on copyright and plagiarism.

E-safety policies should be regularly monitored and reviewed, and all staff should be aware of the appropriate strategies to adopt if they encounter problems. Additionally, all teachers who use ICT in the classroom have a duty to ensure that pupils are reminded about appropriate behaviour on a regular basis. This approach is discussed in further detail in the Becta publication *E-safety: developing whole-school policies to support effective practice*[6].

Section 11 of this publication provides further information on opportunities for collaboration and sharing good practice, including training resources for school staff.

Parents and carers have a key role to play in promoting e-safety at home. ICT offers the opportunity for children and parents to learn together, and e-safety is

an excellent topic which can encourage home–school links – this is discussed further in section 10.

Becta recently commissioned the Department of Education and Social Science at the University of Central Lancashire (UCLAN) to conduct an audit to establish the state of e-safety practices in English schools. The findings[7] include the following:

- Breaches of e-safety are most likely to occur among older pupils in both primary and secondary schools. The most common breach is the viewing of unsuitable online material. However, the research found that when pupils were taught about e-safety, all breaches of e-safety were reduced.

- Breaches are also more likely to occur when pupils are allowed to bring their own equipment (such as laptops or portable storage devices) onto school premises. In some cases, such as incidents of bullying via mobile phone, breaches are not only more likely to occur, but also occur with greater frequency when such items (in this case mobile phones) are allowed on the premises.

- Teachers' ability to deal with breaches of e-safety varies according to the training and support they receive, the policies and procedures in place in schools, and the effectiveness of technical systems.

- Having a designated internet safety co-ordinator and an acceptable use policy better equips teachers to deal with breaches of e-safety.

[6] Becta (2005), *E-safety: developing whole-school policies to support effective practice* [**http://schools.becta.org.uk/index.php?section= pb&catcode=ss_pb_es_02&rid=13069**].

[7] Barrow, C and Heywood-Everett, G (2005), *E-safety: the experience in English educational establishments*, Becta ICT Research [**http://partners.becta.org.uk/index.php? section=rh&rid=11302**].

5

On the basis of these findings, recommendations include that educational establishments take a strategic and integrated approach towards e-safety, with monitoring facilitated by local authorities.

Educational establishments need to consider alternative ways of managing the use of personal equipment brought onto their premises by pupils, and also to consider issues relating to mobile technologies in e-safety teaching and learning.

Targeted directives are required to counter breaches of e-safety within particular pupil groups, while teachers require support that is both tailored to their existing levels of expertise and which also takes account of the increased capabilities and wider uses of new technologies.

Although e-safety is not explicitly referred to within the National Curriculum at present, there are a number of areas within the programmes of study that offer opportunities to discuss e-safety issues, and these are highlighted within this booklet.

Ofsted's school self-evaluation framework (SEF) has recently been updated to incorporate e-safety. Section 4b – To what extent do learners feel safe and adopt safe practices? – now includes this clause:

> 'the extent to which learners adopt safe and responsible practices in using new technologies, including the internet.'

Additionally, Becta's self-review framework offers schools a straightforward route for improving their effective use of ICT including e-safety issues. The framework also offers benchmarking against established best practice and helps schools ensure that their ICT infrastructure meets their needs. Further information can be found on the home page of the Becta Schools website [**http://www.becta.org.uk/schools**].

4 Learning benefits of ICT

There is a growing body of evidence indicating that ICT use can have a positive impact on learners' attainment and other outcomes.

The *Becta review 2005*[8] reported on large-scale studies, such as ImpaCT2[9] and Becta's statistical analysis of national data (SAND),[10,11] which found that ICT had a positive impact on standards on a national scale in certain schools and certain subjects.

The *Becta review 2006*[12] reports on further large-scale studies, including the ICT Test Bed evaluation,[13] which presents attainment data from the second year of the study, based on benchmarking against comparable local authorities. The study found that between 2002 and 2004, in the ICT Test Bed local authorities, the rate of improvement in key stage test scores was higher than the national average in key areas.

A study by the DfES in 2003 investigated the effects of ICT on pupils' motivation. The study – *The motivational effect of ICT on pupils*[14] – examined the impact of ICT on pupils' motivation, alongside related issues, such as learning outcomes, behaviour and school attendance. The study found that ICT had a positive motivational impact overall, although this was dependent on the ways in which ICT was used. ICT typically had a positive impact on the learning processes of engagement, research, writing and editing, and presentation.

A number of pupils in the study reported that ICT positively affected their behaviour outside school. For example, use of the internet and email encouraged more positive activities, longer engagement with school work, deeper and wider discussion with a broader group of friends, and sharing of emotions through chatting. Some secondary school pupils also thought that ICT had a positive impact on their attendance at school or the attendance of others.

A more recent DfES study[15] looked at the impact on attainment of home use of ICT for educational purposes, and found that:

'Pupils, parents and teachers reported that using ICT raised pupils' confidence and had motivational effects. ICT was motivational because it contributed both to making school work more enjoyable and also to pupils' perceptions of achievement. Specifically, ICT was regarded as making homework less boring because children regarded using computers as: "cool"; interactive and multimodal texts were more interesting than books; ICT saved time (e.g. it is easier to write and

[8] Becta (2005), *The Becta review 2005: evidence on the progress of ICT in education*, Becta ICT Research [**http://schools.becta.org.uk/index.php?section=pb&&catcode=ss_pb_lv_02&rid=13043**].

[9] Becta (2002), *ImpaCT2: the impact of information and communication technologies on pupil learning and attainment*, Becta ICT Research [**http://partners.becta.org.uk/page_documents/research/ImpaCT2_strand1_report.pdf**].

[10] Becta (2003), *Primary schools – ICT and standards. An analysis of national data from Ofsted and QCA by Becta* [**http://www.becta.org.uk/page_documents/research/Introduction.pdf**].

[11] Becta (2003), *Secondary schools – ICT and standards. An analysis of national data from Ofsted and QCA by Becta* [**http://www.becta.org.uk/page_documents/research/secschoolfull.pdf**].

[12] Becta (2006), *The Becta review 2006: evidence on the progress of ICT in education*, Becta ICT Research [**http://schools.becta.org.uk/index.php?section=pb&catcode=ss_pb_lv_02&rid=13078**].

[13] Somekh, B, Underwood, J, Convery, A et al (2006), *Evaluation of the ICT Test Bed project: annual report March 2006*, Becta [**http://www.evaluation.icttestbed.org.uk/reports**].

[14] Passey, D, Rogers, C, Machell, J and McHugh, G (2004), *The motivational effect of ICT on pupils*, DfES Research Series Ref No RR 523, DfES [**http://www.dfes.gov.uk/research/data/uploadfiles/RR523new.pdf**].

[15] Valentine, G, Marsh, J and Pattie, C (2005), *Children and young people's home use of ICT for educational purposes: the impact on attainment at Key Stages 1–4*, Research Report 672, DfES [**http://www.dfes.gov.uk/research/data/uploadfiles/RR672.pdf**].

revise documents on a computer than by hand) and enhanced the presentation of children's work; the internet was a good source of information (range and depth) and educational materials (such as revision websites); ICT enabled multi-tasking and was perceived by children to improve grades (just under 50 per cent of children thought that using a computer improved their marks). The subjects in which pupils (in years 6, 9 and 11) used computers at home for school work at least once a week were also the same subjects in which they believed that using a computer improved their grades and in which they had most home-based electronic resources.'

The use of ICT offers particular benefits for those pupils with special educational needs, providing a motivating learning medium. Many learners are attracted to computers and want to learn through them. Software applications incorporating colour, pictures, animations, sound and humour can build on that interest, creating attractive learning opportunities to engage pupils. Information can be presented in different ways, giving pupils more opportunities to connect in ways that suit individual learning styles and strengths.

There are also a range of assistive technology tools which can be used with ICT: hardware and software can enable many learners to overcome barriers, supporting physical, sensory and learning difficulties.

Access to ICT can also be beneficial to those pupils who are unable to attend school on a regular basis. It can allow them to still feel part of the school environment and retain some continuity in their work.

Case study

The Demos report *Their space: education for a digital generation*, by Hannah Green and Celia Hannon presents a case study of technology use at Stiperstones CE Primary School in Shropshire:

'Perhaps most excitingly the school exploits the participatory potential of technology, with whole class "silent" debates conducted MSN style. They cover a wide range of issues ranging from what questions they'd most like to ask their new headteacher (Mark [Klekot] is moving on next term) to PSHE issues and what rule they should all abide by if they're going to take the laptops home. These conversations were mediated by Mark and played out at the front of the classroom on the interactive whiteboard. "It makes me want to type faster," one boy said as he mimed typing slowly with his index fingers. "At the moment I can usually only manage to say one thing!" Others agreed and were also quick to point out that everyone always contributes. "It's not as scary as speaking in front of the whole class, and it's easier because not everyone is shouting out." And it's anonymous; only their ID number comes up, not their name so they are liberated to say whatever they're thinking.

It's not only the innovative use of technology that makes Stiperstones such an interesting and successful school, but the ethos of the school across subjects and classes. Teachers feel confident enough to encourage children to experiment and they work in line with the interests of the students as far as possible. Yet there is a strong sense that this approach can be taken too far: to foster spontaneity and creativity you need to remember that "innovation dies in a measurable and accountable model". Mark is clear that some tools are not suitable for school; part of the reason children enjoy them is because they are not part of a formal system. Above all, technology is successful here because it has the support of an enthusiastic leader and has been adopted across the whole school in a way which reflects children's lives.

Stiperstones is just one of a growing number of schools that have seen the potential of digital technology and that work to align themselves with the way that children approach informal learning without seeking to replicate it wholesale.'

This extract is reproduced with the authors' permission. The full report can be viewed online via the Demos website [**http://www.demos.co.uk/ files/Their space - web.pdf**].

5 Risks associated with using ICT

Alongside the positive educational and social benefits offered by ICT there are, unfortunately, some dangers, particularly for children. As in any other area of life, children are vulnerable and may expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies.

While adult supervision of children's ICT use is preferable, it is not always realistic or practical, particularly outside school. Therefore it is necessary to alert children to the risks they might encounter and help them to develop safe and responsible behaviours when using technologies, whether at school, at home or in any other setting.

For primary school children, certainly in the lower year groups, some of the risks might appear to be outside their level of ICT use. However, as the research shows, children engage with technology at an ever-younger age, and their knowledge and use of technological services, tools and devices can quickly outstrip that of their parents, carers and teachers.

When considering the issues associated with ICT use (and the technologies described in the following section), schools need to be sensitive to the age and awareness of the children within their care: although the core e-safety messages should remain the same, the methods of delivery of e-safety education will differ.

The issues which schools should be raising awareness of can be broadly categorised into three areas:

- Content
- Contact
- Commerce.

A fourth area, culture, cuts across these three areas. Each of these risks is discussed further below.

Content

There is a risk that when using the internet or other online service and technologies, children may be exposed to inappropriate content. This may be material that is pornographic, hateful or violent, encourages activities that are dangerous or illegal, or is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexist views also have a free voice.

Schools provide a degree of protection against this sort of exposure, but even the filtering software installed is not always foolproof. Supervision within the classroom can help, but the same level of supervision does not often extend to the other settings where children may use ICT. It is natural for children to believe what they read, and often online content appears to have as much authority as the printed word, even when it has less authority. It is important, therefore, that schools provide digital literacy education, teaching children to become critical and discriminating users of materials they find online and of information provided through 'direct contact' services, such as email, chat and social software.

Children should also be aware of the security risks of accessing certain types of content. These risks include viruses, adware and spyware. Children should be taught to always question the source and reliability of any content they access or download and be aware of the various technological approaches to minimising the risks.

Contact

E-safety risks associated with contact are perhaps the ones which receive most press attention because of the fear of physical danger.

A criminal minority makes use of the internet and related services, such as chat rooms, gaming and social software, to make contact with children and young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. Paedophiles often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop over months or years as the paedophile gains the trust and confidence of the young person, perhaps progressing to other forms of contact, such as text messaging, as a prelude to meeting in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'. The Sexual Offences Act 2003 includes a grooming offence specifically introduced to combat this abuse of the internet.

There is also a risk that while online, children might provide information that can identify them or others, or arrange to meet people they have met online, thus posing a risk to their safety or that of their family or friends.

New technologies provide an apparently anonymous method by which bullies can torment their victims at any time of day or night. This is known as cyberbullying. While children may not be in physical danger, they may receive email, chat or text messages, or be the target of unfavourable websites or social networking profiles that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

Commerce

When using new technologies, there is a risk that a child could do something that has financial or commercial consequences.

E-commerce continues to grow, and there is a risk that children may give out financial details, for example the credit card details of a parent, while online. This can result in unexpected consequences and charges. Additionally, studies[16] found that children were able to register with online gambling websites using debit cards issued on youth accounts, which are typically available to children as young as 11.

Junk email or spam may provide offers that sound too good to be missed, while phishing and similar scams may trick children (and their parents) into revealing personal or financial information which could be used for identity theft.

Premium-rate services on mobile phones offer ring tones, logos and competitions.

Additionally, research shows that children are not able to differentiate between what is advertising and what is not.

Culture

Cultural e-safety risks cut across the other three areas. Children need frequent education and guidance to embed and reinforce e-safety messages.

There is a risk that children may get involved in inappropriate or antisocial behaviour while using new technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious. Children should be taught to avoid being rude, mean or inconsiderate online. They should be taught that they should behave in the same way online as they would offline.

A growing area of concern is appropriate behaviour in the Web 2.0 environment; that is, with the second generation of internet-based services, such as social networking sites and blogs. These services allow people to publish, collaborate and share information in new ways. Although several social networking sites place age restrictions on new members (users typically need to be 13 or 14 to register), many offer no age-verification mechanisms, meaning that children can simply lie about their age to create a profile, while several sites impose no age restrictions at all. However, some social networking sites are emerging that are aimed specifically at children, and these tend to have a strong e-safety focus.

In the Web 2.0 environment, children and young people are no longer just recipients of content downloaded from the net, but are active participants

---

[16] BBC News: 'Schoolgirl tests online gambling' [**http://news.bbc.co.uk/1/hi/uk/3928261.stm**].

in the online world, uploading content to a worldwide audience. In many cases, young social networkers publish detailed accounts of their personal lives and daily routines, contact information, photographs and videos, oblivious to the possible implications of the content they post (which is sometimes sexually provocative) and the permanence of their profiles. Unfortunately, these sites can also prompt bullying, slander and the humiliation of others.

Many of these issues are compounded by the growing use of increasingly sophisticated mobile phones by an 'always connected' generation of young people. Integrated cameras and mobile internet connections mean that images can be shared in seconds.

Plagiarism and copyright are also key cultural issues, particularly in relation to copying schoolwork and downloading music or games, as popularised by many file-sharing services. Children must understand that these activities can have serious moral, legal and financial consequences – the youngest file-sharer to be sued to date (in the USA) was just 12 years old.[17]

There is also a risk that children may become obsessed with new technology, neglecting offline relationships and family contact as a result of spending too much time online.

