becta advice

Becta

improving learning
through technology

Signposts to safety

Teaching e-safety at Key Stages 3 and 4

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 3 and Key Stage 4 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 also provides 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'.

With the advent of a new curriculum at Key Stages 3 and 4, 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%20space%20-%20web.pdf**].

1 The role of ICT in the lives of young people today

The growth in the number of people using information and communications technology in recent years has been outstanding.

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 compared with fewer than one in three (15 per cent of all UK homes) at the beginning of 2004.

Mobile phone ownership is now approaching saturation point at around 90 per cent of households. 2005 was a record year for sending text messages (by Short Message Service; SMS) in the UK, with approximately 35 billion text messages sent during the year. The data indicates that non-SMS mobile data use – for example, Wireless Application Protocol (WAP) and Multimedia Message Service (MMS) – while still accounting for just a fraction of overall messaging, is nevertheless starting to grow.

These ownership and usage trends are reflected in the younger population.

The UK Children Go Online (UKCGO)[3] 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.

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

[3] 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**].

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 (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.'

A recent study by NCH and Tesco Telecoms looked at parental awareness of new technologies. The resulting report, *Get I.T. safe: children, parents and technology survey 2006*,[4] found 'an alarming gap in knowledge between parents and their children when it comes to technology'.

The study asked 1,003 parents and 1,003 young people aged 11–16 about their use of technology. By surveying both parents and their children it was possible to compare what parents thought their children were doing when using new technologies with what children said they were doing. Specific findings include:

- More than half of all children (53 per cent) are never or hardly ever supervised online by their parents, yet 81 per cent of parents think they know what their children are doing all or most of the time they are online.
- More than a third of parents do not know how to deny access to specific websites or install parental controls, and 40 per cent do not know how to block certain content from being viewed.

  Although two-thirds of parents (65 per cent) are confident they can deny access to specific websites, nearly half of children aged 11–16 (46 per cent), including 43 per cent of 11-year-olds, are confident they can get around such restrictions.
- More than one in 10 of 11-year-olds (11 per cent) say their parents know nothing about who they communicate with online, and 13 per cent say that their parents never supervise their communications.

  When asked about instant messaging, 79 per cent of children say they use it regularly, including 59 per cent of 11-year-olds. However, while 78 per cent of parents are aware that their children use instant messaging, almost one-third (29 per cent) do not understand what instant messaging is.
- One-third (33 per cent) of young people, including 20 per cent of 11-year-olds, regularly use blogging tools (meaning they can publish personal information which can be accessed by anyone). 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.

As the authors of the study conclude, 'this knowledge gap means many parents are unable to provide realistic advice and support to children who are too young to know how to protect themselves from some of the risks associated with new technologies'. There is a clear need, therefore, for children and their parents to learn how to stay safe online.

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. In setting the context, the study asked 11- to 17-year-olds which technologies were most important to them. Thirty-two per cent cited the internet and 26 per cent cited their mobile phone.

[4] 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**].

[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.mobilelife2006.co.uk/PDF/Mobile%20Life%20Youth%20Report%202006%20Colour.pdf**].

Televisions and games consoles were also cited (13 per cent and 12 per cent respectively), as were personal music players (8 per cent). Nine per cent were not sure which technologies were most important to them.

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 said they send or receive texts, 14 per cent make or receive calls, and 12 per cent play games.

When asked specifically about use of mobiles in school, 73 per cent of young people said it is unreasonable to send a text message during a school lesson, but 50 per cent say they have used their mobile phones to send or receive a text during class. Additionally, 11 per cent have used their mobile phones to make or receive calls during a lesson.

When asked specifically about safety issues, 65 per cent of young people think physical bullying is a greater problem for children of their age than bullying by mobile phone (13 per cent). Of boys aged 16 and 17, 20 per cent have sent or received a sexually explicit photo or video, while 11 per cent of girls of the same age have done so. Owning a mobile phone makes 80 per cent of young people feel safer when out and about, but 56 per cent worry that having a mobile phone could make them a target for mugging. Eleven per cent of 11- to 17-year-olds have had their mobile phone stolen.

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. 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.

This booklet provides some signposts for teaching e-safety at Key Stage 3 and Key Stage 4.

2 E-safety and whole-school issues

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 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 young people 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 the older pupils in both primary and secondary schools. The most common breach is the viewing of unsuitable online material. However, the research found that where pupils were taught about e-safety, all breaches of e-safety were reduced.

[6] Becta (2005), *E-safety: developing whole-school policies to support effective practice* [**http://publications.becta.org.uk/download.cfm?resID=25934**].

[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**].

- 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.

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.

The QCA consultation on the review of the secondary curriculum at Key Stages 3 and 4 runs until 30 April 2007. Schools will receive the final statutory programmes of study in autumn 2007 for teaching from autumn 2008. There will then be a three-year period from 2008 to 2010 for schools to implement the revised programmes. The revised programmes of study have a greater emphasis on safe and responsible use of ICT. See section 8 for further details.

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. Strand 1c-4 covers 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 in the leadership and management section of the Becta Schools website [**http://www.becta.org.uk/schools**].

3 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 felt 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:

[8] Becta (2005), *The Becta review 2005: Evidence on the progress of ICT in education*, Becta ICT Research [**http://www.becta.org.uk/corporate/publications/documents/Review_2005.pdf**].

[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://www.becta.org.uk/corporate/publications/documents/The_Becta_Review_2006.pdf**].

[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**].

> ‘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 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.

4 Risks associated with using ICT

Alongside the positive educational and social benefits offered by ICT there are, unfortunately, some dangers, particularly for young people. As in any other area of life, young people 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 young people 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.

The issues that 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 services and technologies, young people 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 young people use ICT. It is natural for young people 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 young people 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 networking sites.

Young people should also be aware of the security risks of accessing certain types of content. These risks include viruses, adware and spyware. Young people 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 networking sites, to make contact with 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, young people might provide information that can identify them or others, thus posing a risk to their safety or that of their family or friends. This risk has increased with the recent popularity of social networking sites. Similarly, young people might arrange to meet someone they have met online.

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 the victims 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 young person could do something that has financial or commercial consequences.

E-commerce continues to grow, and there is a risk that young people 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 young people (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 young people are not able to differentiate between what is advertising and what is not.

Culture

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

There is a risk that young people 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. Young people 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, social networking sites are emerging that are aimed specifically at children and young people, 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 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.

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

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 and young people may become obsessed with new technology, neglecting offline relationships and family contact as a result of spending too much time online.

Young people 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, young people 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 networking sites. Additionally, they may have access to a mobile phone offering text, picture and video 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 young people 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. A complementary Becta publication aimed at teaching e-safety at Key Stages 1 and 2[18] may also be useful.

Additionally, the Internet Proficiency Scheme, developed by Becta, QCA and the DfES, 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. 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**].

[17] Kidsmart: File sharing [**http://www.kidsmart.org.uk/yp/under11/filesharing.aspx**].

[18] *Signposts to safety: teaching e-safety at Key Stages 1 and 2*. See Becta publications [**http://www.becta.org.uk/publications**].

5 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 and pupils. More e-safety resources are described in section 6.

The real-life stories in this section are taken from calls to ChildLine. These stories are often hard hitting, but indicate the real risks and dangers associated with using the internet and related technologies for young people today. All names and identifying details have been changed.

Sections 8 and 9 complement this section, suggesting in more depth areas in which safety messages can be incorporated within the curriculum. They make reference to the National Curriculum programmes of study at Key Stages 3 and 4 and the ICT Key Stage 3 National Strategy, where appropriate.

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, scientific 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 young people, particularly regarding sensitive issues or topics that they would not want to discuss face to face.

The internet also provides efficient means of communicating, such as 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 young people. 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 young people.

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.

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.

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, children should be made aware that such content is not always verified.

Equally, not all educational materials are age-appropriate for secondary school 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[19] 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

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

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 young people and families. Search Engine Watch[20] provides tips and information about searching the web, along with a comprehensive list of search engines for young people.

The Home Office[21] 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**].

Case study

Examples of what is good about the internet:

Carlton, 14: "I wanted to know about a health problem; it was a bit personal and I found the answer on a website. I was too embarrassed to ask my parents or teacher."

Leila, 17: "I've known a boy for two years over the internet... we text and email each other. I have a speech problem, and I can't get out the words I want to say. I'm not shy, but on the internet nobody notices my problem – it's great."

Amanda, 15, talked about her home life, which deeply troubles her just now. There is domestic violence and her parents are divorcing. She self-harms by cutting her arms. "I found some ideas about how to stop on the net, like squeezing ice cubes in my hands. I tried it and it helps."

Carlton's, Leila's and Amanda's stories have been taken from calls to ChildLine. All names and identifying details have been changed.

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

[21] 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 offer opportunities to discuss e-safety issues, and these are highlighted within this section.

This booklet focuses on the curriculum areas of ICT, citizenship and PSHE. The relevant teaching points from the National Curriculum programmes of study are highlighted below.

The ICT Key Stage 3 National Strategy offers similar opportunities for teaching about e-safety.

Sections 8 and 9 of this booklet provide a fuller discussion of how e-safety can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Finding things out	Using data and information sources Searching and selecting
		Exchanging and sharing information	Fitness for purpose Communicating
	Year 8	Finding things out	Using data and information sources Searching and selecting Organising and investigating
		Exchanging and sharing information	Fitness for purpose
	Year 9	Finding things out	Using data and information sources
		Exchanging and sharing information	Communicating

Key Stage 3	ICT	1a, 1b, 3c, 4d
	Citizenship	1a, 1h, 2a
	PSHE	2f, 3a, 3j, 3k

Key Stage 4	ICT	1b, 4b, 4c, 6
	Citizenship	1a, 1g, 2a
	PSHE	1b, 1d, 2b, 3c

Using email

Background

Email is a great way of communicating 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 spelled 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 young people, 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.

Case study

Claire, 13, called ChildLine in the summer holidays because the bullying she was experiencing at school had continued over the summer by computer. Claire said she hated school and dreaded going back. Her parents and brother said she 'should get over it'.

Claire's story is taken from a call to ChildLine. All names and identifying details have been changed.

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 young people 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 young people 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. However, 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.

For further information on cyberbullying, see the DfES's Don't suffer in silence website [**http://www.dfes.gov.uk/bullying**].

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

See also sections 8 and 9 of this booklet for a fuller discussion of how safe use of email can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Exchanging and sharing information	Fitness for purpose Communicating
	Year 8	Exchanging and sharing information	Communicating
	Year 9	Exchanging and sharing information	Communicating

Key Stage 3	ICT	3c
	Citizenship	3c
	PSHE	3k

Key Stage 4	ICT	4b
	Citizenship	3c
	PSHE	–

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 young people 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' young people: that is, to develop relationships online with the aim of persuading young people 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 young people 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[22,23] on the moderation of interactive services.

[22] 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**].

[23] 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**].

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 young people 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[24] website 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. 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.

Section 7 provides information on reporting abuse and seeking further help and advice.

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.

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

Case study

Amy, 14, called ChildLine because she had visited a chat room on the computer after school. She was scared – although she had given a false name and age in the chat room, she had given her mobile number and was receiving obscene messages.

Josie, 13, called because she wondered whether it was safe to meet a boy she had been chatting to online. "I've known him for ages in the chat room, and I really like him. I'm supposed to meet him on Saturday, but I'm not sure I should go."

Sammy, 16, said she had made friends with a boy on the internet and they had arranged to meet. "He said he was the same age as me, but when I got there, there was just this man who looked a lot older. I didn't talk to him, I just came back home."

Carrie-Ann, 14, told the ChildLine counsellor: "Me and my friend Julie met this boy in a chat room who said he was 16. He got Julie's phone number and now he won't stop ringing us. He sounds like he's older."

Dee, 15, rang ChildLine because a man had forced her to have sex with him. "I met him in a chat room and then we said we'd meet up. But he wasn't like I thought. I feel like it's my fault."

Sangeeta, 14, had visited a chat room on the computer after school. She had given a false name and age in the chat room, but she had also given her mobile phone number. "I'm getting really horrible messages, and I'm scared."

Daniel, 16: "I met this guy in an internet chat room. We got chatting and he said he was the same age as me. We were getting on really well, so we swapped email addresses and phone numbers. But then he emailed me a photo which makes him look at least 50, and he said some strange things. He keeps calling my mobile and I don't know what to do."

One girl did not give her name or age: "I've given my mobile phone number to someone over the internet. I think he's a lot older than me, and I've told him not to phone, but he still does. What can I do?"

These stories have been taken from calls to ChildLine. All names and identifying details have been changed.

Automatic login

Many instant messaging programs automatically log registered users on when they access the internet. Young people 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 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

Sections 8 and 9 of this booklet offer a fuller discussion of how safe use of chat and instant messaging can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Exchanging and sharing information	Fitness for purpose Communicating
	Year 8	Finding things out	Organising and investigating
	Year 9	Exchanging and sharing information	Communicating

Key Stage 3	ICT	3c
	Citizenship	3c
	PSHE	2f, 2g, 3a, 3j, 3k

Key Stage 4	ICT	4c, 6
	Citizenship	3c
	PSHE	1b, 1d, 2b, 3b

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.[25] Recent research by Cox Communications in partnership with the National Center for Missing & Exploited Children (NCMEC) in

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

the USA[26] 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 young people 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 and young people, 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 students. GoldStarCafe (a subscription-based service [**http://www.goldstarcafe.net**]) is one such example, providing an online protected learning community open exclusively to Key Stage 3 children (aged 11–14) and their teachers. The Cafe 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.

Section 7 provides information on reporting abuse and seeking further help and advice.

Strategies for safe use

There is much debate over access to social networking sites within educational environments in the UK. Many schools find that these tools are of educational benefit, but equally many are concerned about the risks they can pose. Schools continually need to make decisions about risk factors affecting the day-to-day operation of the school and the wellbeing of pupils, and social networking is no different. Schools need to weigh up the issues, benefits and risks and decide their approach.

It is clear, however, that even if use of social networking sites is blocked within schools, young people will still access them from other settings. As already seen, the NCH/Tesco research (as referenced on page 4) found that parents are largely unaware of tools such as blogs, so schools must therefore teach young people to use these tools safely and responsibly.

[26] 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**].

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 young people by trusted organisations – many of these offer the social experience to young people within a safe, moderated environment.

Keep personal information private

Young people should be taught to keep their personal information private when using social networking tools 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.

Young people should be encouraged to use the privacy features provided on the social networking sites, 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 networking websites could create an anonymous email address that could be easily deleted or changed should unwelcome messages or attention be received.

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 be viewed, copied, shared and manipulated within seconds in front of a worldwide audience.

A good question to ask young people 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.

Young people 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.

Young people 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.