Children need to learn how to become critical and discriminating users of online services. They must learn to assess online materials and relationships formed through 'direct contact' services. By developing their own judgements of what feels right and what feels wrong, children will be better placed to remain safe wherever and whenever they use new technologies. It is essential, therefore, that digital literacy education should cover these cultural issues.

Bridging the gap between home and school

Schools are relatively protected areas where pupils can access a range of technologies under human and technological supervision and monitoring. In the home, however, there is likely to be minimal technological monitoring, and supervision by parents may not be to the same degree as that in the school environment.

Schools operate policies which allow pupils access to certain types of ICT (for example, access to email via the school network or group email addresses), give clear guidelines on how the technology may be used

(for example, pupils may be able to access educational chat rooms, but only within the classroom context), and impose sanctions for misuse. However, pupils can go home and access a whole range of services, such as webmail, chat rooms, instant messaging services and social software. Additionally, they may have access to a mobile phone offering text and picture messaging and, increasingly, new forms of mobile content and services. Therefore it is important that even if schools do not allow the use of a certain technology within the school, they teach pupils how to behave sensibly and appropriately when using it, and educate them about the risks.

Schools also have a role in sharing information and details of good practice with parents. This can help to reinforce the work carried out in school and ensure that children receive consistent and comprehensive e-safety advice (see section 10 for further information).

E-safety and pupils with special educational needs

A pupil who has a learning difficulty or disability may be even more vulnerable to deceptive messages offering friendship or to opening dialogue on topics of mutual interest. For example, many pupils with autistic spectrum disorder take messages very literally and could be persuaded to act upon them. These pupils are likely to need additional advice on safe behaviours and what they should never disclose to others online; they may also need increased supervision. This could include, for example, guidance that before entering dialogue with anyone new, they should always consult a trusted adult.

Although this booklet does not highlight e-safety resources specifically for pupils with special educational needs, many of the resources mentioned may be suitable and/or adaptable for this purpose.

Additionally, the Thinkuknow Cybercafé, developed by CEOP, together with Becta and the Internet Proficiency Group, may be a useful resource. Aimed primarily at Key Stage 2 pupils, the scheme aims to develop a set of safe and discriminating behaviours for pupils to adopt when using the internet and other technologies.

---

[17] Kidsmart: File sharing [**http://www.kidsmart.org.uk/yp/ under11/filesharing.aspx**].
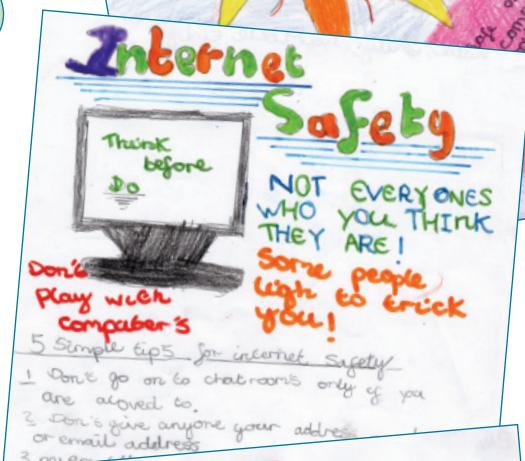
The scheme consists of an interactive website and a range of teaching resources and activities for pupils. Many of the lesson ideas can be adapted to suit the learning styles and previous experience of the pupils involved. The Internet Proficiency Scheme can be downloaded as PDF documents from the GridClub website [**http://www.gridclub.com/teachers/ t_internet_safety.html**].

E-safety in practice

Children at Semley CE VA Primary School in Wiltshire recently took part in a Safer Internet Day* competition to create safety awareness material on the power of image. The children discussed traditional and digital images, and then worked with a school in the USA to create posters and leaflets.

The children learned a lot about working collaboratively using the internet as a means of communication, as well as about some of the risks associated with these technologies.

* Safer Internet Day, typically held in February each year, is an annual international celebration of making the internet a safer place [**http://www.saferinternet.org**].

6 Using the technologies safely

This section looks at the various technologies, giving background information, an overview of the benefits and risks, and ways of avoiding the dangers. Key issues such as cyberbullying and digital literacy are also covered. This section includes teaching pointers and signposts to resources for teachers, pupils and parents. More e-safety resources are described in section 7.

Section 9 complements this section, suggesting in more depth areas in which safety messages can be incorporated within the curriculum, making reference to the National Curriculum programmes of study at Key Stages 1 and 2.

In the news...

With a few quick clicks of a mouse, a boy of three 'bought' a £9,000 car on the internet after his parents inadvertently left their computer logged in to an online auction site.

For further information, see the BBC News story 'Boy, three, buys car on internet' [**http://news.bbc.co.uk/1/hi/england/lincolnshire/5379930.stm**].

Using the internet

Background

The internet enables users to obtain information and resources, to communicate with each other and to publish information. It effectively consists of a worldwide system of computer networks, in which users at any one computer can, if they have permission, access information made available on other computers.

The amount of information available on the internet is vast and can often be quite daunting, particularly if you are looking for specific information. Search engines can help you to refine your search, and make it much easier to find what is required.

Benefits

The internet enables access to a vast range of cultural, educational and intellectual material, which might not otherwise be freely or readily available, and provides a powerful resource for learning. It extends the access to resources far beyond the school – to museums, galleries and organisations of every kind. Resources may be displayed interactively so that pupils can experiment and see how things work. The internet can also prove an excellent source of information for children, particularly regarding sensitive issues that they would not want to discuss face to face.

The internet also provides efficient means of communicating, including video conferencing, and can remove barriers to communication.

Risks

While the web can be a useful educational tool, there are some risks. Some content on the internet, such as pornography, hate material, or information that encourages illegal activities, is clearly unsuitable for children. While it may be easy to judge the suitability of some web pages, other pages may look appropriate on the surface, but the actual content may be unreliable or unsuitable. Some commercial sites may be inappropriate for children.

There is also the question of the reliability, credibility and validity of information on some websites. In a school setting, teachers evaluate the educational value of a website, and pupils should be taught to critically assess the materials they find.

Strategies for safe use

Specific issues to consider include:

Acceptable use policies

As part of their responsibility for ensuring safe access to the internet, schools should develop an acceptable use policy.

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will use the school's computers only for schoolwork and homework.
- I will delete only my own files.
- I will not look at other people's f
- I will keep my login and passwor
- I will not bring files into scho
- I will ask permission from a internet and will not visit in school.
- I will send email only to p
- The messages I send ar polite and sensible.
- I will not open an att permission or I know
- I will not give my video, or give any identify me, my f permission.
- I will never ar on the interne guardian or t adult with m
- If I see ar not like, I responsibl

School logo

Example e-safety agreement form: primary

Keeping safe: stop, think, before you click!

Pupil's name: _____

I have read the school rules for responsible ICT use. My teacher has explained them to me.

I understand that these rules exist to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, internet, email, online communities, digital cameras, video recorders and other ICT in a safe and responsible way. I understand that the school can check my computer files and the internet sites I visit, and that if they have concerns about my safety, they may contact my parents or guardians.

Pupil's signature _____

Date: ___/___/___

An acceptable use policy provides a framework for safe and responsible use of the internet in school, and may give guidance for pupils and parents using the internet at home. It typically outlines safe and responsible behaviours for pupils, procedures for reporting unsuitable material, and information on protecting the computer network, for example from viruses.

The policy should cover the whole range of technology which might be used, both in and out of school, such as email, chat, instant messaging, camera phones, webcams, blogs and social networking sites.

The tone of the acceptable use policy must be appropriate to the age of the pupils: schools may want to create different versions of the policy for different year groups.

Evaluating web materials

While there is plenty of reliable information on the web, there is also plenty that is incorrect, out of date or seriously biased. The popularity of collaborative authoring tools, such as blogs and wikis, is growing, allowing visitors to add, edit and remove content, sometimes without the need for registration. While such resources can be valuable, contributing to a huge body of knowledge, there is a risk that such content could be incorrect or misleading if it has not been checked or verified.

Equally, not all educational materials are age-appropriate for pupils: they may have been developed for a different audience. The critical evaluation of web resources is therefore necessary to determine the reliability, accuracy and currency of the material. Pupils should be taught the value of this process as part of their core digital literacy skills development.

When evaluating materials, pupils should ask:

- Who has published the content? The URL might give some clues.
- Where does the content originate from? It may come from a different source than the person who published the site. Does it have authority? Is it free from copyright restrictions?
- Does the content seem up to date?
- Is the content easy to read and understand?
- Does it present a one-sided point of view?
- Does the content provide everything I need?
- Are the links useful?

Internet filtering

Most educational internet service providers (ISPs) offer a filtered internet service. This can help prevent access to undesirable content and can filter other services, such as incoming and outgoing email. Additional software can by used in school to supplement this service. Many filtering tools are also available for home users.

The Becta internet services accreditation scheme[18] enables schools and other educational establishments to make an informed choice of ISP. The minimum requirements of the accreditation have been developed in consultation with partners in education and industry to ensure a reliable and sustainable service is provided. During the accreditation process, a technical assessment is made of internet services for factors such as filtering web-based content, email filtering, virus alerting, connectivity and managed support processes.

Remember that although filtering systems are effective tools, they are not completely foolproof, so must be supported by a safe and responsible approach to using the internet at all times.

Internet search tools

The web offers a vast quantity of information in a wide range of formats. However, the extensiveness of the internet can also be a major drawback: a variety of search tools and techniques may be required to locate information quickly and easily.

Search engines provide a way of searching the internet using keywords. While typing a keyword or phrase into a search engine quickly provides a large number of websites containing that word, unfortunately the sheer volume of links will be unworkable and the level of potentially useful links will be low. Pupils should therefore be taught the principles of effective searching as part of their core digital literacy skills development.

Searching the internet successfully requires careful planning and definition of the exact information needs. Most keyword search engines offer advanced searching techniques which allow users to define their searches more precisely. Although search commands may vary from one search engine to another, the concepts remain the same, and so the skills acquired are transferable. Many search engines rank results, placing priority on the first search term, and some may allow searches to be limited to UK sites only.

Common words such as 'of' or 'the' are not normally recognised for the purposes of a search, and it is often possible to exclude words from the results. However there are still occasions when no amount of refining creates a manageable number of results. If this is the case, pupils need to be selective and remember to critically evaluate any information they find.

As an alternative to keyword searching, a directory or menu-based search categorises the information on the web into topic areas, starting with very general topic menus which are gradually refined through choices made by the user until the relevant information is reached. A menu-based search can provide a structured method of searching, but lists only those sites classified by the search engine provider.

Many search engines provide filtering facilities to remove unsuitable sites and advertising from search results, and there are a number of search engines aimed specifically at children and families. Search Engine Watch[19] provides tips and information about searching the web, along with a comprehensive list of search engines specifically for children.

The Home Office[20] has developed some good practice guidelines for search service providers, which also incorporate advice to the public on how to search safely. The document includes an overview of child safety concerns and a safe searching checklist for parents and carers.

Customising web browsers

Most web browsers provide some customisation facilities to allow the settings for security, privacy and content to be adjusted. Refer to the help facility within your browser for further information.

Further information on safe use of the internet is available in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/ schools/esafety**].

---

[18] Becta Schools: Internet services accreditation [**http://www.becta.org.uk/schools/ispsafety**].

[19] Search Engine Watch: Kids search engines [**http://searchenginewatch.com/links/article.php/2156191**].

[20] Home Office Task Force on Child Protection on the Internet (2005), *Good practice guidance for search service providers and advice to the public on how to search safely* [**http://police.homeoffice.gov.uk/ news-and-publications/publication/operational-policing/ search-and-advice-public.pdf?version=1**].

Curriculum context

ICT and, specifically, web-based resources, are increasingly being used across the curriculum. It makes sense therefore that guidance on safe use of the internet should be given to pupils wherever and whenever such use occurs.

Schools are encouraged to look for opportunities for teaching e-safety across the curriculum, rather than as a discrete subject, to cover issues that might not typically be encountered during in-school use of ICT. Although e-safety is not explicitly referred to within the National Curriculum at present, a number of appropriate areas within the programmes of study and non-statutory guidelines offer opportunities to discuss e-safety issues, and these are highlighted within this section.

This booklet focuses on ICT, and PSHE and citizenship. The relevant teaching points from the National Curriculum programmes of study/non-statutory guidelines are highlighted here.

Section 9 of this booklet provides a fuller discussion of how e-safety can be embedded into the curriculum areas below.

| Key Stage 1 | ICT | 1a, 2a, 2b, 3a, 5a, 5c |
| | PSHE and citizenship | 1a-1d, 2b-2d,3a, 3g, 4a, 5a, 5c, 5h |

| Key Stage 2 | ICT | 1a, 1c, 2a, 3b, 5a-5c |
| | PSHE and citizenship | 1c, 2a-2d, 2k, 3a, 3e-3g, 4a, 4c, 4g, 5a, 5g, 5h |

Using email

Background

Email is a great way of sending messages over the internet. Just about anything can be attached to, or included in, an email, such as text, pictures, sound, animation or movies.

Benefits

Email can be an extremely valuable tool in schools, encouraging the development of communication skills and transforming the learning process by opening up possibilities that, conventionally, would not exist.

Teachers have reported that using email helps pupils to take greater care with their spelling (an email with an incorrectly spelt email address will not reach the intended recipient) and to be more precise with their choice of words, since email encourages brevity and clarity.

Email can also be particularly rewarding for pupils with special educational needs. Pupils with physical or cognitive impairments may take a long time to create a message, but the recipient would not know that

they have difficulties. Pupils with hearing impairment may find email an alternative, and accessible, channel for communication.

Risks

Despite the benefits, email is open to abuse, which can take many forms:

Spam, spoofing, phishing and pharming

Spam is unwanted email, often from an unfamiliar source. Spam often contains inappropriate content, such as advertising – possibly under the pretence of offering a prize – or pornography. Spammers gather email addresses from websites or discussion groups, and there are also companies that specialise in creating email distribution lists.

Email-address spoofing is practised to embarrass the owner of the spoofed address, to veil the source of virus-laden emails or, often, to obtain sensitive information from spam recipients, again without revealing the source of the spammer.

Spam and spoofed email addresses are linked to practices called 'phishing' and 'pharming'. Spoofed emails and websites fake the brand and identity of known and trusted banks, credit card companies or online retailers in an attempt to trick people into revealing personal financial data, which is then used fraudulently. Identity theft can have serious financial consequences.

Flaming

'Flaming' is the term used for angry or abusive email sent to one person by another, often in discussion groups or chat rooms.

Bullying and harassment

Email can facilitate bullying between children, and it is possible to be harassed with unwanted and obsessive attention via email.

Bombing

A 'bomb' is a program that is intended to crash a computer program. An email bomb is a huge email message, or a large volume of messages, sent in an attempt to make the recipient's email program crash.

Viruses

A computer virus can cause serious problems, possibly destroying files or allowing hackers to access the hard disk of your computer. Viruses can be sent as email attachments. They may even be sent from spoofed email addresses and appear to come from people you know.

Webmail

Some free webmail accounts have inherent dangers. Some service providers allow email addresses to be shared with third parties, resulting in a higher incidence of spam. However, many webmail services offer effective email-filtering tools, though often these are optional.

Strategies for safe use

When children use email, they risk receiving unsuitable messages. Pupils should therefore be taught the appropriate behaviours to adopt if they receive an inappropriate or offensive email. They should be taught never to reply, but instead to close the message and seek advice from their teacher. This allows the teacher to check the message, talk through

any issues, reassure the pupil it was not their fault and take any other action as appropriate.

Pupils should also be taught how to use email appropriately and develop suitable writing conventions.

Listed below are some specific issues to consider for remaining safe when using email:

Acceptable use policies

In addition to providing guidelines for acceptable use of the internet, a school's acceptable use policy should provide clear guidelines for email use. These might include guidance on appropriate tone and language when sending emails, policies on using webmail accounts, and measures for protecting the school's network against viruses. Schools might want to share these guidelines with parents as a framework for safe email use for children when away from school.

Email addresses

Most schools need to limit the use of pupil's email addresses within school for management reasons, but, in any case, care should be taken to ensure that individual pupils cannot be identified via their email address, particularly beyond the school.

A class or teaching group email address may be more appropriate for younger children. Individual accounts can be created as children gain the appropriate skills and knowledge to understand the security implications. Increasingly schools using virtual learning environments (VLEs) make use of email within the school, and VLEs can also be accessed from outside school. Particular caution must be taken when using email beyond an internal email system.

Webmail

Schools usually prohibit the use of free webmail accounts within school. However, some pupils may use webmail outside school. Teach pupils to check for privacy statements when signing up for webmail accounts and not to consent to their details being shared with third parties, to minimise the amount of spam they receive.

Email bullying

Pupils should be made aware of the characteristics of email bullying, the effects it can have on the recipient, and strategies for dealing with it.

Filtering

In the same way that internet access may be filtered, email messages should also be filtered for inappropriate content and spam. The Becta internet services accreditation scheme, as mentioned in the internet section, includes information on email filtering.

Remember that although email filtering systems are effective tools, they are not completely foolproof, so must always be supported by a safe and responsible approach to using email.

Viruses

Email attachments should always be treated with caution. Some viruses attach themselves to messages without the sender's knowledge: if an email address is spoofed, a message containing a virus may appear to be from someone you know and trust. A virus checker should be used on all outgoing and incoming email, and always before opening or saving any attachment.

Further information on the safe use of the email is available in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/schools/ esafety**].

Curriculum context

Section 9 of this booklet provides a fuller discussion of how safe use of email can be embedded into the curriculum areas below.

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2b, 4e, 5c, 5e

Key Stage 2	ICT	3a, 3b, 4b, 5c
	PSHE and citizenship	2c, 4d, 5e, 5f

Using chat and instant messaging

Background

Chat is a way of communicating with other people in real time over the internet in virtual meeting places called 'chat rooms'. There are many different chat rooms available on the internet. They can be a dedicated part of a website, part of a gaming facility or a service offered by an ISP.

Users normally have to register in a chat room by choosing a username (ID) and password; the username is often a pseudonym or false name.

Normally there is a list of users currently chatting, and users are alerted when someone new enters the room. To contribute to the chat, the user can type a message into the message box, and the message is then shown on screen for all to see and respond to if they want.

Users can also enter a chat room without contributing to the discussion, but still see what others are saying. This is known as 'lurking' – it is an accepted practice, and is a good way of familiarising yourself with how a chat room works.

Many chat rooms also offer a 'whispering' or private chat room facility that enables users to chat privately without others in the chat room seeing the conversation.

Some chat rooms are public and can be joined by anyone, while others are private and can be used only by invited chatters and specific groups.

Instant messaging is a form of online chat which is private between two people. It is not moderated, and cannot be joined by others. When you send an instant message, it goes almost immediately to the person you sent it to and appears on their computer screen. Some services also allow the sending of files or the ability to conduct voice conversations over the internet. Instant messaging is also known as 'IM' or 'IMing'. MSN Messenger, Internet Relay Chat (IRC) and ICQ ('I seek you') are examples of instant messaging programs.

To use instant messaging, you need to install software on your computer, as does anyone you want to exchange instant messages with.

Lists of contacts you want to exchange instant messages with are called 'buddy lists' or 'contact lists'.

Typically, you must invite people to be on your buddy list and agree to be listed on other people's lists.

When you go online, you can see who in your buddy list is also online, and they can see that you are online. You can then exchange instant messages.

It should not be possible for anyone to add you to a buddy list, and hence see when you are online, without your consent.

Benefits

Although mainly regarded as a leisure activity, chat rooms can also provide educational benefits. Pupils are able to chat with their peers anywhere in the world, in real time, sharing experiences, comparing lifestyles or working collaboratively. Online chats are frequently hosted by a notable figure, such as a successful business person or television personality, giving access to a wealth of information and experience that would not be available to pupils otherwise.

Examples of the use of chat in the classroom can be found in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/schools/esafety**].

Instant messaging can, like chat, provide many benefits as an instant and effective method of communicating.

Risks

Chat rooms have an element of anonymity, so children often talk about things they may not have the confidence to say face to face. They can pretend to be someone else: older, smarter and more popular. While this can be a positive aspect for some, others misuse this facility. The use of pseudonyms is accepted and encouraged in chat rooms, and again, while this can protect anonymity, it also means that you can never be sure who you are chatting to.

Chat rooms have unfortunately attracted a criminal element, with paedophiles using the anonymity offered to 'groom' children: that is, to develop relationships online with the aim of persuading children into sexual activity in the real world.

Just like at school, groups can be formed in chat rooms. These groups often use an invented set of acronyms to keep conversations private and exclude others. Unfortunately, this can also lead to bullying.

With instant messaging, others are notified when a user who is signed up to the service goes online. However, if used on a shared computer, the instant messaging service may automatically sign on when another user connects to the internet, so giving a misleading impression of who is online.

There may also be an issue of privacy in the level of detail which is required to register with an instant messaging service. This information could be made available to others.

Strategies for safe use

Many schools limit access to services such as chat and instant messaging, so many of the issues with these services may be associated primarily with use at home. However, it is important that pupils are made aware of the risks and of ways of avoiding them, as part of their core digital literacy skills development.

Acceptable use policies

Schools' acceptable use policies should also provide guidelines for using chat and instant messaging services, both in school and beyond. This information should be shared with parents, particularly as use of these technologies, with the associated risks, is likely to occur out of school.

Keeping personal information private

Anyone who uses a chat room or instant messaging service should be careful about how much personal information they reveal while chatting. This is particularly important for children to remember – they may feel they know the person they are chatting to very well, especially if talking about intimate or sensitive subjects. 'Personal information' extends beyond the obvious details such as name, age and location, to information such as extra-curricular activities, names of friends, or details that may be particular to your location – these details can be pieced together to form a very detailed profile of a person. This could lead to an individual being identified or even contacted.

If registration is necessary to use chat or instant messaging services, pupils should ensure that they give as little personal information as possible, and should look for clear privacy statements stating that the information they provide will not be made publicly available. Pupils should choose not to appear in member directories or similar, where their details will be made available for all to see.

Moderated chat rooms

Some chat rooms are monitored or moderated. This means that there is either a human moderator checking what is being said and ensuring that contributors stay on topic (proactive monitoring) or technology that monitors the conversation and alerts a moderator if it detects any unsuitable chat (reactive monitoring).

Proactive moderation is best in an educational context as the moderator is able to step in and ensure that the conversation remains focused and on topic. The Home Office has produced various good practice guidance[21,22] on the moderation of interactive services.

Additionally, all good chat rooms should have clear policy and privacy statements, an archive of previous conversations and an outline of forthcoming topics.

Outside school, it is likely that children will come across unmoderated chat rooms, so it is essential that they are aware of the safe and responsible behaviours to adopt.

Harassment

Pupils should be taught what to do if they suffer abuse or harassment in a chat room. They should not respond in anger, but should instead save a copy of the conversation by using a 'log the chat' function, by copying and pasting or by using 'print screen' – the FKBKO website[23] gives some tips on how to do this. The chat room moderators or service providers should be contacted, giving as much detail as possible, including usernames, dates and times.

[21] Home Office Task Force on Child Protection on the Internet (2005), *Good practice guidance for the moderation of interactive services for children* [**http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document-final.pdf?view=Standard&pubID=339594**].

[22] Home Office Task Force on Child Protection on the Internet (2002), *Good practice models and guidance for the internet industry on: chat services, instant messaging (IM), web-based services* [**http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf?view=Standard&pubID=187078**].

[23] FKBKO website [**http://www.fkbko.co.uk**].

The service providers can than take appropriate action, such as warning the offending user that such behaviour is unacceptable or banning the person from the service completely.

If harassed when using instant messaging, users should contact the service provider, giving the nickname or ID, dates, times and details of the problem. The service provider will then take appropriate action, which could involve a warning or disconnection from the instant messaging service. It might also be worth re-registering for instant messaging with a new user ID.

Buddy lists

Pupils should add only people they know to their buddy lists and should always use an instant messaging service which prevents others from adding their name to a buddy list without the owner's permission. It may be possible to adjust privacy settings in the software to prevent this.

Automatic login

Many instant messaging programs automatically log registered users on when they access the internet. Children should always check that the person they are exchanging instant messages with is who they think they are, perhaps by using a simple password and response as the first message of an instant messaging session. It may also be possible to adjust privacy settings in the instant messaging software to always ask for a password before signing in a user.

Some software enables users to appear to be offline if they do not want to receive messages.

Viruses

Care should be taken when sending or receiving attachments via instant messaging, and, as with email, attachments should always be checked for viruses.

Further information on the safe use of the chat and instant messaging is available in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/schools/esafety**].

Curriculum context

Section 9 of this booklet contains a fuller discussion of how safe use of chat and instant messaging can be embedded into the curriculum areas below.

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2b, 4e, 5c, 5e

Key Stage 2	ICT	3a, 3b, 4b, 5c
	PSHE and citizenship	2a, 2c, 3f, 4a, 4d, 5e, 5f

Using social software

Background

The emergence of social media tools, or social software, is perhaps one of the biggest online stories of recent years.

Blogs, or weblogs, were one of the first widely available social media tools providing an online diary or journal. These were followed by moblogs (blogs sent from a mobile phone), wikis (modifiable collaborative web pages) and podcasting (subscription-based broadcasting over the web). These tools enhance or gain value from social interactions and behaviour, and provide opportunities for collective intelligence, therefore adding value to data.

The term 'social networking', or 'Web 2.0', is typically used to describe online communities where content, such as text, photos, music and video, is created and shared by users. Additional features allow users to create profiles, post comments, exchange instant messages and develop 'friends' lists. Examples of social networking communities include general sites such as MySpace, Bebo, Xanga and Friendster, and those that focus on particular types of media or interests, such as Pizco and Flickr (photo sharing), and YouTube and Google Video (video sharing).

The popularity of social networking sites is remarkable. Bebo, for example, attracted more than 25 million members in little more than a year of

operation, generating in excess of 3 billion monthly page views worldwide.[24] Recent research by Cox Communications in partnership with the National Center for Missing & Exploited Children (NCMEC) in the USA[25] found that 61 per cent of 13- to 17-year-olds have a personal profile on sites such as MySpace, Friendster or Xanga, and over half have posted pictures of themselves online. The situation in the UK is likely to be similar.

Although several social networking sites place age restrictions on new members (users typically need to be 13 or 14 to register), many offer no age-verification mechanisms, so children can simply lie about their age to create a profile, while several sites impose no age restrictions at all. Additionally, some social networking sites are emerging that are aimed specifically at children, although many of these have a strong e-safety focus.

Benefits

Social media tools provide new opportunities for personal expression, allowing users to create communities, collaborate, experiment, share and learn in a virtual world. Young people have embraced these tools as a source of information and entertainment, often using them to seek approval and critical comment on work they have created.

These tools can also offer excellent educational benefits by supporting VLEs, which deliver flexible and accessible online learning to pupils. SuperClubsPLUS (a subscription-based service [**http://www.superclubsplus.com**]) is one such example, providing an online protected learning community open exclusively to Key Stage 1 and 2 children (aged 6–12) and their teachers. SuperClubsPLUS provides a professionally mediated facility where children can communicate and collaborate safely online with others across the UK and beyond. Validated members can use email, instant messaging and forums and build their own multimedia websites. All communication is monitored and moderated, while an educational programme provides support to children, teachers and parents to help them stay safe online.

Risks

It is important to remember that social networking sites are not just youth environments. These are public spaces for both adults and young people, and published content can be seen by a worldwide audience.

While social networking tools encourage young people to be creative users of the internet, publishing content rather than being passive consumers, the personal element of what is being published needs careful consideration. The concerns are shifting from the content that children are downloading to what they are uploading to the net.

Some young people publish detailed accounts of their personal lives, including contact information, details of their daily routines, photographs and videos, so providing an online shopping catalogue for those who seek to exploit children and young people, either sexually or for identity fraud. Additionally, there have been some cases in which young people have published inappropriate content, such as provocative photos and videos of themselves, apparently oblivious to the visibility and permanence of the content online long after their profiles have been updated or deleted.

As with other technologies, contact issues are a clear risk, with many social networkers developing extended 'friend' networks, which could lead to more direct forms of contact in the future.

Unfortunately, social networking sites can also be the ideal platform for facilitating bullying, slander and humiliation of others.

The better social networking sites now take these issues seriously, ensuring that they have safety guidelines and codes of practice in place, and encouraging users to report abuse.

Strategies for safe use

There is much debate over access to social software within educational environments in the UK. Decisions to allow or disallow access within schools are typically made locally, based on local needs, issues and risks. Many schools use blogging tools, for example, to positive educational effect, teaching children effective communication skills against a backdrop of e-safety, as illustrated by the following case study.

---

[24] Bebo, 17 July 2006, press release: 'Bebo.com announces appointment of chief safety officer' [**http://www.bebo.com/Press.jsp?PressPageId=1533927716**].

[25] NCMEC, 11 May 2006, press release: 'New study reveals 14% of teens have had face-to-face meetings with people they've met on the internet' [**http://www.netsmartz.org/pdf/cox_teensurvey_may2006.pdf**].

It is clear, however, that even if use of social software is blocked within schools, young people will still access it from other settings. A recent study by NCH and Tesco Telecoms, *Get I.T. safe: children, parents and technology survey 2006*,[26] found 'an alarming gap in knowledge between parents and their children when it comes to technology'. The study found that one-third (33 per cent) of young people (aged 11–16), including 20 per cent of 11-year-olds, regularly use blogging tools. However, 67 per cent of parents do not know what a blog is, and only 1 per cent of parents think their children are blogging. This general lack of awareness of blogs by parents suggests that the responsibility for teaching young people how to use these social software tools safely must fall to schools.