Keep online friends online

Some young people have several hundred online friends. Young people 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. Young people 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, young people should never arrange to meet anyone that they know only online.

Limit time spent online

Young people 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. Young people 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

Sections 8 and 9 of this booklet provide a fuller discussion of how safe use of social networking tools can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Finding things out	Using data and information sources Searching and selecting
		Exchanging and sharing information	Fitness for purpose Communicating
	Year 8	Finding things out	Using data and information sources Organising and investigating
		Exchanging and sharing information	Fitness for purpose
	Year 9	Finding things out	Using data and information sources
		Exchanging and sharing information	Communicating

Key Stage 3	ICT	3c, 4d
	Citizenship	1a, 2a, 3c
	PSHE	2f, 2g, 3a, 3j, 3k

Key Stage 4	ICT	4c, 6
	Citizenship	1a, 1g, 2a, 3c
	PSHE	1b,1d, 2b, 3b, 3c

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 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.

Young people are not exempt from prosecution – as already referenced in section 4, the youngest file-sharer to be sued to date (in the USA) was just 12 years old.

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, young people 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 young people.

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 young people 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 young people.

Using filtering tools

Many P2P applications 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.

In the news...

More than 8,000 alleged file-sharers, across 17 countries, faced legal action in October 2006 in a continuing fight by the international recording industry to put an end to illegal downloading. Parents whose children have been illegally file-sharing were also targeted in the crackdown.

For further information, see the BBC News story 'File-sharers facing legal action' [**http://news.bbc.co.uk/1/hi/technology/6058912.stm**].

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

Sections 8 and 9 of this booklet contain a fuller discussion of how safe use of P2P networks can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Finding things out	Using data and information sources
	Year 8	Exchanging and sharing information	Communicating
	Year 9	Exchanging and sharing information	Communicating

Key Stage 3	ICT	4d
	Citizenship	3c
	PSHE	2f, 3j

Key Stage 4	ICT	4b
	Citizenship	3c
	PSHE	1b, 3c

Using mobile phones and the mobile internet

Background

Mobile phone use and ownership by young people is growing.

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, and 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.

Physical danger

The risks when accessing the mobile internet are the same as, or possibly greater than, those associated with fixed internet use: young people may make inappropriate 'friends', perhaps providing information

[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.mobilelife2006.co.uk/PDF/Mobile Life Youth Report 2006 Colour.pdf**].

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 meeting and 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.

Case study

Fourteen-year-old Karen is asthmatic and her dad bought her a mobile phone for use in emergencies. She received two threatening text messages: 'In five days you'll be dead' and 'You must do what we say, wait for our next call.' Karen thought they might be from two girls in her class who used to be her friends. She was very upset and didn't know who to talk to about the threats.

Danny, 12, called ChildLine because he was being bullied. "They keep kicking and punching me. They send me horrible text messages on my mobile. I've been thinking about committing suicide. I tried to commit suicide once by taking an overdose."

Fifteen-year-old Aisha told her ChildLine counsellor she was being "threatened and mentally bullied" by her former best friend Linda. Aisha had been through quite a lot over the last two years as her mum had died of cancer and she had to take time off school as her hair started to fall out. Aisha said she was really upset by text messages Linda had started sending her. Linda was threatening to kill her and calling her names such as 'slag' and 'prostitute'.

Karen's, Danny's and Aisha's stories have been taken from calls to ChildLine. All names and identifying details have been changed.

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

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

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 may be able to set some 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, young people 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.

Young people 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 mobiles 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#.

The IMEI number of lost or stolen phones 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.

Young people 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.

[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**].

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, young people 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:** Young people 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:** Young people 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 young people as research has shown that children are not able to differentiate between what is advertising and what is not. Such messages are sent indiscriminately, often do not provide clear pricing information, and the prize may be subject to numerous terms and conditions. Young people should be taught not to respond to any unsolicited text messages or emails.
- **Access to inappropriate material:** Young people should be aware of the risks of accessing inappropriate material if using premium rate services. Services with 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 young people 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.

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 6 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**].

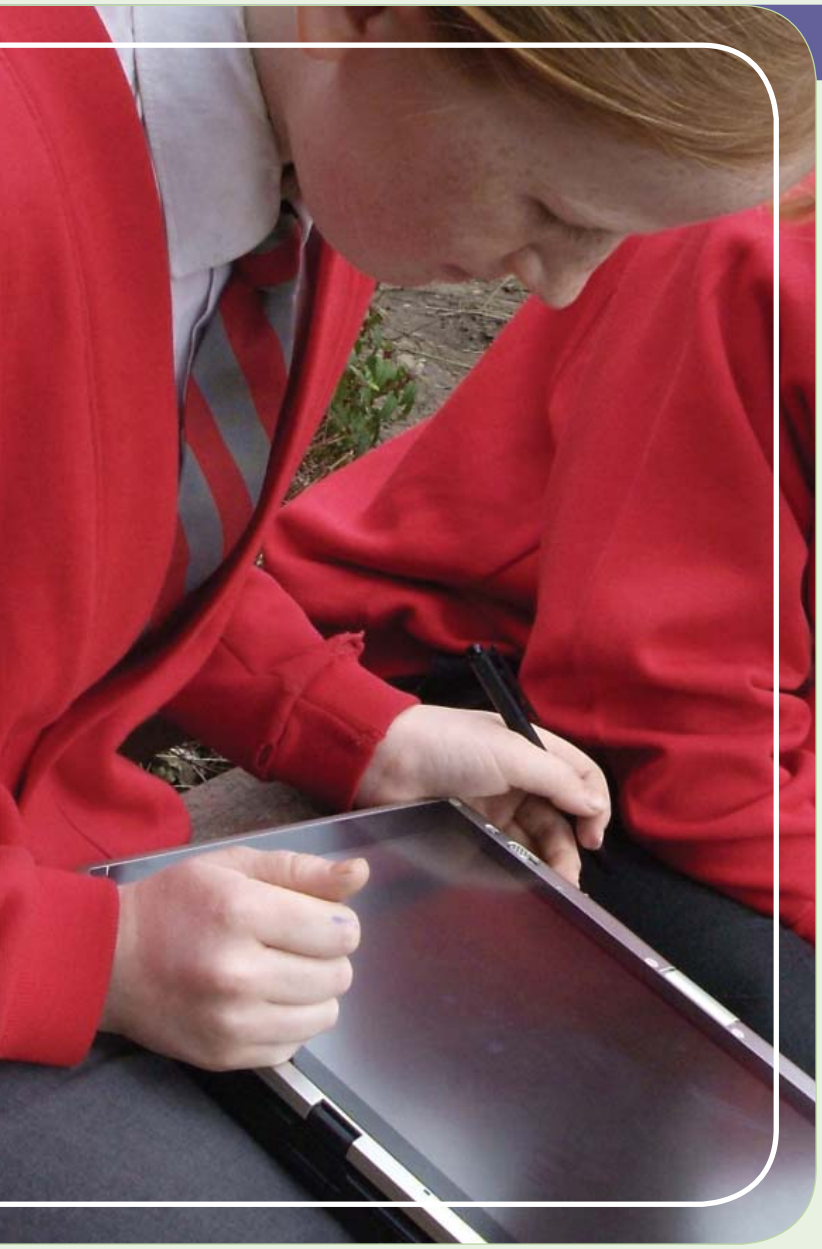
Curriculum context

Sections 8 and 9 of this booklet offer a fuller discussion of how safe use of mobile phones can be embedded into the curriculum areas below.