Key strategies for safe use include:

Respect age restrictions

Most social networking sites have age restrictions on their membership. When registering on social network sites, users must agree to the terms and conditions – many sites terminate accounts if they believe users are under the required age.

Look for social software tools developed specifically for children by trusted organisations – many of these offer the social experience to children within a safe, moderated environment.

Keep personal information private

Children should be taught to keep their personal information private when using social software and to protect the personal information of others. This not only includes the obvious information, such as name, address, phone numbers and school name, but also less obvious details such as favourite hang-outs or references to friends, after-school clubs or social activities, all of which could be pieced together to form a fairly comprehensive profile identifying the user.

Children should also be encouraged to use the privacy features provided by social software, by password-protecting profiles and permitting access only to people they know in the real world.

Privacy also extends to email addresses: users of social software could create an anonymous email address that could be easily deleted or changed should unwelcome messages or attention be received.

[26] NCH and Tesco Telecoms (2006), *Get I.T safe: children, parents and technology survey 2006* [**http://www.nch.org.uk/ stories/index.php?i=387**].

Case study

Topteachers, an online mailing list for teachers and others involved or interested in promoting the effective use of ICT in the classroom, recently highlighted some of the positive benefits of blogging tools. One contributor writes:

'A while ago, I read some messages on this list about blogging... I just wanted to say a big thank you to the person who emailed in about it as I have begun to use it this term for my Year 5 class... My class are eating it up!! It's so easy to use, secure, easy to monitor... we love it. We have it set so it's only accessible to others in the class at present but already they are using it really imaginatively and interactively.'

The contributor then went on to describe her work in more detail:

'We began by discussing ways of e-communicating and I introduced the idea of a blog. We viewed... examples of school blogs, then we had a lesson sharing ideas of what sorts of themes/strands/topics we would like to see blogs on, that would be interesting, fun and useful.

The children began with a personal welcome page with a bit of background info about themselves. They chose their icon and wrote some text, then navigated to each others and left stickies. We incorporated e-safety into this and have clear rules about what may or may not be posted and why.

Children are now creating and developing themed pages. Some examples include history, animals, school lessons, sports, music, reviews, fundraising, school council, jokes, and Dr Who. Our class pages (which I am responsible for) have a general page, a page about our Xmas production and a homework page and this is developing further. So far, children have included uploaded pictures, votes, brainstorms, message boards, question & answer features and text.

Some are more organised and themed than others and I am using these as examples of good practice to help other children manage their pages.

...It is my intention that after this unit of work, the blogs will become an integral part of our learning across the curriculum even though we will be learning about other things in ICT.'

Topteachers is hosted on the Becta website [**http://lists.becta.org.uk/mailman/listinfo/ topteachers**].

Keep online friends online

Some young people have several hundred online friends. Children should learn to recognise that online friends are not real friends, and that they can never be really sure that they are who they say they are. They should never divulge personal or sensitive information that could allow them to be identified or that could be used against them in the future. They should also be aware that 'friendly advice' from online friends could be used as a means of manipulation.

As with other forms of online contact tool, when using social networking, children should never arrange to meet anyone that they only know online.

Limit time spent online

Children should be encouraged to limit their time spent online, balancing time spent social networking with time spent with offline friends and social interactions in the real world.

Use the safety tips and advice provided

Many of the more responsible social networking sites take safety issues very seriously. Children should be encouraged to look for safety information and advice on the sites they are using, respect the terms and conditions of the site, and make use of facilities to report abuse.

Further information on the safe use of social networking tools is available in the e-safety section of the Becta Schools website [**http://www.becta.org. uk/schools/esafety**].

Curriculum context

Section 9 of this booklet provides a fuller discussion of how safe use of social networking tools can be embedded into the curriculum areas below.

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2b, 4e, 5c, 5e

Key Stage 2	ICT	3a, 3b, 4b, 5c
	PSHE and citizenship	2a, 2c, 3f, 4a, 4d, 5e, 5f

Be responsible publishers

Young people need to learn how to be responsible publishers within the social networking world. They should appreciate the longevity of online content and understand that any content they upload is out of their control the minute it is published: online content can effectively be viewed, copied, shared and manipulated within seconds in front of a worldwide audience.

A good question to ask children is whether they would be happy for their parents or a prospective employer to view their social networking profile. If the answer is no, they should seriously reconsider what they are uploading.

Children should learn to respect the rights of others in the social networking world and not post any information which could compromise the identity or safety of others, and avoid being mean, rude or abusive to others in their online interactions.

Children must also develop an appreciation of the intellectual property rights of others when posting content online, ensuring that any images, video or music they incorporate within their profiles are not protected by copyright.

Case study

The Demos report *Their space: education for a digital generation* by Hannah Green and Celia Hannon presents a case study of technology use at Montenay Primary School in Sheffield:

'All those schools experimenting with different media relied on the enthusiasm of individual teachers who exploited the potential of new technologies. These teachers were supported to develop their ideas and were knowledgeable enough to feel confident working with children who spanned the full range of abilities. Peter Winters at Monteney Primary School in Sheffield, in collaboration with the School of Education at the University of Sheffield, has set up a "dinoblog" for his year 3 pupils and has linked up with a school in the US that has its own blog. The children can carry on their own long distance exchange of images and ideas. Blogging is one in a range of digital tools that empowered teachers are using to stimulate and engage students.

..Peter Winters has also used the blog as a real life context in which to encourage the children to learn about safety issues. Although he originally had misgivings about their ability to safeguard passwords he found he was quickly able to instil a sense of responsibility in his pupils. In this way, schools can become a reliable source of a safety code of conduct for children who may not always be able to develop this on their own.'

These extracts are reproduced here with the permission of the authors. The full report can be viewed online via the Demos website [**http://www.demos.co.uk/files/Their space - web.pdf**].

Using file-sharing services

Background

File-sharing services, also known as peer-to-peer networking (P2P), use distributed network architectures to allow users to share files, computing capabilities, networks, bandwidth and storage. Users connect to each other directly, without the need for a central point of management. File-sharing software is typically used to download and share music, images, software, videos, games and documents.

Various file-sharing software is available on the internet. Common applications are Morpheus, Kazaa, eMule and LimeWire. Some are free, while others make a nominal charge to download the file-sharing software.

Some free versions of file-sharing software include banners and pop-up advertising, spyware and third-party software. Software for which a charge is made typically does not include these, while offering other facilities, such as voice chat rooms and Internet Relay Chat.

Benefits

File-sharing networks, like chat services, can develop a sense of community among users, particularly in areas such as gaming. The use of file-sharing networks is primarily a recreational activity; it is unlikely that it has any application in the school setting, although this may change in the future.

Risks

There are numerous concerns regarding file-sharing:

Intellectual property

A key risk of file-sharing networks is that many of the files available for download have been made available illegally, and hence those downloading or swapping files are breaching intellectual property rights.

The British music industry estimates that illegal file-sharing has cost it £1.1 billion over the last three years and continues to take legal action against individuals involved in illegal file-sharing. The British Phonographic Industry (BPI) hopes to work with ISPs to freeze the accounts of customers who illegally file-share.

Children are not exempt from prosecution – as already referenced in section 5, the youngest file sharer to be sued to date (in the USA) was just 12.

There are, however, an increasing number of authorised sites, such as Napster and iTunes, where files can be downloaded for a small charge without breaching copyright.

Exposure to inappropriate content

There is a risk that when using file-sharing services, children may be exposed to inappropriate or illegal content. This could be in the form of songs with age-inappropriate or explicit lyrics, or image or video files that have incorrect or misleading titles or descriptions. It is unfortunate but true that some users of P2P networks circulate porn or other offensive content by disguising it as a file with an innocent name, such as the name of the latest family blockbuster, in a bid to attract children.

Exposure to inappropriate contact

Many P2P applications make additional services available, such as voice chat rooms and Internet Relay Chat. The same rules should be applied when using P2P chat services as when using chat rooms or any other communications device: keep personal information private and if any conversation makes you feel uncomfortable, leave the conversation and do not respond. It may be wise to change your username too.

Viruses and hacking

Users of P2P networks can lay themselves open to increased risks of virus infections and hacking attempts. When joining a P2P file-sharing service, you are asked which directory on your hard drive you want to permit other P2P users access to, but it is very difficult to ensure that the rest of your PC is absolutely secure.

Strategies for safe use

Given it is unlikely that P2P networks have any application in the school setting at present, schools may want to block the installation of file-sharing software onto school networks.

It is, however, likely that children will access P2P networks in other settings. Schools should therefore take a role in educating pupils about the issues.

Use only authorised services

As already stated, downloading unauthorised copies of files is illegal and may result in prosecution. Many services offer legal downloading of files for a small charge. However, this could have financial implications for children.

Using filtering tools

Many P2P applications, such as Kazaa, offer a level of filtering based on the descriptive data (metadata) attached to a file to exclude files that may contain offensive or adult content, or that contain any of a user-defined list of blocked words. However, such filters are effective only if the creator of the file has taken the time and effort to attach suitable keywords; some creators attach misleading keywords as a way of distributing inappropriate content.

Some P2P software also allows blocking of certain file types, such as images or video, or executable files with extensions such as .exe, .vbs or .scr, which can contain viruses.

It is worth noting that some filtering software for home use does not block access to file-sharing applications.

Security

Anyone using file-sharing software should ensure that all downloaded files are checked for viruses, and that appropriate firewall technology is in place.

Further information on the safe use of file-sharing networks is available in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/ schools/esafety**].

Curriculum context

Section 9 of this booklet contains a fuller discussion of how safe use of P2P networks can be embedded into the curriculum areas below.

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2b, 2c, 5c

Key Stage 1	ICT	2a, 3a, 5c
	PSHE and citizenship	5a

Using mobile phones and the mobile internet

Background

Mobile phone use and ownership by young people is growing. The age of ownership is set to fall lower still as handsets become cheaper. A number of handsets are appearing on the market aimed specifically at the under 10s.

The *Mobile life youth report 2006*[27] surveyed 1,256 young people (aged 11–17) in the UK to consider the impact of the mobile phone on daily life, family, relationships and school. The report found that more than half of 10-year-olds own a mobile phone (51 per cent), and by the age of 12, 91 per cent own a mobile phone. When asked what they do most with their mobile phones, 74 per cent say they send or receive texts, 14 per cent make or receive calls, and 12 per cent play games.

Mobile technologies have developed rapidly over recent years and continue to do so. A range of services are now available from mobile handsets.

The Short Message Service (SMS) system enables users to send and receive text messages via mobile phones. Messages are usually short and replace a full conversation, particularly if the other user is not available to take a voice call. Messages are usually created from the mobile phone keypad, often using abbreviations.

The Multimedia Message Service (MMS) allows senders to incorporate text, sound, images and video into their messages. Messages are sent as multimedia presentations in a single entry rather than text files with attachments, as with many other forms of electronic communication. MMS also provides support for email addressing, so that messages can be sent from phone to email and vice versa. The sending of MMS messages is also known as 'multimedia messaging', 'mobile multimedia messaging' and 'picture messaging'.

Increasingly, mobile phones and similar devices connected to the mobile networks are available with enhanced and 3G (third generation) features, such as:

- high resolution digital cameras
- MP3 players
- video messaging
- two-way video calling

- mobile access to the internet
- entertainment services in the form of video streaming and downloadable video clips from films or sporting events, and music, horoscopes and games
- location-based services, such as maps and route planners, and finding services based upon the location of the mobile phone user.

Newer handsets capable of receiving these services have traditionally been expensive and available only to customers on contract, so limiting their availability to young people, but this is changing. Handsets are getting cheaper all the time, and there are several 3G pay-as-you-go handsets available that offer all of the above services.

Benefits

Mobile phones offer great opportunities for young people. They can offer freedom, independence and an excellent way to communicate with friends, and, increasingly, a source of mobile entertainment.

Other benefits include the safety aspects: a mobile phone enables a young person to make contact and be contacted, and acts as a location finder for emergency services.

Risks

Potential dangers of mobile phones can be grouped into several key areas:

Exposure to inappropriate materials

Young people may be exposed to material that is pornographic, hateful or violent or encourages activities that are dangerous or illegal. Equally, content may be age-inappropriate, inaccurate or misleading.

[27] The Carphone Warehouse and The London School of Economics and Political Science (LSE) (2006), *The mobile life youth report 2006: the impact of the mobile phone on the lives of young people* [**http://www.yougov.com/archives/pdf/CPW060101004_2.pdf**].

Physical danger

The risks when accessing the mobile internet are the same as, or possibly greater than, those associated with fixed internet use: children may make inappropriate 'friends', perhaps providing information or arranging a meeting that could risk their safety or that of family or friends. As mobile phones are such personal and private devices, it is difficult for parents to supervise access and contacts in the same way that they can with a PC in the home. Mobile phones are typically always on, and hence a child is always contactable and always vulnerable.

Mobile phones have also been used as a link in the grooming process – when an adult contacts a young person in a chat room with the intention of luring them to an offline meeting for the purpose of sexually abusing the young person. Paedophiles have been known to give their victims mobile phones, so providing a direct route for the 'friendship' to develop from online chat.

The rich content capabilities of mobile phones mean that young people may be sent inappropriate images or videos, or be encouraged to send images or videos of themselves by using integrated cameras. Mobile phone cameras may also enable photos of children and young people to be taken and circulated or posted on websites without their knowledge or permission. Newer services, such as chat, online gaming or dating services, may also provide more opportunities for personal contact.

Location-identification capabilities may make it possible to pinpoint the exact location of children and young people. While this may be welcomed by parents keen to know where their child is at all times, it is not difficult to see how misuse of the technology could arise.

Additionally, mobile phone theft is an increasing problem. The British Crime Survey 2005/6 surveyed 45,000 people. Resulting data suggests a rise in robberies by 22 per cent to 311,000 crimes – the highest level for four years. Factors such as the rise in the number of young people carrying expensive goods, such as mobile phones and MP3 players, are thought to contribute to this increase. Almost half of the victims were under 18.[28]

Cyberbullying

Bullying by mobile phone is particularly harmful. Previously, bullying was mainly an activity conducted in the playground or on the way to or from school, and often the victim could escape for a while to the safety of their home. Bullying by mobile phone, however, can happen at any time, day or night, making it very difficult to ignore.

Legal, financial and commercial considerations

A number of issues that relate to the fixed internet also relate to mobile internet access. These issues include: concerns that a child could do something that has legal or financial consequences, such as giving out a parent's credit card details or doing something that contravenes another person's rights; plagiarism and copyright, especially in relation to downloading music or games; and the fact that children may not be able to differentiate between what is advertising and what is not. These issues could increase with the mobile internet, with easy access to chargeable content in the form of games, downloads, ring tones, logos and other services – all of which are particularly attractive to children and young people.

Spam by text message is already a growing problem, and the rich media capabilities of 3G devices will undoubtedly mean that advertisers become more sophisticated in their campaigns.

Strategies for safe use

The dangers and risks associated with using mobile phone services can be reduced through effective education about the safe and appropriate behaviours to adopt. In common with general e-safety recommendations, young people should be taught the importance of keeping personal information private, the appropriate behaviours to adopt when using mobile phones, the need to critically evaluate any information they find or receive, and the importance of seeking advice from an adult if they see any content or are contacted in a way which makes them feel uncomfortable.

There appear to be no technical solutions yet to filter content and block unwanted contacts on mobile handsets, although mobile operators can set some

---

[28] Out of your hands? website [**http://www.outofyourhands.com**].

restrictions on accounts to limit the types of content which can be viewed and received.

Some specific guidance follows:

Abusive messages

Abusive messages are sometimes sent. When alerted, the mobile phone service provider will help to trace the message and block any further messages from that number. Keeping a note of the times and dates of abusive messages may help to identify the sender. As a last resort, mobile service providers can change a mobile phone number.

Bullying by mobile phone

Bullying by text message has become an unfortunate result of the convenience that SMS and MMS offer. If being bullied by text message, children should immediately seek help from a teacher, parent or carer. They should not respond to the messages, but should keep a detailed diary, recording information such as the content of the message, the date, time and caller ID.

Spam by text or multimedia message

Text messages received from an unknown number are likely to be spam. Such messages should be deleted or, if in doubt, pupils should ask an adult for advice. Children should not be tempted to respond to spam in any form, even if wild promises or incentives are offered.

New forms of content

Mobile phone operators in the UK are taking the concerns arising from new forms of mobile phone content very seriously. In 2004, they published a code of practice for the self-regulation of new forms of content on mobile phones[29] in an attempt to alleviate some of these concerns.

The code of practice aims to protect all mobile phone users, and offers some specific provision for the protection of children and young people. It provides guidance on: new forms of commercial content services when these provide adult content and experiences; internet access provided by the mobile operators; and combating illegal content hosted by third parties on mobile network facilities.

The code does not, however, cover personal communications between individuals, although the mobile phone operators recognise that they have an important educational role when new services offer

opportunities to communicate in ways that have not previously been possible.

Mobile phone theft

In recent years, a mobile phone database has been created to block stolen and lost mobile phones so that they will not work on any UK mobile network, therefore making a stolen phone worthless.

A note of the IMEI number of the handset (a unique 15-digit serial number) should be kept in a safe place. The IMEI number can be found by looking behind the battery of the phone or by keying in *#06#.

If a mobile is lost or stolen, the IMEI number should be reported to the network operator or by calling 08701 123 123. The theft should also be reported to the police. The Immobilise Phone Crime website [**http://www.immobilise.com**] provides further details.

[29] Orange, O2, T-Mobile, Virgin Mobile, Vodafone and 3 (2004), *UK code of practice for the self-regulation of new forms of content on mobiles* [**http://www.mobilebroadbandgroup.com/social.htm**].

Children with mobile phones can take some practical steps to protect themselves from mobile phone theft. For example: keeping a phone out of sight when not in use, using it discreetly, and using the PIN code feature (if available) when the phone is not in use.

Young people should also be taught not to buy cheap mobile phones from friends or acquaintances. Buying phones in this way encourages the cycle of crime. Also, if the IMEI number has been blocked, the handset will not work.

Premium rate services

Premium rate services offer information and entertainment via landline telephone, mobile phone, PC (by email, the internet or bulletin boards) and interactive digital TV services. Services range from voting and advice lines to competitions and chat services.

With increasing access to technology outside school, whether by mobile phone or PC, children should be taught the safe and responsible behaviours to adopt when using premium rate services, as part of their general digital literacy skills development. Key considerations are:

- **Obtaining parental permission:** Children should be encouraged to always seek permission before accessing a premium rate service, be it via the home landline, their mobile phone or their PC.

- **Cost implications:** Children should be made aware of the cost implications of using premium rate services. They should always look for and understand the pricing policy for premium rate services before accessing them, and be aware that charges can mount up very quickly.

- **Unsolicited text messages:** Unsolicited text messages, typically stating that the recipient has won a prize which can be claimed by calling a given number, are becoming more widespread. This is of particular concern for children as research has shown that they are not able to differentiate between what is advertising and what is not. Such messages are sent indiscriminately to any mobile phone number, often do not provide clear pricing information, and the prize may be subject to numerous terms and conditions. Children should be taught not to respond to any unsolicited text messages or emails.

- **Access to inappropriate material:** Children should be aware of the risks of accessing inappropriate material if using premium rate services. Services with an adult content should always carry a warning and a declaration that users must be over 18 years of age. However, there may be services which fall outside these controls but still carry age-inappropriate content for young people.

If children do come across any material which makes them feel uncomfortable, they should be taught to disconnect from the service and tell a parent or teacher, who can then take the necessary action.

PhonepayPlus, (formerly ICSTIS, the Independent Committee for the Supervision of Standards of Telephone Information Services), is responsible for regulating the content and promotion of all phone services charged at a premium rate. Its PHONEbrain website, aimed at children aged 10–13, aims to show young people how to stay safe and in control when using premium rate services and understand the mechanisms used to apply charges to phone bills. See section 7 for further information.

Further information on the safe use of mobile phones is available in the e-safety section of the Becta Schools website [**http://www.becta.org.uk/schools/esafety**].

Curriculum context

Section 9 of this booklet offers a fuller discussion of how safe use of mobile phones can be embedded into the curriculum areas below.

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2b, 4e, 5c, 5e

Key Stage 1	ICT	3a, 5c
	PSHE and citizenship	2c, 4d, 5e, 5f

On the horizon...

Technology is constantly evolving and, increasingly, converging to make a greater range of voice and data services available over networks that are accessible from different fixed and mobile devices, such as mobile phones, laptops and PCs.

With the advent of Web 2.0 technologies it seems that every day brings news of emerging interactive services, new and diverse uses of technology and, unfortunately, new e-safety risks.

The capabilities of social software are set to bring about a new wave of virtual communities, many of which may be aimed specifically at children and young people, offering opportunities to share, collaborate and socialise in new ways. Social networking is also set to become increasingly mobile, with sophisticated handsets allowing users to upload content to their profiles while on the move, and location-based services allowing social networkers to 'broadcast' their physical location to those on their 'friends' lists.

Regardless of the constantly changing technological environment, the core e-safety messages remain the same. For example: keep personal information private, remember that people online may not be who they say they are, seek help if you experience anything online that makes you feel uncomfortable, and so on.

The resources featured in the next section can help to teach children and young people these key messages and assist them in developing their own set of safe and discriminating behaviours. By developing e-safety awareness from a young age, children can learn to adapt their behaviours to better protect themselves in any online situation, regardless of how the technologies and their associated risks might evolve.

In the news...

The BBC has announced plans to build a virtual online world for 7 to 12-year-olds. Users will be able to create an online presence and create and share content. There will be a strong focus on safety and responsibility.

For further information, see the BBC News story 'BBC plans online children's world' [**http://news. bbc.co.uk/1/hi/entertainment/6290585.stm**].

7 E-safety resources

The following pages contain an alphabetical listing of some useful resources for teaching e-safety messages. The matrix below indicates which topics are covered by each site.

Resource	General web safety	Email	Chat/IM	Social networks/ blogs	File-sharing	Mobile phones	Online gaming	Cyberbullying	Privacy/identity theft	Digital literacy	Resources for teachers	Resources for parents	See page
BBC ChatGuide	✔		✔	✔		✔	✔	✔	✔		✔	✔	33
Bullying Online	✔					✔		✔			✔	✔	33
CBBC–Stay Safe	✔					✔							34
CEOP's Thinkuknow Cybercafé for Key Stage 2 pupils	✔	✔	✔			✔					✔		34
CyberQuoll	✔		✔								✔		35
Cybersmart Kids Online	✔		✔			✔					✔	✔	35
FKBKO–For Kids By Kids Online	✔	✔	✔		✔	✔							36
Hector's World	✔									✔	✔	✔	36
iKeepSafe.org	✔	✔								✔	✔	✔	37
Internet Safety Zone	✔	✔	✔	✔		✔	✔	✔				✔	37
Kidsmart	✔		✔		✔	✔					✔	✔	38
NetSmartzKids	✔	✔	✔		✔			✔	✔		✔	✔	38
Netty's World	✔	✔	✔			✔	✔	✔	✔	✔		✔	39
PHONEbrain						✔					✔	✔	39
QUICK: The QUality Information ChecKlist	✔									✔			40
Safe Surfing with Doug	✔											✔	40
Smart Surfers	✔								✔	✔	✔	✔	41
Staying SMART Online	✔										✔		41
Surf Swell Island: Adventures in internet safety	✔							✔	✔		✔	✔	42

Please note, inclusion of resources within this booklet does not imply endorsement by Becta, nor does exclusion imply the reverse. Becta does not accept any responsibility for, or otherwise endorse, any information contained within referenced resources, and users should be aware that some resources may contain sponsorship or advertising information. URLs and information given were correct at the time of publication, but may be vulnerable to change over time.

Teachers are advised to check any resources in advance of use to confirm that the content is as expected, and that it is appropriate in tone and level for their pupils.

BBC ChatGuide

http://www.bbc.co.uk/chatguide
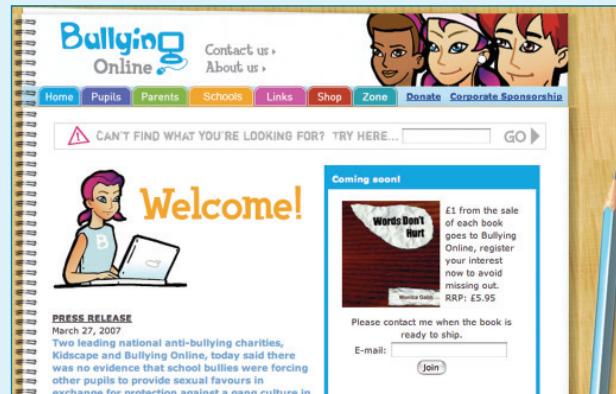
Screen shot reprinted with permission from the BBC

The BBC ChatGuide website provides a range of resources aimed at children, teenagers, parents and teachers.

The Key Stage 2 teaching pack provides resources to assist with providing a lesson on internet safety for children. The downloadable resources include a ChatGuide video and notes for teachers, including suggestions for whole-class activities and a template letter telling parents what they can do to help their children learn the 'rules of the online road'. A Key Stage 3 version of the pack is also available.

Bullying Online

http://www.bullying.co.uk

Screen shot reprinted with permission from Bullying Online

Bullying Online is an online help and advice service combating all forms of bullying. Sections for pupils, parents and schools cover the subject of cyberbullying, with advice on topics including:

- how to stay safe on the internet
- mobile phone bullying and happy slapping
- dangerous websites
- abusive websites.

Bullying Online also provides an email service for pupils in need of further help and advice.

CBBC – Stay Safe

**http://www.bbc.co.uk/cbbc/ help/safesurfing**

Screen shot reprinted with permission from the BBC

CBBC's Stay Safe website invites children to join Dongle the rabbit in learning how to stay safe on the web. The site features a cartoon and quiz, along with a screensaver and wallpaper giving tips on safe surfing. Visitors to the site can also print out Dongle's factsheet reinforcing the SMART rules, which have been adapted to give advice on mobile phone use also.

The site links to the BBC ChatGuide website and to several of the organisations providing advice and support to young people, such as Think U Know, Kidsmart and NCH.

CEOP's Thinkuknow Cybercafé for Key Stage 2 pupils

http://www.thinkuknow.co.uk/cybercafe

Screen shot reprinted with permission from CEOP

The Thinkuknow Cybercafé for Key Stage 2 pupils has been developed by CEOP, together with Becta and the Internet Proficiency Group. It aims to develop a set of safe and discriminating behaviours for pupils to adopt when using the internet and other technologies.

Hosted on the **www.thinkuknow.co.uk** website, the scheme consists of an interactive resource, called CyberCafe, and a teachers' pack consisting of teaching activities, pupils' worksheets and advice and information for teachers on internet safety. Although aimed at Key Stage 2, some of the materials may be particularly useful for introducing e-safety topics to pupils in year 7, or for pupils with special educational needs.

The teachers' pack files and lesson plans can be downloaded as PDF documents from the website.

CyberQuoll

http://www.cyberquoll.com.au

Screen shot reprinted with permission from NetAlert Limited

CyberQuoll helps primary school pupils, aged 8–12, learn about e-safety through a range of fun, interactive activities. It has been developed by NetAlert – Australia's Internet Safety Advisory Body – but the general safety messages still hold for a UK audience.

The main learning tool is an interactive story in which pupils 'follow the cousins from hell through six epic adventures as they stumble through the pitfalls and triumphs of using the internet safely'.

Topics covered include:

- finding stuff
- making waves
- putt'n stuff up
- trying it on
- kids in cyberspace.

A range of teachers' materials are available online to support this resource.

Cybersmart Kids Online

http://www.cybersmartkids.com.au

Screen shot reprinted with permission from ACMA: The Australian Communications and Media Authority

This site has been created by ACMA – the Australian Communications and Media Authority – which is responsible for the regulation of broadcasting, radio communications, telecommunications and online content. The general safety messages still hold for a UK audience.
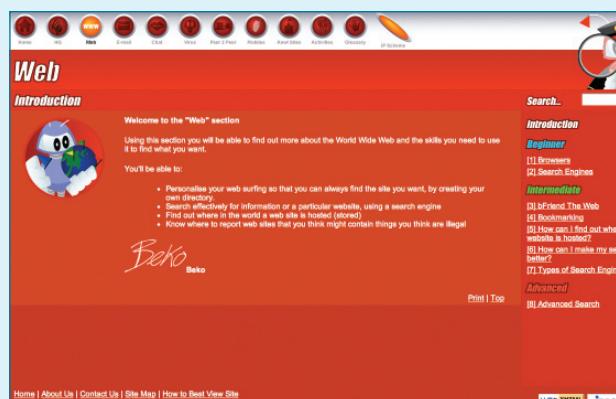
Cybersmart Kids Online provides information on 'smart net surfing for kids and their grownups'. The site gives general tips on staying safe online, along with specific guidance on using chat and mobile phones, and a quiz.

Content in the main information sections is split into three user types – littlies, kids and young people – so pupils can be directed to relevant information depending on their age and/or level of understanding.

A teachers' section provides lesson plans, homework help and links to good educational sites, many of which are UK based.

FKBKO – For Kids By Kids Online
http://www.fkbko.co.uk

Screen shot reprinted with permission from the Cyberspace Research Unit

FKBKO provides a range of e-safety information for children and young people, covering:

- the web
- email
- chat
- viruses
- peer 2 peer
- mobiles.

Topics under each section are typically categorised by 'beginner', 'intermediate' and 'advanced'.

The 'HQ' section also provides some useful background information on topics such as:

- How does the internet work?
- How is my computer identified?
- Am I invisible on the internet?
- Who is in charge of IP addresses?

Hector's World™
http://www.hectorsworld.com

© Internet Safety Group Inc. 2006
Screen shot reprinted with permission from the Internet Safety Group

Hector Protector® – a bottlenose dolphin – and his underwater friends aim to help children aged 3–10 stay safe in cyberspace in Hector's World. This resource comes from NetSafe® – the cyber safety education programme of New Zealand's Internet Safety Group – but the general safety messages still hold for a UK audience.