ICT Key Stage 3 National Strategy	Year 7	Exchanging and sharing information	Fitness for purpose
	Year 8	–	–
	Year 9	Exchanging and sharing information	Communicating

Key Stage 3	ICT	3c
	Citizenship	3c
	PSHE	2f, 2g, 3a, 3j, 3k

Key Stage 4	ICT	4c
	Citizenship	3c
	PSHE	1d, 2b



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 young people these key messages and assist them in developing their own set of safe and discriminating behaviours. By developing and reinforcing e-safety awareness from an early age, young people 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.

6 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.

	E-safety topic												
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	✔		✔	✔		✔	✔	✔	✔		✔	✔	34
BBC Webwise	✔	✔	✔										34
Be Safe Online	✔	✔	✔		✔			✔					35
Blogsafety.com				✔							✔	✔	35
Bullying Online	✔					✔		✔			✔	✔	36
Chatdanger		✔	✔			✔	✔	✔					36
CyberNetrix	✔		✔			✔			✔		✔	✔	37
CyberQuoll	✔		✔								✔		37
Cybersmart Kids Online	✔		✔			✔					✔	✔	38
FKBKO – For Kids By Kids Online	✔	✔	✔		✔	✔							38
Get Safe Online	✔	✔	✔	✔	✔	✔		✔	✔	✔	✔	✔	39
Internet Proficiency Scheme for Key Stage 2 Pupils	✔	✔	✔			✔					✔		39
Internet Safety Zone	✔	✔	✔	✔		✔	✔					✔	40
Kidsmart	✔		✔		✔	✔			✔		✔	✔	40
Know IT All	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔	41
NetSmartz - Teens	✔		✔	✔				✔			✔	✔	42
Out of your hands						✔					✔		43
PHONEbrain						✔					✔	✔	43
QUICK: The QUality Information CheckKlist	✔									✔			44
Sorted	✔	✔			✔				✔	✔			44
Stoptextbully.com								✔			✔	✔	45
Thinkuknow.co.uk	✔		✔	✔	✔	✔	✔				✔	✔	45
Websafe Crackerz	✔	✔	✔		✔	✔		✔					46
Wise Up to IT	✔							✔					46

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.

With the aim of helping teenagers to get the best out of chat and stay safe, the guide is grouped into three key areas:

- Socialising: covering online communities, sharing, blogging, mobile phones, gaming, internet and digital TV.
- Personal safety: covering personal details, meeting up, and moderation and hosting.
- Antisocial behaviour: covering identity, disruption, harassment and grooming.

There is also an extensive glossary covering the language of chat.

The Key Stage 3 teaching pack provides resources to assist with a lesson on internet safety for teenagers. The downloadable resources include:

- notes for teachers, including a quiz and a template for students to keep an internet diary
- ChatGuide video
- PowerPoint presentation.

A downloadable ChatGuide booklet for parents is also available online, which schools can print out and give to parents and carers.

BBC WebWise

http://www.bbc.co.uk/webwise/course

Screen shot reprinted with permission from the BBC

The BBC WebWise site has a range of information on using the internet. The WebWise online course consists of ten lessons to help you become familiar with using the internet. Topics covered include:

- how to hook up
- web page basics
- finding stuff online
- email basics
- stay out of danger
- make new friends.

The 'Stay out of danger' section has an interactive guide and a quiz on child safety, based on the SMART rules.

Be Safe Online

http://www.besafeonline.org

Screen shot reprinted with permission from Learning and Teaching Scotland

The Be Safe Online website, produced by Learning and Teaching Scotland, provides advice and information about internet safety for teachers and parents.

The website covers a wide range of topics, including:

- personal web pages
- email
- chat
- instant messaging
- file-sharing
- bullying online.

BlogSafety.com

http://www.blogsafety.com

Screen shot reprinted with permission from BlogSafety.com

BlogSafety.com is a USA-based forum where parents, teens, educators and experts can discuss and learn about safe blogging and social networking.

Users need to sign up before they can post to the forums, but safe blogging tips for teens and numerous other articles and advice can be accessed without registering.

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.

Chatdanger

http://www.chatdanger.com

Screen shot reprinted with permission from Childnet International

Childnet International's Chatdanger website informs children and young people about the potential dangers of interactive services online, and gives advice to keep them safe.

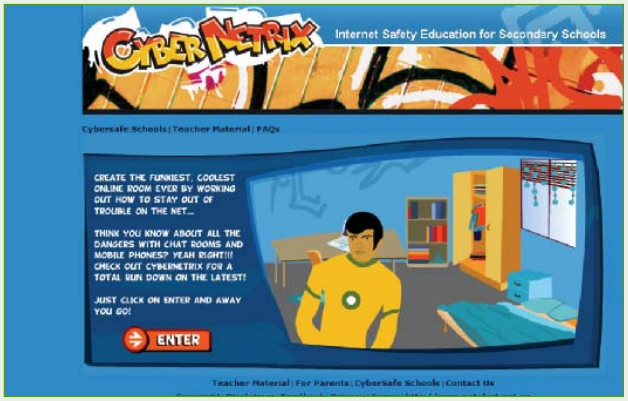
The site covers:

- mobiles
- chat
- email
- Messenger
- games.

The site uses real-life stories and online quizzes to reinforce e-safety messages.

CyberNetrix

http://www.cybernetrix.com.au



Screen shot reprinted with permission from NetAlert Limited

CyberNetrix helps secondary school pupils, aged 13–16, learn about the risks of using the internet and provides advice on managing and minimising those risks. 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 room where students can create their own character and customise their surroundings. By clicking on objects around the room, students can learn key safety messages.

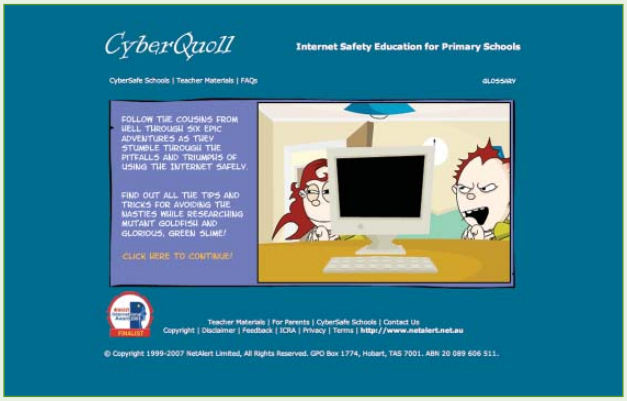
Topics covered include:

- keeping your computer secure
- chat rooms
- internet banking
- identity theft
- mobile phones.

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

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.

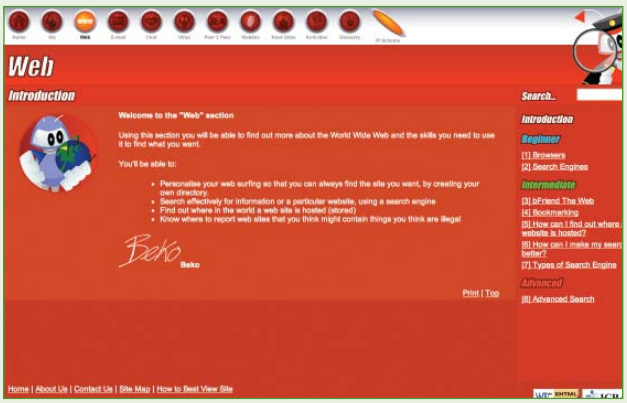
Cybersmart Kids Online provides information on 'smart net surfing for kids and their grownups'. The site gives general tips on staying safe online, along with specific guidance on using chat and mobile phones, and a quiz.