Animated episodes help children learn about online safety.

A key feature of the resource is the Hector safety button. Once downloaded, Hector can swim alongside children (in a corner of their computer screen) as they surf the internet using Internet Explorer or communicate with others using Outlook or Outlook Express. A child who is upset or worried about an image on the screen can click on Hector. An underwater scene then covers the screen and a reassuring message is displayed saying that the child has done the right thing and can now get adult help. The Hector safety button can be downloaded from the Microsoft New Zealand website [**http://www.microsoft.com/nz/athome/security/children/hector.mspx**].

iKeepSafe.org
http://www.ikeepsafe.org

Screen shot reprinted with permission from the Internet Keep Safe Coalition
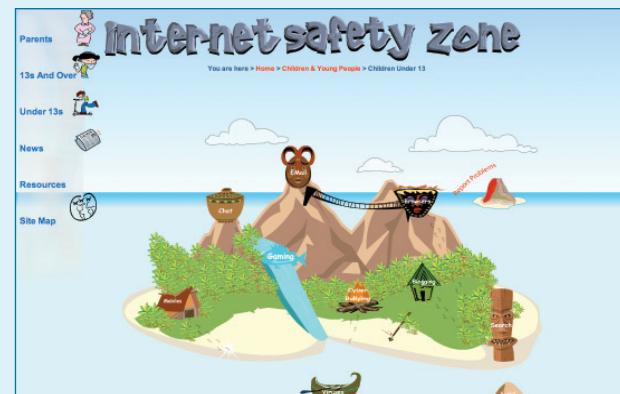
iKeepSafe.org – the online home of the US-based Internet Keep Safe Coalition – teaches the basic rules of e-safety to children and parents. Although the site is US-based, the general safety messages still hold for a UK audience.

The website uses an animated mascot, Faux Paw the Techno Cat, to teach children the importance of protecting personal information and avoiding unsuitable material on the internet. Children can learn how to safely navigate the internet through a virtual playground, Faux Paw's adventures in story books, an animated video download and educational games.

Educational materials, including worksheets and tests, are also available for parents and teachers.

Internet Safety Zone
http://www.internetsafetyzone. com/kids

Screen shot reprinted with permission from the Cyberspace Research Unit

The Internet Safety Zone provides a range of e-safety information categorised into two key areas for under 12s and over 13s.

The under-12s area deals with a range of general e-safety topics, such as:
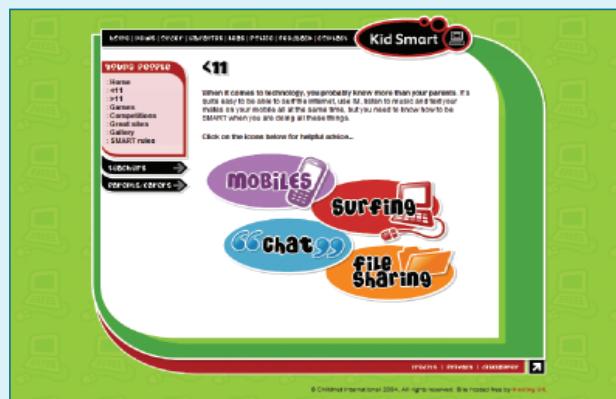
- chat
- email
- browsers
- search
- mobiles
- cyberbullying
- social networking
- blogging
- gaming
- viruses.

There is a general section on reporting problems, which provides links to further sources of help and advice for children and young people.

The site also includes a section for parents covering the basic safety issues of internet use, and the key concerns which parents might have. There is extensive information on how parents can help their children to handle problems and encourage 'cyberwellness'.

Kidsmart

http://www.kidsmart.org.uk/yp/ under11

Screen shot reprinted with permission from Childnet International
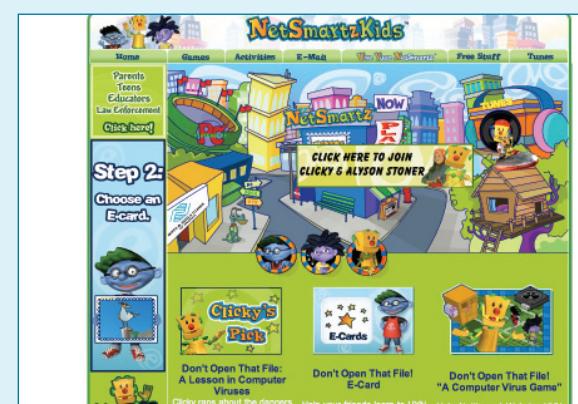
Childnet International's Kidsmart website has a section for young people under the age of 11, dealing with mobiles, surfing, chat and file-sharing.

The site also includes games, competitions and a gallery of young people's artwork on how to stay safe online.

The website reinforces the SMART rules and has additional sections for teachers, and parents and carers.

NetSmartzKids

http://www.netsmartzkids.org

Screen shot reprinted with permission from the National Center for Missing and Exploited Children (NCMEC)

The NetSmartz workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) for children aged 5–17, parents, guardians, educators and law enforcement that uses age-appropriate, 3-D activities to teach children and young people how to stay safer on the internet.

NetSmartzKids.org, aimed at the lower age groups, teaches internet safety messages in a fun way using a range of characters, songs, videos and quizzes.

The site is USA based, but the general safety messages still hold.

Netty's World

http://www.nettysworld.com.au

Screen shot reprinted with permission from NetAlert Limited

Netty's World helps young children, aged 2–7, learn about internet safety through a range of fun, interactive activities. It has been developed by NetAlert – Australia's Internet Safety Advisory Body – but the general safety messages still hold for a UK audience.

The main learning tool is Netty's net adventure, in which Netty travels through a number of adventures similar to those that young children are likely to encounter on the internet. Each adventure includes three levels, of increasing complexity, each of which raise issues which will prompt discussion on important internet safety topics.

Topics covered include:

- exploring the net
- getting things off the net
- using smart phones
- putting work on the net
- making friends on the net.

All of the activities reinforce 'Netty's five forget-me-not's' – important safety messages specifically developed for a younger audience:

- Get help
- Be nice
- Think again
- Stay safe and secure
- Protect what's private.

PHONEbrain

http://www.phonebrain.org.uk

Screen shot reprinted with permission from ICSTIS

PHONEbrain is a new website from PhonepayPlus (the phone-paid services regulator), aimed at children and young people aged 10–13.

Covering four key areas – mobile, landline, TV and PC – the site aims to show young people how to stay safe and in control when using premium rate services and understand the mechanisms used to apply charges to phone bills.
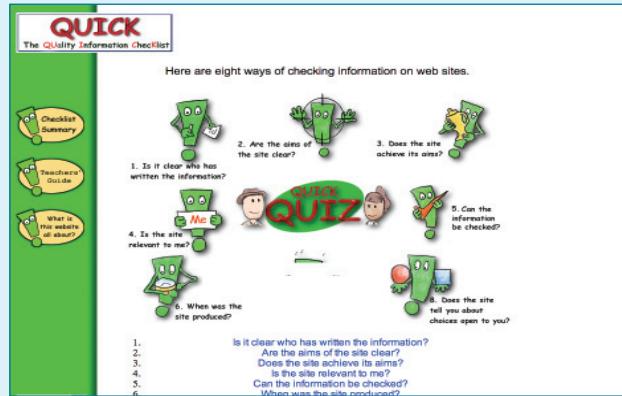
The site uses a number of real-life case studies to reinforce the key messages. Other resources include a jargon buster, technology overview covering 3G services, Wireless Application Protocol (WAP), Bluetooth, and Voice over Internet Protocol (VoIP), and a FAQ section.

Teaching resources include a lesson plan, PowerPoint slides and worksheets, along with 'top tips' sheets which can be downloaded as PDF documents.

Visitors to the site can build up virtual credits by completing various games and activities. Sufficient credits allow users to customise their virtual phones.

QUICK: The QUality Information ChecKlist

http://www.quick.org.uk

*See note below regarding permission

The QUICK website is a teaching aid for Key Stages 2 and 3, and in particular years 5, 6 and 7. It aims to help children evaluate the information they find on the internet, by using fictional examples, quizzes and puzzles to encourage children to explore the concepts around information quality. Although many examples are health related, the concepts can be used with any subjects that require information skills.

There is a useful, printable summary checklist for evaluating information, and a teachers' guide.

*Every effort has been made to trace the copyright holder of this site, without success. We have included it in this updated publication based on permission received for the original publication, as the site continues to provide useful e-safety resources. Should the copyright holder want to contact us, please send an email to **publications@becta.org.uk**.

Safe Surfing with Doug

http://www.disney.co.uk/ DisneyOnline/Safesurfing

Screen shot reprinted with permission from Walt Disney Internet Group

Disney Online's Safe Surfing with Doug, featuring an animated Disney character, uses a variety of fun, interactive tools to help children and young people learn e-safety messages.

Features include safe surfing tips, a printable cyber charter, and a cybernetiquette comic. There is also a parents' guide to safe surfing.

Smart Surfers

http://www.smartsurfers.co.uk

Screen shot reprinted with permission from Link2ICT

Smart Surfers is a web-based resource for Key Stage 2, developed to aid the teaching of critical skills for information searching and staying safe on the web.

The resource focuses on three main areas:

- Smart searching: enables children to gain a comprehensive understanding of the range of issues and technologies involved in searching for information. It introduces the basic elements of the language and grammar of the internet, and gives children the tools and strategies to help them develop essential skills in searching and managing the information they receive.

- Real information: develops the skills to help children identify misleading or harmful information that they come across. Information literacy skills empower pupils to think critically about website information and how they use the web.

- Staying safe: encourages safe, responsible and appropriate behaviour, looking at sharing personal information, passwords, viruses, copyright and plagiarism, trusting people and sites, protecting your data, and correct netiquette.

The teaching units within Smart Surfers can be used as small focused activities within lessons. Activities can be mixed and matched according to pupils' ages and curriculum content. Each unit of work has lesson notes, teachers' resources and pupils' worksheets.

The resource also features an area for 'teaching' parents. This enables schools to share internet skills with parents, so reinforcing key messages to a wider school community.

Smart Surfers is available as an annual subscription: see the website for further information.

Staying SMART Online

http://www.kidsmart.org.uk/ stayingsmart

Screen shot reprinted with permission from Childnet International

Staying SMART Online from Childnet International is an online interactive guide for teachers of primary age children (aged 7–11). It can be used as a presentation tool for teachers or as a stand-alone tool for children to help reinforce the SMART rules.

The 'how-to' guide provides information for teachers about where Staying SMART fits within the National Curriculum and how it could be used as part of a lesson or for a whole lesson. There are also suggestions for follow-up activities.

Surf Swell Island: Adventures in internet safety

http://disney.go.com/surfswell

Screen shot reprinted with permission from Walt Disney Internet Group

Disney Online's Surf Swell Island site is a quiz-driven adventure game.

Internet safety materials are presented in a series of three games, each featuring a classic Disney character and focusing on an area of concern: privacy, viruses or netiquette. Each game is followed by a mini-quiz reinforcing what was presented in the game.

The Challenge of Doom mega-quiz brings together the content from the first three games. By answering correctly, children gain access to a collection of Surf-Swell-themed activities located in the password-protected Treasure Palace.

The site features a printable teachers' guide, which, although based on the US curriculum, gives useful ideas about how to use this resource in the classroom, along with a variety of extension activities. A parents' guide provides similar advice about using the resource in the home.

8 Reporting abuse and seeking further help and advice

In addition to knowing the safe and responsible behaviours to adopt, children and young people, along with the adults who care for them, should know where they can find further information and advice or report problems that they encounter online. The following organisations can help.

Reporting suspicious behaviour online with or towards a child

Image reprinted with permission from CEOP

The Child Exploitation and Online Protection (CEOP) Centre aims to tackle child sex abuse wherever and whenever it happens. It provides a facility, in association with the Virtual Global Taskforce, to report any inappropriate or potentially illegal activity towards a child online. This might be an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child for sex.

If a child is in immediate danger, dial 999 for immediate police assistance.

There are prominent reporting links from the CEOP website [**http://www.ceop.gov.uk**], the Virtual Global Taskforce website [**http://www. virtualglobaltaskforce.com**] and the Thinkuknow website [**http://www.thinkuknow.co.uk**].

A reporting link is also available as a tab option on MSN Messenger.

General help and advice for children and young people

Image reprinted with permission from ChildLine and the NSPCC

ChildLine is a free and confidential helpline. Children and young people in the UK can call 0800 1111 to talk about any problem, 24 hours a day.

For further information, see the ChildLine website [**http://www.childline.org.uk**].

ChildLine is a service provided by the NSPCC. Registered charity numbers 216401 and SC037717.

Reporting illegal content online

Image reprinted with permission from the Internet Watch Foundation

The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal content, specifically child abuse images hosted worldwide and content that is criminally obscene and/or an incitement to racial hatred, hosted in the UK.

A prominent link for reporting illegal content is available from the homepage of the IWF website [**http://www.iwf.org.uk**].

Help and advice for adults concerned with their own or someone else's behaviour, including that of young people

Image reprinted with permission from Stop it Now!

Stop it Now! aims to prevent child sexual abuse by increasing public awareness and empowering people to act responsibly to protect children.

Stop it Now! operates a freephone helpline on 0808 1000 900. It offers confidential advice and support to adults that might be unsure or worried about their own thoughts or behaviour towards children, or the behaviour of someone they know, whether they are an adult or a child. Experienced advisors are available to discuss concerns and can offer confidential advice and guidance on an appropriate course of action.

Further information is available via the Stop it Now! website [**http://www.stopitnow.org.uk**].

43

Help and advice for victims of Cyberbullying and those who support them

Image reprinted with permission from Kidscape

Kidscape is a UK charity committed to keeping children safe, established specifically to prevent bullying and child sexual abuse. The charity works with children and young people under the age of 16, their parents and carers, and those who work with them, to help equip vulnerable children with practical non-threatening knowledge and skills in how to keep themselves safe and reduce the likelihood of future harm.

Kidscape also offer a range of training programmes for both children and those who work with them, covering areas such as:

- Child protection
- Anti bullying
- Personal development
- Promoting positive behaviour
- Staff development.

Kidscape trainers work extensively with a range of organisations including schools and local authorities (and related groups such as parent teacher associations (PTAs), governors, midday supervisors, nursery nurses, and initial teacher trainers), and service groups such as police, youth workers, social workers, children's homes, leisure centres, and foster carers.

For further information, see the Kidscape website [**www.kidscape.org.uk**].

Premium rate services on mobile phones

Image reprinted with permission from PhonepayPlus

PhonepayPlus (formerly known as ICSTIS) is the industry regulator for phone-paid services – the goods and services that we can buy by charging the cost to our phone bills and mobile pre-pay accounts. It has the power to investigate complaints, fine companies and bar access to services that do not comply with the published PhonepayPlus Code of Practice. PhonepayPlus can deal with complaints about the promotion, content and overall operation of phone-paid services (for example numbers beginning with 090 or 091, directory enquiry services beginning with 118 and reverse-billed SMS shortcodes).

The PhonepayPlus website provides information for the public and includes an online complaints form [**http://www.phonepayplus.org.uk**].

If children and young people receive nuisance calls or are bullied by mobile phone, they should contact their mobile operator for further information and advice.
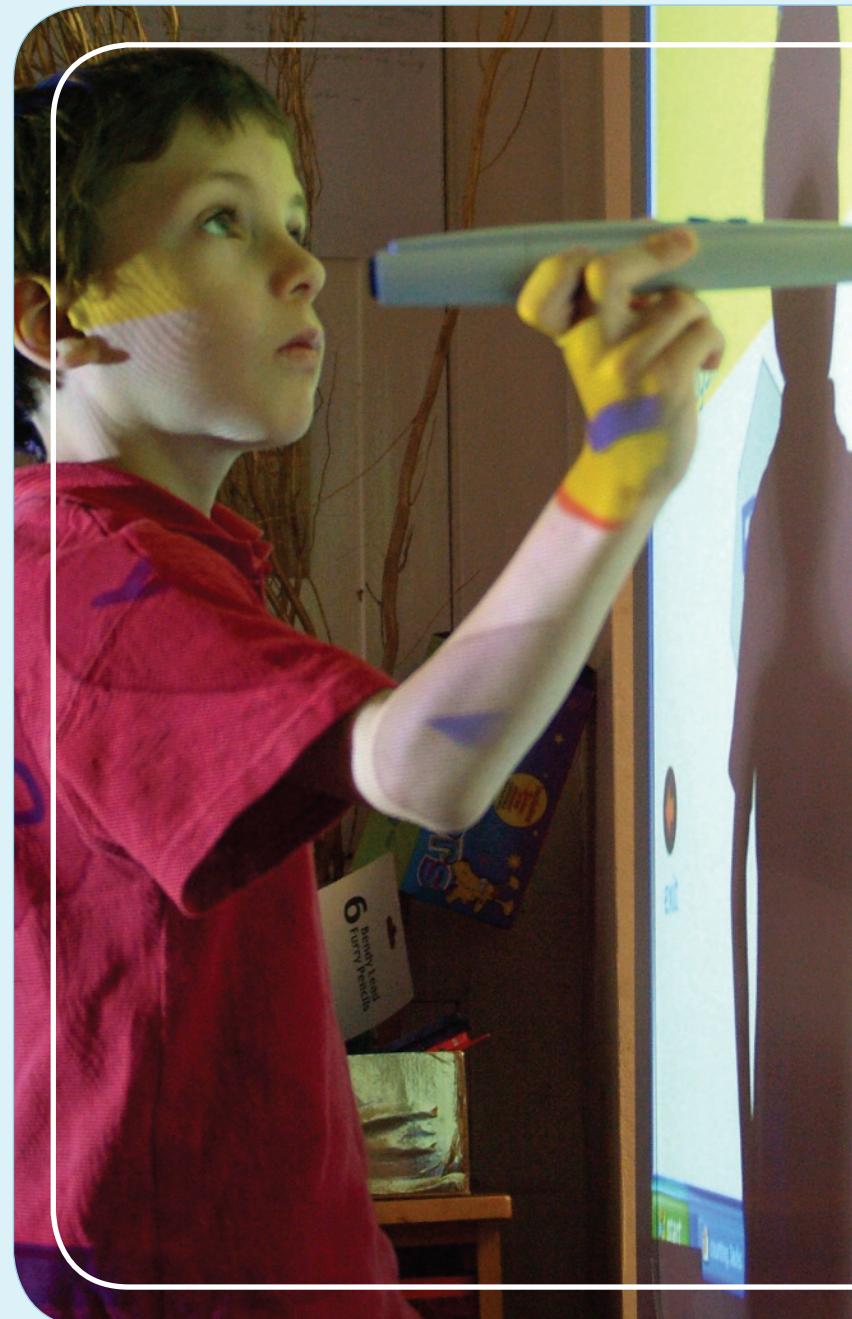
9 Embedding e-safety issues into the curriculum at Key Stages 1 and 2

ICT and, specifically, web-based resources, are increasingly being used across the curriculum. It makes sense, therefore, that e-safety guidance should be given to pupils wherever and whenever such use occurs, in a manner appropriate to the age, understanding and skill level of the children.

Schools are encouraged to look for opportunities for teaching e-safety across the curriculum rather than as a discrete subject, possibly to cover issues that might not be encountered during in-school use of ICT. Although e-safety is not explicitly referred to within the National Curriculum at present, there are a number of appropriate areas within the programmes of study and non-statutory guidelines that offer opportunities to discuss e-safety issues, and these are highlighted within this section.

This booklet focuses on the curriculum areas of ICT, and PSHE and citizenship, and the relevant teaching points from each are duplicated below.

Full details can be found online [**http://www.nc.uk.net**].

Key Stage 1 ICT programme of study

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Finding things out	1a: Pupils should be taught how to gather information from a variety of sources [for example, people, books, databases, CD-ROMS, videos and TV].	This aspect gives opportunities for teaching digital literacy skills to pupils, including how to search effectively on the web, and the importance of critically evaluating any materials they find.
Developing ideas and making things happen	2a: Pupils should be taught to use text, tables, images and sound to develop their ideas.	This teaching point gives an opportunity to highlight the importance of recognising copyright when creating multimedia materials.
	2b: Pupils should be taught how to select from and add to information they have retrieved for particular purposes.	As above (1a), this aspect gives opportunities for teaching digital literacy skills to pupils.
Exchanging and sharing information	3a: Pupils should be taught how to share their ideas by presenting information in a variety of forms [for example, text, images, tables, sounds].	Under this area, pupils can be made aware of some of the safety issues of using email, chat rooms, instant messaging and any other 'direct contact' communications device, along with the importance of keeping personal information private. The notion of appropriate writing conventions, such as language, brevity and tone, for electronic communications could be introduced here. Viruses and other technological risks of exchanging and sharing information could also be covered, along with the issues of plagiarism and copyright.
Breadth of study	During the key stage, pupils should be taught the knowledge, skills and understanding through:	
	5a: working with a range of information to investigate the different ways it can be presented [for example, information about the sun presented as a poem, picture or sound pattern].	This aspect gives opportunities for teaching digital literacy skills, such as the importance of critically evaluating any materials they find for factors such as persuasion, bias or manipulation.
	5c: talking about the uses of ICT inside and outside school.	This is a good opportunity to discuss e-safety within the general context of opportunities and risks presented by new technologies, particularly those that will not typically be encountered in schools; for example, mobile phones and games consoles.

Key Stage 1 PSHE and citizenship

General area of knowledge, skill or understanding	Specific teaching point from the non-statutory guidelines	Relevance to e-safety issues
Developing confidence and responsibility and making the most of their abilities	1a: Pupils should be taught to recognise what they like and dislike, what is fair and unfair, and what is right and wrong.	These teaching points offer a general point of discussion on e-safety issues. Schools may want to focus on the need for children and young people to take responsibility for their own use of technology, developing their own set of safe and responsible behaviours, and recognising when they need help with any issues encountered online.
	1b: Pupils should be taught to share their opinions on things that matter to them and explain their views.	
	1c: Pupils should be taught to recognise, name and deal with their feelings in a positive way.	
	1d: Pupils should be taught to think about themselves, learn from their experiences and recognise what they are good at.	
Preparing to play an active role as citizens	2b: Pupils should be taught to take part in a simple debate about topical issues.	This teaching point could provide an opportunity for discussing topical e-safety issues in general – for example, 'stranger danger' online or the effects of cyberbullying.
	2c: Pupils should be taught to recognise choices they can make, and recognise the difference between right and wrong.	Pupils should learn the responsible behaviours they should adopt when online and develop their own sense of right and wrong in their online activities.
	2d: Pupils should be taught to agree and follow rules for their group and classroom, and understand how rules help them.	This is an excellent area for introducing the concept of acceptable use policies for ICT use. Pupils should be aware of the rules and understand that they exist to help keep them safe when online. They should also be aware of the consequences of not following the rules.
Developing a healthy, safer lifestyle	3a: Pupils should be taught how to make simple choices that improve their health and well-being.	Pupils should learn to develop a set of safe and discriminating behaviours to help protect their wellbeing when online.
	3g: Pupils should be taught rules for, and ways of, keeping safe, including basic road safety, and about people who can help them to stay safe.	Pupils should be taught to minimise the risks to their personal safety when using ICT. They should be taught the basic e-safety rules (for example, the SMART rules), and be encouraged to develop their own set of safe and discriminating behaviours when using the internet and other technologies.

Key Stage 1 PSHE and citizenship (continued)

General area of knowledge, skill or understanding	Specific teaching point from the non-statutory guidelines	Relevance to e-safety issues
Developing good relationships and respecting the differences between people	4a: Pupils should be taught to recognise how their behaviour affects other people.	Pupils should be taught about their right to privacy and the responsibility to protect the privacy of others by not disclosing information when using the internet.
	4e: Pupils should be taught that there are different types of teasing and bullying, that bullying is wrong, and how to get help to deal with bullying.	This is a good area in which to introduce issues relating to cyberbullying, such as by mobile phone or email, or in chat rooms. Pupils should be made aware of the damaging impact that cyberbullying can have on its victims, along with information on where they can go for help and advice if they are suffering.
Breadth of study	During the key stage, pupils should be taught the knowledge, skills and understanding through opportunities to:	
	5a: take and share responsibility [for example, for their own behaviour; by helping to make classroom rules and following them; by looking after pets well].	As above (2d), this is a good area in which to discuss acceptable use policies. When using new technology, pupils need to take responsibility for their own actions, develop a sense of right and wrong, and know where to get further help if they encounter problems.
	5c: take part in discussions [for example, talking about topics of school, local, national, European, Commonwealth and global concern, such as 'where our food and raw materials for industry come from'].	This teaching point could provide an opportunity for a general discussion of e-safety issues.
	5e: meet and talk with people [for example, with outside visitors such as religious leaders, police officers, the school nurse].	The opportunities for communicating with others online (such as via web-based hot seats, video conferencing or controlled chat rooms) could be embraced under this teaching point. E-safety guidance should be reinforced whenever technology is used in the classroom.
	5g: consider social and moral dilemmas that they come across in everyday life [for example, aggressive behaviour, questions of fairness, right and wrong, simple political issues, use of money, simple environmental issues].	This teaching point provides the opportunity for discussing a range of e-safety issues: using technology appropriately, what to do if they see something online that makes them feel sad or embarrassed, or cyberbullying, for example.
	5h: ask for help [for example, from family and friends, midday supervisors, older pupils, the police].	Pupils should know that they can, and should, ask for help if they experience problems when using the internet and other technologies.

Key Stage 2 ICT programme of study

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Finding things out	1a: Pupils should be taught to talk about what information they need and how they can find and use it [for example, searching the internet or a CD-ROM, using printed material, asking people].	This aspect gives opportunities for teaching digital literacy skills to pupils, including how to search effectively on the web and the importance of critically evaluating any materials they find.
	1c: Pupils should be taught to interpret information, to check it is relevant and reasonable and to think about what might happen if there were any errors or omissions.	As above (1a), this is a good area in which to teach digital literacy skills.
Developing ideas and making things happen	2a: Pupils should be taught how to develop and refine ideas by bringing together, organising and reorganising text, tables, images and sound as appropriate [for example, desktop publishing, multimedia presentations].	This teaching point gives an opportunity to highlight the importance of recognising copyright when creating multimedia materials.
Exchanging and sharing information	3a: Pupils should be taught how to share and exchange information in a variety of forms, including e-mail [for example, displays, posters, animations, musical compositions].	Under this area, pupils can be alerted to the safety issues of using email, chat rooms, instant messaging and any other 'direct contact' communications device, along with the importance of keeping personal information private. Viruses and other technological risks of exchanging and sharing information could also be covered here, along with the issues of plagiarism and copyright.
	3b: Pupils should be taught to be sensitive to the needs of the audience and think carefully about the content and quality when communicating information [for example, work for presentation to other pupils, writing for parents, publishing on the internet].	The notion of appropriate writing conventions, such as language, brevity, tone and accuracy, for electronic communications could also be introduced here.
Reviewing, modifying and evaluating work as it progresses	4b: Pupils should be taught to describe and talk about the effectiveness of their work with ICT, comparing it with other methods and considering the effect it has on others [for example, the impact made by a desktop-published newsletter or poster].	There is potential here for discussions regarding the opportunities offered by ICT, particularly in terms of communication, and the corresponding risks.

Key Stage 2 ICT programme of study (continued)

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Breadth of study	During the key stage, pupils should be taught the knowledge, skills and understanding through:	
	5a: working with a range of information to consider its characteristics and purposes [for example, collecting factual data from the internet and a class survey to compare the findings].	This aspect gives opportunities for teaching digital literacy skills to pupils, including how to search effectively on the web, and the importance of critically evaluating any materials they find.
	5b: working with others to explore a variety of information sources and ICT tools [for example, searching the internet for information about a different part of the world, designing textile patterns using graphics software, using ICT tools to capture and change sounds].	As above (5a), digital literacy skills could be covered under this teaching point.
	5c: investigating and comparing the uses of ICT inside and outside school.	This is a good opportunity to discuss e-safety within the general context of opportunities and risks presented by new technologies, particularly those that will not typically be encountered in schools; for example, mobile phones and games consoles.

Key Stage 2 PSHE and citizenship

General area of knowledge, skill or understanding	Specific teaching point from the non-statutory guidelines	Relevance to e-safety issues
Developing confidence and responsibility and making the most of their abilities	1c: Pupils should be taught to face new challenges positively by collecting information, looking for help, making responsible choices, and taking action.	New technologies offer many opportunities and challenges for children. Pupils need to develop their own set of responsible behaviours that can be used and adapted whenever, and wherever, they encounter new technologies.
Preparing to play an active role as citizens	2a: to research, discuss and debate topical issues, problems and events.	This teaching point could provide an opportunity for discussing topical e-safety issues – for example, 'stranger danger' online, or the effects of cyberbullying.
	2b: Pupils should be taught why and how rules and laws are made and enforced, why different rules are needed in different situations and how to take part in making and changing rules.	This is an excellent area for introducing the concept of acceptable use policies for ICT use. Pupils should be aware of the rules and understand that they exist to help keep them safe when online. They should also be aware of the consequences of not following the rules.
	2c: Pupils should be taught to realise the consequences of anti-social and aggressive behaviours, such as bullying and racism, on individuals and communities.	This is a good area in which to introduce issues relating to cyberbullying, such as by mobile phone or email, or in chat rooms. Pupils should be made aware of the damaging impact that cyberbullying can have on its victims, along with information on where they can go for help and advice if they are suffering.
	2d: Pupils should be taught that there are different kinds of responsibilities, rights and duties at home, at school and in the community, and that these can sometimes conflict with each other.	As above (2b), this could be a good area in which to discuss acceptable use policies (AUPs).
	2k: Pupils should be taught to explore how the media present information.	This is a good area in which to explore digital literacy education, evaluating content they find online for tone, bias, accuracy, and so on.
Developing a healthy, safer lifestyle	3a: Pupils should be taught what makes a healthy lifestyle, including the benefits of exercise and healthy eating, what affects mental health, and how to make informed choices.	Pupils should learn how to adopt a healthy online lifestyle – for example, being responsible for their own actions, avoiding risky behaviours, keeping personal information private, and limiting their time spent online.
	3e: Pupils should be taught to recognise the different risks in different situations and then decide how to behave responsibly, including sensible road use, and judging what kind of physical contact is acceptable or unacceptable.	Pupils should be taught to minimise the risks to their personal safety when using ICT. They should be taught the basic e-safety rules (for example, the SMART rules) and be encouraged to develop their own set of safe and discriminating behaviours to adopt when using the internet and other technologies.