Content in the main information sections is split into three user types – littlies, kids and young people – so students 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-to-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?

Get Safe Online

http://www.getsafeonline.org

Screen shot reprinted with permission from Get Safe Online

Get Safe Online aims to provide expert advice for everyone to protect against internet threats. Although not specifically aimed at children and young people, there is a section titled 'Resources for parents, teachers and young people', which provides a number of helpful articles on topics such as:

- setting ground rules for children
- protecting children from online threats
- filtering internet content
- sharing a home computer.

There are also links to resources for young people and parents and teachers.

Some of the 'knowledgebase' resources on the site are also useful for teaching e-safety issues. These include:

- Protect your PC: This section contains a range of information on how to protect your PC using technology tools such as firewalls, antivirus software and the latest operating system updates. It also provides guidance on stopping spam and spyware, securing wireless networks, and making regular backups.
- Protect yourself: This section contains advice on how to use the internet safely. It is concerned more with behaviour than technology, and provides guidance on how to bank and shop online safely, avoiding fake and unsafe websites, and how to create strong passwords.

There are also a number of interactive tools, such as 'Create a personal security checklist' and a 'Take a risk-assessment quiz'.

Internet Proficiency Scheme for Key Stage 2 pupils

http://www.gridclub.com/teachers/t_internet_safety.html

Screen shot reprinted with permission from Grid Learning Ltd

The Internet Proficiency Scheme for Key Stage 2 pupils, developed by Becta, QCA and the DfES, aims to develop a set of safe and discriminating behaviours for pupils to adopt when using the internet and other technologies.

Hosted on the GridClub website, the scheme consists of an interactive website, called CyberCafe, and a teachers' pack consisting of teaching activities, pupils' worksheets, advice and information for teachers on internet safety, and certificates to award on completion of the scheme.

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 can be downloaded as PDF documents from the website.

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 for under 12s and over 13s.

The over-13s area deals with a range of general e-safety topics such as email, mobiles, chat, gaming and browsing, and also covers many of the negative social and abusive aspects of new technology, such as:

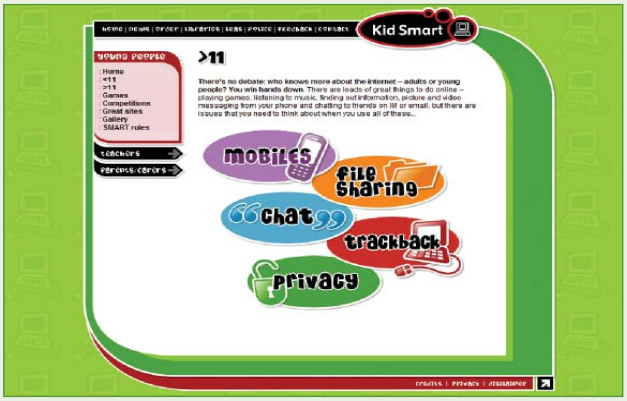
- sexual content
- violence
- abusive cybersex and grooming
- cyberbullying
- eating disorders
- self-harm and suicide
- prejudice.

Each of the topics provides information on reporting abuse and further sources of help and advice for 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 handle problems and encourage 'cyberwellness'.

Kidsmart

http://www.kidsmart.org.uk



Screen shot reprinted with permission from Childnet International

Childnet International's Kidsmart website has a section for young people aged 11 plus, dealing with mobiles, file-sharing, chat, trackback (for example, digital footprints) and privacy.

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

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

Know IT All
CD-ROM and resource pack

http://www.childnet-int.org/kia

Image reprinted with permission from Childnet International

Know IT All (KIA) is an interactive CD-ROM aimed at Key Stage 3 and 4 pupils, to help them understand a broad range of issues when using the internet or mobile phones. Every secondary school in the UK was sent a free Know IT All pack in late 2005. Additional packs can be purchased directly from Childnet International [**http://www.childnet-int.org/kia/order.aspx**].

The main aim of Know IT All is to help students reflect on their use of communication technology, be aware of the dangers and develop safe and discriminating behaviour when using new technology.

Using a combination of animation, fictional stories, interactive quizzes and movies, the resource emphasises how young people can protect themselves from hazards online and how they can look after each other by behaving responsibly and not putting others at risk. Topics covered include:

- anonymity and online behaviours
- evaluating web content, including identifying illegal content
- unwelcome communications, including spam, viruses and phishing scams
- online friends, including issues relating to cyberbullying, online harassment and chat dangers
- the use and abuse of mobile phones
- file-sharing, including issues relating to downloading music and video, and associated risks and legal issues.

An additional Know IT All Teachers' Guide gives background to each of the sections covered on the CD-ROM, with explanations of terms, and is essential for getting the most out of this resource. The guide contains ideas on how to use KIA as part of a lesson or a whole-school assembly, as well as further resources on a broad range of topics from copyright to cyberbullying. The guide also maps the sections within KIA to relevant parts of the National Curriculum at Key Stage 3 for ICT, PHSE and Citizenship.

The Teachers' Guide can be downloaded from the Childnet International website [**http://www.childnet-int.org/kia/teachers.aspx**].

Image reprinted with permission from Childnet International

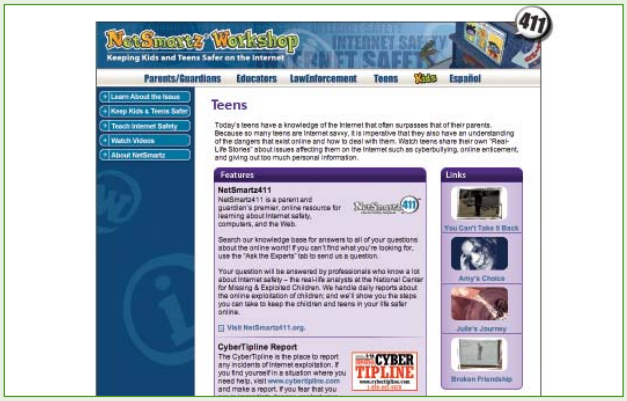
A new CD-ROM resource, Know IT All for Parents, commissioned by the DfES, aims to help parents and their children get the most out of the internet and mobile phones.

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.

NetSmartz – Teens

http://www.netsmartz.org/netteens.htm



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.

The NetSmartz Teens section provides hard-hitting e-safety messages predominantly through a series of real-life stories told by teens who have been victims of internet exploitation. These include:

- Amys' Choice: gives an account of the risks of meeting people in the real world that you have first met while chatting.
- Julie's Journey: tells the story of a 13-year-old girl who left home for three weeks with a convicted murderer after developing a relationship online.
- Tracking Teresa: demonstrates how even the smallest details provided while chatting create a trail of personal information.
- Teens PSA: 'Promises', a public service announcement, warns teenagers of the dangers of falling for promises from people they first meet online.

The site also features a new series on cyberbullying:

- Feathers in the Wind: discusses what teens can do to avoid becoming a victim or victimising someone else.
- You Can't Take It Back: tells the story of teen who reflects on his participation in a website created to rate others at his school, and his subsequent regret.
- Broken Friendship: tells about the impact of sharing online passwords, even with best friends.

Each of the stories links to a series of activity cards and related news articles which can be used to prompt further discussion in the classroom.

The site also features numerous resources for teachers and parents.

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

Out of your hands?

http://www.outofyourhands.com

Screen shot reprinted with permission from the Home Office

Out of Your Hands? is a citizenship resource for Key Stage 3 pupils, designed to tackle the problem of mobile phone crime.

Aimed at 11- to 14-year-olds, the website offers an interactive, peer-led approach to dealing with the issues of mobile phone crime, including how to prevent it and what to do if you have your phone stolen.

There are accompanying notes for teachers and youth leaders, consisting of printable activities and National Curriculum links.

PHONEbrain

http://www.phonebrain.org.uk

Screen shot reprinted with permission from ICSTIS

PHONEbrain is a new website from ICSTIS (the premium rate services regulator), aimed at 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.

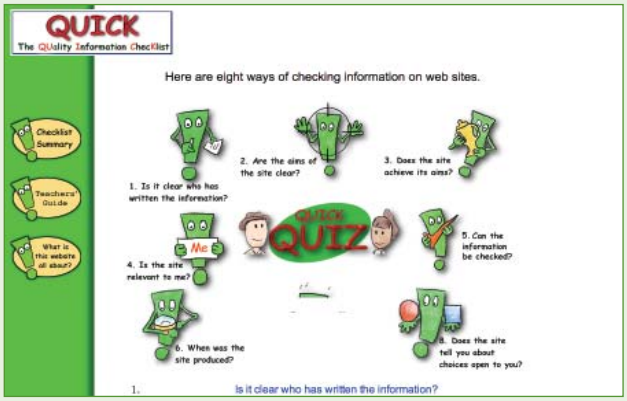
The site uses a number of real-life case studies to reinforce the key messages. Other resources include a jargon buster, technology overview covering 3G services, Wireless Application Protocol (WAP), Bluetooth, and Voice over Internet Protocol (VoIP), and a FAQ section.

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 games and activities. Sufficient credits allow users to customise their virtual phones.

QUICK: The QUality Information CheckKlist

http://www.quick.org.uk



*See note below regarding permission

The QUICK website is a teaching aid to help young people evaluate the information they find on the internet. It consists of fictional examples, quizzes and puzzles to allow young people 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.

The site is aimed at Key Stages 2 and 3, and in particular years 5, 6 and 7. Some of the examples might seem a little 'young', but the underlying principles are sound.

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 email to **publications@becta.org.uk**.

Sorted: Keep your information secure online

http://www.childnet-int.org/sorted

Screen shot reprinted with permission from Childnet International

Childnet International's Sorted website has been designed by young people, for young people, to provide advice and information on computer security issues in a practical and simple way. It covers:

- spyware and adware
- trojans and viruses
- spam and phishing
- identity theft
- pop-ups
- file-sharing.

The site also includes 10 top rules for maintaining privacy.

Stoptextbully.com

http://www.stoptextbully.com

Screen shot reprinted with permission from NCH [http://www.nch.org.uk]

This NCH site gives advice on cyberbullying under a number of headings, such as:

- text
- calls
- photos
- emails
- chats
- web
- identity.

It includes information for parents and teachers, along with a downloadable poster of top-10 tips, and an (offline) classroom quiz designed to find out how much pupils know about mobile bullying and the sources of help available to them.

Thinkuknow.co.uk

http://www.thinkuknow.co.uk

Screen shot reprinted with permission from CEOP

This website, developed by the Child Exploitation and Online Protection (CEOP) Centre, provides information for young people on how to stay safe online. It covers various topics, including:

- mobiles
- gaming
- social networking
- chatting
- podcasts
- blogs
- P2P TV.

A teachers' area provides information on training and materials to support the Think U Know programme. The site also provides a link to a parents' area (hosted on the CEOP website) with a good overview on technologies such as:

- chat and instant messenger
- blogs, forums and social networking
- mobiles
- gaming.

Each of the parents' topics includes a summary of what's good, what's bad and what parents can do to help their children stay safe.

In all areas of the site, there are prominent links to the CEOP 'report abuse' page where you can make a complaint or report a problem.

Websafe Crackerz

http://www.websafecrackerz.com

Screen shot reprinted with permission from Microsoft Corporation

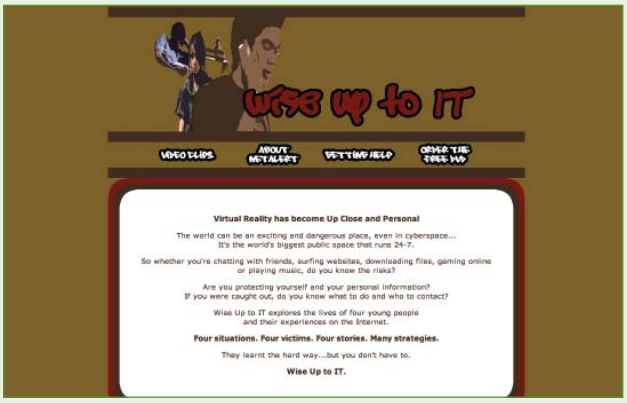
Websafe Crackerz is a spoof world, with a range of microsites offering teenagers strategies to help them deal with all kinds of technology-related situations. The site makes use of interactive stories and games to teach e-safety in a fun, non-patronising way, offering prizes to those that can navigate the cyber-hazards and crack the safe.

The microsites include:

- BBB or BlahBlahBlah.com: deals with issues surrounding communicating via the internet – for example, using chat and IM. It also looks at anonymity and how to protect your personal information.
- Don't click here: deals with the world of dodgy sites, including online scams, pop-ups and spyware. It provides advice on evaluating material found online and how to be a safe online shopper.
- S.P.A.M. Corp: deals with all the issues relating to spam, including how to protect your presence and your PC, and how to prevent mobile spam.
- Ih8u: deals with the many forms of abuse – such as online abuse, mobile phone abuse, cyberbullying, self abuse and identity theft – that can happen with new technology.
- Nick-star: is a mock file-sharing site which deals with issues surrounding safe downloading, legal issues, and bugs, spyware and adware.
- InTransit: deals specifically with the ever-expanding range of services available via mobile phones and the issues which these raise. Topics covered include Bluetooth, tracking services, moblogging and camera phones.
- H@cktev15t: provides a news-based section for teenagers, drawing together technology-related news from the BBC, details of current technology security threats and links to virus-removal tools, and general information on the law and reporting online abuse.

Wise Up to IT

http://www.wiseuptoit.com.au



Screen shot reprinted with permission from NetAlert Limited

Wise Up to IT explores the lives of four young people and their experiences on the internet through four hard-hitting video case studies. Topics covered include cyberbullying, spyware, the risks of meeting online friends in the real world, and cyberstalking.

This resource was developed by NetAlert – Australia's Internet Safety Advisory Body – but the general safety messages still hold for a UK audience.

7 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.

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**].

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 and the NSPCC joining together for children.

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**].

Premium rate services on mobile phones

Image reprinted with permission from ICSTIS

ICTIS, the Independent Committee for the Supervision of Standards of the Telephone Information Services, is the industry regulator for premium rate telephone services. It has the power to investigate complaints, fine companies and bar access to services that do not comply with the published ICSTIS code of practice.

ICSTIS can deal with complaints about the promotion, content and overall operation of premium rate services (for example numbers beginning with 090 or 091, directory enquiry services beginning with 118 and reverse-billed SMS shortcodes).

The ICSTIS website provides information for the public and includes an online complaints form [**http://www.icstis.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.