Key Stage 2 PSHE and citizenship (continued)

General area of knowledge, skill or understanding	Specific teaching point from the non-statutory guidelines	Relevance to e-safety issues
Developing a healthy, safer lifestyle	3f: Pupils should be taught that pressure to behave in an unacceptable or risky way can come from a variety of sources, including people they know, and how to ask for help and use basic techniques for resisting pressure to do wrong.	This is a good area in which to highlight that people you meet online may not be who they say they are, and that grooming tactics can be used to put pressure on children. Pupils should also be aware of peer pressure in chat rooms – for example, to bully others – or other forms of inappropriate behaviour, and develop strategies for protecting themselves.
	3g: Pupils should be taught school rules about health and safety, basic emergency aid procedures and where to get help.	Pupils should be aware of acceptable use policies for the use of ICT in school, along with what they can do if they experience problems.
Developing good relationships and respecting the differences between people	4a: Pupils should be taught that their actions affect themselves and others, to care about other people's feelings and to try to see things from their points of view.	Pupils should be taught to behave in the online world as they would in the real world: to respect other people's views and avoid being rude or mean to others, and should understand the impact of cyberbullying.
	4c: Pupils should be taught to be aware of different types of relationship, including marriage and those between friends and families, and to develop the skills to be effective in relationships.	This may be a good area in which to discuss friendships and relationships in the online world and the risks that these can present.
	4d: Pupils should be taught to realise the nature and consequences of racism, teasing, bullying and aggressive behaviours, and how to respond to them and ask for help.	This is a good area in which to introduce issues relating to cyberbullying, such as by mobile phone or email, or in chat rooms. Pupils should be made aware of the damaging impact that cyberbullying can have on its victims, along with information on where they can go for help and advice if they are suffering.
	4g: Pupils should be taught where individuals, families and groups can get help and support.	Pupils should learn that they can, and should, seek help from a trusted adult if they see or experience things online that make them feel uncomfortable, embarrassed or upset. They should also be aware of the other organisations that can offer help and advice – see section 8 of this booklet.

General area of knowledge, skill or understanding	Specific teaching point from the non-statutory guidelines	Relevance to e-safety issues
Breadth of study	During the key stage, pupils should be taught the knowledge, skills and understanding through opportunities to:	
	5a: take responsibility [for example, for planning and looking after the school environment; for the needs of others, such as by acting as a peer supporter, as a befriender, or as a playground mediator for younger pupils; for looking after animals properly; for identifying safe, healthy and sustainable means of travel when planning their journey to school].	When using new technology, pupils need to take responsibility for their actions, develop a sense of right and wrong, and know where to get further help if they encounter problems – this could be a good area in which to introduce these ideas.
	5e: meet and talk with people [for example, people who contribute to society through environmental pressure groups or international aid organisations; people who work in the school and the neighbourhood, such as religious leaders, community police officers].	The opportunities for communicating with others online (such as via web-based hot seats, video conferencing or controlled chat rooms) could be embraced under this teaching point. E-safety guidance should be reinforced whenever technology is used in the classroom.
	5f: develop relationships through work and play [for example, taking part in activities with groups that have particular needs, such as children with special needs and the elderly; communicating with children in other countries by satellite, e-mail or letters].	As above (5e).
	5g: consider social and moral dilemmas that they come across in life [for example, encouraging respect and understanding between different races and dealing with harassment].	This teaching point provides the opportunity for discussing a whole range of e-safety issues with pupils; for example: using technology appropriately; what to do if they see something online that makes them feel sad, embarrassed or scared; or cyberbullying.
	5h: find information and advice [for example, through helplines; by understanding about welfare systems in society].	Pupils should learn that they can, and should, seek help from a trusted adult if they see or experience things online that make them feel uncomfortable, embarrassed or upset. They should also be aware of the other organisations that can offer help and advice – see section 8 of this booklet.

10 Opportunities for working with parents, carers and the wider community

This booklet has already mentioned the key role that parents can play through promoting e-safety at home.

ICT offers the opportunity for children and their parents to learn together, and e-safety is an excellent topic for encouraging home–school links.

Childnet International produces a range of materials – as part of its schools awareness programme, Kidsmart – to help schools share information on e-safety issues. Resources include leaflets, books and a series of downloadable fact sheets covering topics such as:

• mobile phones
• searching the internet
• chatting online
• internet addiction
• your family and spam
• putting photos on the web.

Childnet also provides a 54-slide PowerPoint presentation which can usefully be shown at parents' evenings. A multimedia version is also available. For further information, see the Childnet International parents' support website [**http://www.childnet-int. org/safety/parents.aspx**] and the Kidsmart website [**http://www.kidsmart.org.uk**].

A new CD-ROM from Childnet, Know IT All for Parents, commissioned by the DfES, aims to help parents and their children get the most out of the internet and mobile phones. The CD-ROM contains a special section presented by children and young people as well as an advice section for teachers on how they can use the CD-ROM with parents and pupils. There is also a summary 'Overview' section which has been translated into Arabic, Bengali, Gujarati, Mandarin, Polish, Punjabi, Urdu and British Sign Language. Schools in England can order bulk quantities of this resource free of charge from Prolog on 0845 60 222 60, quoting reference: 00308-2007CDO-EN.

NCH, the children's charity, also provides a range of information for parents, including *Dick and Dom's Get IT? Got IT! Good!: a family guide on getting to grips with technology*, produced in association with Tesco Mobile and Tesco Telecoms. For further information, see the e-safety section of the NCH website [**http://www.nch.org.uk/itok**].

The ParentsCentre website has a variety of detailed e-safety information, including information on the benefits of home access to ICT, issues to consider when buying a family PC, developing a family code of practice, and health and safety issues for home ICT use [**http://www.parentscentre.gov.uk/ usingcomputersandtheinternet**].

The *Net family newsletter* is a weekly newsletter designed to keep parents informed of the latest child-relevant developments concerning the internet and related technologies. Although US in origin, it gives a good overview of current and emerging issues, particularly in the areas of social networking, online gaming and mobile phone use. It is distributed via email, blog and RSS feed, or available online [**http://www.netfamilynews.org**].

The resources matrix on page 32 indicates some other sites which also provide information targeted at parents and carers.

Additionally, ICT is a key feature of the extended school programme. Schools are encouraged to support government priorities by extending their ICT facilities to help:[30]

• open up their facilities to the wider community
• bridge the digital divide for those in need of better access to ICT
• enhance access to e-government services
• build skills – to raise the nation's ICT capability
• improve internet access and skills for small businesses
• develop an e-competent population.

When making their ICT facilities available, schools must not only consider how to provide a safe ICT environment for their extended learners, but also the e-safety education and training they can, and should, provide.

---

[30] Teachernet, *Extending the school's ICT to the community* [**http://www.teachernet.gov.uk/_doc/8293/ACF5F55.pdf**].

11 Opportunities for collaboration and sharing good practice

E-safety need not be an activity that schools, or indeed individual teachers, face in isolation. Instead they should look for opportunities to share good practice and learn from the experiences of others. This section suggests a few ideas for doing this.

Local contacts, events and activities

It may be worth checking to see what is going on in your local area.

Local education authorities or Regional Broadband Consortia may have, or be developing, e-safety resources, or may provide guidance on good practice based on local circumstances. Additionally, local safeguarding children boards or local child protection teams may also be able to offer advice in this area.

Many local libraries and UK online centres [**http://www.ufi.com/ukol**] provide guidance on using the internet safely; they may run e-safety events with which the school could be involved.

Likewise many regional police forces run e-safety programmes and may be able to provide specialist training and advice in schools as part of their neighbourhood policing initiatives and safer school partnerships.

Training opportunities

There are a number of resources emerging specifically to help school staff develop their awareness of e-safety issues. These include:

CEOP Training for educators
[**http://www.thinkuknow.co.uk/teachers**]

CEOP offers training through the Thinkuknow Education Programme, aimed at children aged 11-16.

The training is available to anyone who has a professional role in child protection, education or law enforcement – which can include police officers, teachers, social workers, child protection specialists, children's charities and voluntary organisations.

Once trained, educators are able to directly deliver the Thinkuknow programme to children. Further completion of the CEOP Ambassador Training scheme will also allow educators to cascade the training to colleagues.

Training for child protection professionals
[**http://www.ceop.gov.uk/training/courses.html**]

CEOP work alongside colleagues in the criminal justice and child protection agencies in the UK and abroad to add value to existing services and provide greater support to professionals working in this area.

They provide a series of specialist training courses aimed at professionals who:

- conduct criminal investigations where the sexual abuse of children is a factor
- manage offenders in the community or within the justice system
- take responsibility for safeguarding children from sexual predators.

The training courses are designed to help delegates better understand the nature of sexual offending and to develop the skills and knowledge that can better equip professionals to deal with the very difficult and distressing nature of such crimes. One of the courses deals specifically with internet sex offenders.

Reporting abuse

REPORT ABUSE

CEOP provides a facility, in association with the Virtual Global Taskforce, to report any inappropriate or potentially illegal activity towards a child online. This might be an online conversation with someone who a child thinks may be an adult, who is treating a child in a way which makes them feel uncomfortable, or who is trying to meet a child for sex.

If a child is in immediate danger, dial 999 for immediate police assistance.

There are prominent reporting links from the CEOP website, the Virtual Global Taskforce website and the Thinkuknow website. A reporting link is also available as a tab option in MSN Messenger.

Children and the Net
[**http://www.nspcc.org.uk/inform/ trainingandconsultancy/learningresources/ childrenandthenet_wda47890.html**]

The National Society for the Prevention of Cruelty to Children (NSPCC) offers support or training for trainers. Please contact **packs@nspcc.org.uk** or the Information and Administration Officer, Child Protection Learning Resources, NSPCC Training and Consultancy, 3 Gilmour Close, Beaumont Leys, Leicester, LE4 1EZ.

University Certificate in Child Safety on the Internet
[**http://www.internetsafetyzone.co.uk**]

This training for teachers, education and child services professionals aims to enable them to promote safe and responsible use of internet and mobile technologies and services. It is validated by the University of Central Lancashire. Look in the 'news' section for the latest information.

Know IT All
[**http://www.childnet-int.org/kia**]

Childnet International has developed interactive resources to educate young people, parents and teachers about safe and positive use of the internet.

TDA induction materials for teaching assistants in primary schools – ICT
[**http://www.tda.gov.uk/upload/resources/PDF/ P/prim_induction_ict.pdf**]

This course has been designed to support teaching assistants in developing an understanding of ICT in schools, with a particular focus on safety and security.

Home–school links

This booklet has already mentioned the key role that parents can play through promoting e-safety at home. Schools should consider running parents' workshops to share good practice and achieve consistency between safety guidelines in the home and the school.

E-safety resources on the Becta schools website
[**http://www.becta.org.uk/schools/esafety**]

The e-safety section of the Becta Schools website aims to highlight the safety issues relating to new technologies and provide practical information and advice for schools on how to use these technologies safely.

The site is regularly updated with information on emerging technologies and issues, and there are a number of examples of good practice in areas such as email, chat rooms and acceptable use policies.

Any updates or additions to information contained within this booklet will also be posted online.

Becta communities, including the Safetynet online community

The Becta Schools website also offers a number of online communities and forums. Each online community focuses on a different aspect of the use of ICT in education, such as a particular technology or classroom practice, or planning and management issues such as e-safety (see Safetynet opposite). The communities are also a good place to share advice, get feedback on ideas and talk to colleagues with experience of similar roles and situations. An online community can also help you stay informed (and help you inform others) about new events, lesson ideas or funding sources.

Participation takes place via email groups which are free to join. All you need is an email address which you can access and check for messages regularly. To join a group, visit the Becta Schools website and click on the 'Communities' link to see a list of current categories. Once you have found a community you would like to join, click the 'Register' link to start making contributions. You can subscribe to as many groups as you want. Many forums also provide searchable archives of discussions.

Becta Safetynet online community
[**http://lists.becta.org.uk/mailman/listinfo/safetynet**]

Safetynet is a community specifically for anyone who wants to discuss and share information to support the development of e-safety good practice. The community is for educational practitioners, Local Authorities, LSCBs and others who have an interest and/or responsibility in this area. It has been set up to provide:

- peer-to-peer support and access to the shared knowledge and experience of the community
- instant access to colleagues, some of whom may have similar difficulties and concerns
- access to help from other experienced practitioners and interested parties
- up-to-date information.

Safetynet is an open community. This means that anyone with an interest in e-safety is welcome to participate in the discussions. Safetynet is free to join. All you need is an email address which you can access regularly.

For further information go to: [**http://lists.becta. org.uk/mailman/listinfo/safetynet**]

The service is reactively monitored, and all participants are expected to adhere to the Becta Communities Acceptable Use Policy.

Other publications in this series
Becta has produced a number of publications on various aspects of e-safety. Current titles include:

Signposts to safety: teaching e-safety at Key Stages 3 and 4

Signposts to a selection of resources to help teachers of Key Stages 3 and 4 teach e-safety messages in the classroom, along with appropriate curriculum links.

E-safety: developing whole-school policies to support effective practice

This publication provides guidance for schools on developing appropriate policies and procedures to ensure safe use of the internet by the children and young people in their care. It outlines the risks, suggests a policy framework for schools, and gives an overview of the internet safety responsibilities of all the key stakeholders in a child's education. It also provides practical strategies to follow should problems be encountered.

Safeguarding children in a digital world: developing a strategic approach to e-safety

This publication is intended to provide a strategic overview of e-safety issues to policy makers, and outlines a model for a co-ordinated approach by all of the key stakeholders in a child's education. The guidance in this publication refers to policies and documentation related to England. However the principles have resonance across the UK and beyond.

Safeguarding children online: a guide for local authorities and local safeguarding children boards

This publication contains a series of practical checklists for local authorities and, more specifically, for the newly formed local safeguarding children boards for developing a co-ordinated approach to e-safety across all services under their remit. A summary version is also available.

All titles may be ordered (subject to availability) or downloaded as PDF documents from Becta publications [**http://www.becta.org.uk/publications**].