8 Embedding e-safety issues into the curriculum at Key Stages 3 and 4

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 pupils. This could be in the form of a reminder of the school's acceptable use policy before going online in a geography lesson to look at a live webcam of volcanic activity, or a reminder, in an English lesson, of the need to critically evaluate materials found on the web and observe copyright restrictions.

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 that offer opportunities to discuss e-safety issues, and these are highlighted within this section.

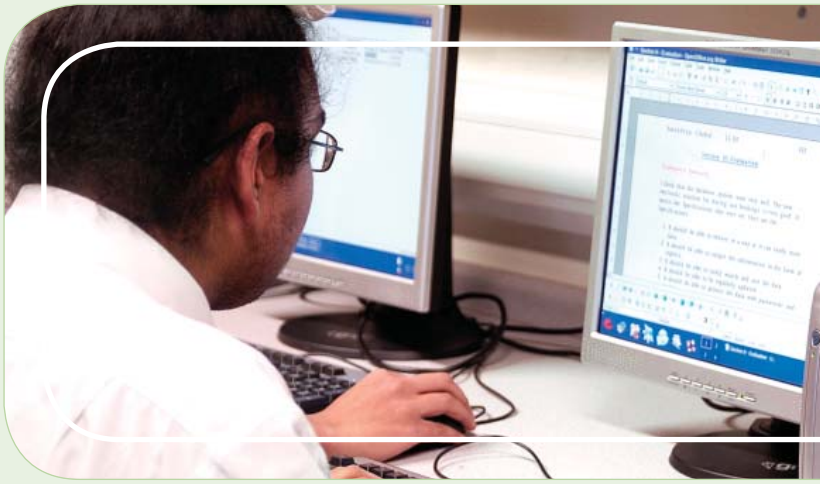
This booklet focuses on the curriculum areas of ICT, citizenship and PSHE, and the relevant teaching points from the programmes of study of each are duplicated below.

The full programmes of study can be found on the National Curriculum online website [**http://www.nc.uk.net**].

Additionally, the QCA consultation on the review of the secondary curriculum at Key Stages 3 and 4 runs until 30 April 2007. Schools will receive the final statutory programmes of study in autumn 2007 for teaching from autumn 2008. There will then be a three-year period from 2008 to 2010 for schools to implement the revised programmes of study.

The revised programmes of study are designed to provide greater flexibility for teachers, greater coherence for the curriculum as a whole, and increased personalisation of the curriculum for learners. The revisions will provide opportunities for schools to renew their curriculum based on greater flexibility to meet pupils' needs, and enhanced by newer priorities such as:

- the Every Child Matters agenda
- personal, learning and thinking skills
- the aims of the curriculum.



The revised programmes of study can be viewed on the QCA website [**http://www.qca.org.uk/secondarycurriculumreview**], where you can also view supporting materials designed to help you develop the new curriculum and implement the programmes of study.

There is a greater emphasis on safe and responsible use of ICT in the revised programmes of study. Examples of this emphasis include:

- a case study on promoting safety in ICT at Key Stage 3 [**http://www.qca.org.uk/secondarycurriculumreview/subject/ks3/ict/planning/case-study-1/index.htm**]
- explanatory notes within the programme of study for PSHEE personal well-being (non-statutory) Key Stage 3 curriculum opportunities that state 'internet safety should be addressed explicitly' [**http://www.qca.org.uk/secondarycurriculumreview/subject/ks3/pshee/personal-well-being/index.htm**] (explanatory notes are available as speech bubbles or via the download)
- guidance within the programme of study for PSHEE personal well-being (non-statutory) Key Stage 4 curriculum opportunities that states 'They [students] should communicate safety messages relating to internet use' [**http://www.qca.org.uk/secondarycurriculumreview/subject/ks4/pshee/personal-well-being/index.htm**].

Continuing opportunities for teaching e-safety should also be explored, such as the QCA ICT functional skills standards for 14–19 education [**http://www.qca.org.uk/15895.html**].

Key Stage 3 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 be systematic in considering the information they need and to discuss how it will be used.	This aspect gives opportunities for teaching pupils about copyright issues, particularly in relation to materials which they find on the internet and may want to use to inform their work.
	1b: Pupils should be taught to obtain information well matched to purpose by selecting appropriate sources, using and refining search methods and questioning the plausibility and value of the information found.	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.
Exchanging and sharing information	3c: Pupils should be taught how to use ICT, including email, to share and exchange information effectively (for example, web publishing, video conferencing).	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. This is also a good place to discuss issues relating to Web 2.0, such as social networking tools. The notion of appropriate writing conventions, such as language, brevity and tone, for electronic communications could also be introduced here.
Reviewing, modifying and evaluating work as it progresses	4d: Pupils should be taught to be independent and discriminating when using ICT.	This aspect effectively underpins all ICT work with an awareness of e-safety issues. Pupils should be encouraged to take a common-sense approach to using the internet and related technologies, knowing the appropriate behaviours that they (and others) should adopt online, along with appropriate strategies to use if things go wrong.

Key Stage 3 citizenship programme of study

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Knowledge and understanding about becoming informed citizens	1a: Pupils should be taught about the legal and human rights and responsibilities underpinning society, basic aspects of the criminal justice system, and how both relate to young 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.
	1h: Pupils should be taught about the significance of the media in society.	The internet is becoming an increasingly important form of media in our society As part of becoming 'informed citizens', pupils should be aware of the risks and dangers of this form of media, alongside the many benefits.
Developing skills of enquiry and communication	2a: Pupils should be taught to think about topical political, spiritual, moral, social and cultural issues, problems and events by analysing information and its sources, including ICT-based sources.	While looking at internet-based resources, pupils should be encouraged to consider their appropriateness. They should be aware that they might encounter inappropriate content on the internet which may contain extreme political or social views, and may be biased in opinion. As part of digital literacy education, pupils should be taught to critically evaluate any material they find.
Developing skills of participation and responsible action	3c: Pupils should be taught to reflect on the process of participating.	This teaching point provides a good opportunity to discuss the issues relating to communicating using ICT. The safety issues of using email, chat rooms, instant messaging and text messaging can be discussed, alongside the problems of cyberbullying which are often associated with these forms of technology. This is also a good place to discuss issues relating to Web 2.0 technologies, such as social networking tools.

Key Stage 3 PSHE programme of study (non-statutory)

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Developing a healthy, safer lifestyle	2f: Pupils should be taught to recognise and manage risk and make safer choices about healthy lifestyles, different environments and travel.	Pupils should be taught to minimise the risks to their personal safety when using ICT. Studies have identified that young people often engage in risky behaviours when using chat rooms, and this is a good place to discuss the issues. This includes areas such as keeping personal information private, protecting online identities and passwords, and never arranging to meet anyone in person who they have only met online. This is also a good place to discuss issues relating to Web 2.0 technologies, such as social networking tools.
	2g: Pupils should be taught to recognise when pressure from others threatens their personal safety and wellbeing, and to develop effective ways of resisting pressures, including knowing when and where to get help.	Building on the comments under 2f (above), this teaching point provides an opportunity to develop pupils' understanding of the risks associated with chat rooms and similar services, where their personal safety or wellbeing might be threatened. Pupils should be taught how to respond if they are contacted in any way which makes them uncomfortable, and where they can turn to for help and advice. This is also a good area in which to discuss the issues relating to, and impact of, cyberbullying.
Developing good relationships and respecting the differences between people	3a: Pupils should be taught about the effects of all types of stereotyping, prejudice, bullying, racism and discrimination, and how to challenge them assertively.	This is a good area in which to introduce issues relating to cyberbullying, such as by mobile phone or in chat rooms and social networking services. 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.
	3j: Pupils should be taught to resist pressure to do wrong, to recognise when others need help and how to support them.	Pupils should be aware of peer pressure in chat rooms, for example to bully others, or other forms of inappropriate behaviour using new technologies, and develop strategies for protecting themselves. This teaching point could also be used to discuss issues relating to copyright and intellectual property relating to materials available on the internet, possibly within the context of plagiarism or illegal file-sharing networks. Pupils should also be aware of the many organisations that exist to help make the internet a safe place for all.
	3k: Pupils should be taught to communicate confidently with their peers and adults.	This is a good area in which to discuss e-safety issues relating to email, chat rooms and other 'direct contact' communications services.

Key Stage 4 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	1b: Pupils should be taught to be discriminating in their use of information sources and ICT tools.	This aspect gives opportunities for teaching pupils digital literacy skills, including how to search effectively on the web, and the importance of critically evaluating any materials they find.
Reviewing, modifying and evaluating work as it progresses	4b: Pupils should be taught to reflect critically on the impact of ICT on their own and others' lives, considering the social, economic, political, legal, ethical and moral issues (for example: changes to working practices; the economic impact of e-commerce; and the implications of personal information gathered, held and exchanged using ICT).	There are opportunities here for discussing a number of e-safety issues. Pupils should be aware of potential legal consequences of their activities on the internet. They should be aware of the relevant legislation, such as copyright and intellectual property law in terms of plagiarism of coursework or downloading music files from illegal file-sharing networks. The Computer Misuse Act (which prohibits unauthorised access to or modification of computer materials, such as through hacking) could also be discussed, along with data protection legislation which protects personal information. Young people should also be aware of the commercial implications of using the internet, and of related risks, including online fraud or 'phishing' scams (sending emails designed to fool recipients into divulging personal financial data).
	4c: Pupils should be taught to use their initiative to find out about and exploit the potential of more advanced or new ICT tools and information sources (for example, new sites on the internet, or new or upgraded application software).	Technology is developing at such a rate that it is impossible to keep pace with all the potential issues in a publication such as this. There is an opportunity, however, to alert pupils to the need to critically evaluate any new technology they encounter in terms of potential risks to their personal safety. Pupils should be encouraged to adopt safe and responsible behaviours regardless of the technology they are using.
Breadth of study	6: Pupils should be taught to be independent, responsible, effective and reflective in their selection, development and use of information sources and ICT tools to support their work, including their application in other areas of their study and in other contexts (for example, work experience or community activity).	As with 1b (above), this aspect gives opportunities for teaching pupils digital literacy skills. Pupils should have confidence in their ability to use the internet and related technologies safely and responsibly, but also know that help and advice is available if needed.

Key Stage 4 citizenship programme of study

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Knowledge and understanding about becoming informed citizens	1a: Pupils should be taught about the legal and human rights and responsibilities underpinning society and how they relate to citizens, including the role and operation of the criminal and civil justice systems.	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.
	1g: Pupils should be taught about the importance of a free press and the media's role in society, including the internet, in providing information and affecting opinion.	While pupils should be aware of the role of the internet in providing a free voice to anyone wanting to publish materials, they should also consider the reliability and appropriateness of such materials. Pupils should be aware of bias and context in the materials they find and should learn to critically evaluate them.
Developing skills of enquiry and communication	2a: Pupils should be taught to research a topical political, spiritual, moral, social or cultural issue, problem or event by analysing information from different sources, including ICT-based sources, showing an awareness of the use and abuse of statistics.	As with the Key Stage 3 programme of study, when looking at internet-based resources, pupils should be encouraged to consider their appropriateness. Pupils should be aware that they might encounter inappropriate content on the internet which may contain extreme political or social views and may be biased in opinion. Again, pupils should be taught to critically evaluate any material they find.
Developing skills of participation and responsible action	3c: Pupils should be taught to reflect on the process of participating.	This teaching point provides a good opportunity to discuss the issues relating to communicating using ICT. The safety issues of using email, chat rooms, instant messaging and text messaging can be discussed, alongside the problems of cyberbullying which are often associated with these forms of technology. This is also a good place to discuss issues relating to Web 2.0 technologies, such as social networking tools. Pupils should also be aware of the immediacy and permanency of any communications they make using ICT, and should learn the importance of protecting their personal information and that of others.

Key Stage 4 PSHE programme of study (non-statutory)

General area of knowledge, skill or understanding	Specific teaching point from the programme of study	Relevance to e-safety issues
Developing confidence and responsibility and making the most of their abilities	1b: Pupils should be taught to have a sense of their own identity and present themselves confidently in a range of situations.	This is a good place to discuss the rights of pupils to protect their personal information. Pupils should be taught to look for privacy statements and opt-out clauses when registering for services online, and be encouraged to use these.
	1d: Pupils should be taught to recognise influences, pressures and sources of help and respond to them appropriately.	Pupils should be aware of the impact of cyberbullying in its numerous forms, and be aware of sources of help and advice. They should recognise that peer pressure can also exist online, for example in chat rooms. Pupils should also be aware of the many organisations that exist to help make the internet a safe place for all.
Developing a healthy, safer lifestyle	2b: Pupils should be taught to use assertiveness skills to resist unhelpful pressure.	As 1d (above), pupils should be encouraged to develop strategies for dealing with peer pressure or bullying online, and should be confident in their ability to seek additional help if needed.
Developing good relationships and respecting the differences between people	3b: Pupils should be taught to be aware of exploitation in relationships.	Pupils should understand the need to be cautious when developing relationships online, and should never be coerced into activities which make them feel uncomfortable. It may be particularly relevant to raise safety issues relating to chat rooms and grooming here.
	3c: Pupils should be taught to challenge offending behaviour, prejudice, bullying, racism and discrimination assertively, and take the initiative in giving and receiving support.	Pupils should be aware of the existence of offensive material and views on the internet, and should know the appropriate behaviours to adopt if they, or others, encounter it. They should also develop an awareness of the many organisations which exist to minimise the amount of offending and illegal content on the internet.

9 Embedding e-safety messages into the ICT Key Stage 3 National Strategy

In addition to embedding e-safety into the curriculum, there are a number of points within the ICT Key Stage 3 National Strategy where it is also appropriate to teach e-safety issues. These are briefly highlighted below.

The full strategy can be found on the Standards Site [**http://www.standards.dfes.gov.uk/keystage3**].

ICT Key Stage 3 National Strategy – Year 7

Teaching objective and area	Specific teaching point	Relevance to e-safety issues
Finding things out		
Using data and information sources	Identify the purpose of an information source (eg to present facts or opinion, to advertise, publicise or entertain) and whether it is likely to be biased. Understand how someone using an information source could be misled by missing or inaccurate information.	These teaching points all relate the development of digital literacy skills, such as effective searching on the internet and critical evaluation of materials found. Pupils should be aware of tone, bias and context in the materials they find online, and should be aware that some web publishers deliberately aim to mislead users.
Searching and selecting	Search a variety of sources for information relevant to task (eg using indexes, search techniques, navigational structures and engines).	
Exchanging and sharing information		
Fitness for purpose	Recognise common forms and conventions used in communications and how these address audience needs (eg columns of text in newspapers, graphics and enlarged print in posters, hyperlinks on websites). Apply understanding of common forms and conventions to own ICT work. Use given criteria to evaluate the effectiveness of own and others' publications and presentations.	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. This is also a good place to discuss issues relating to Web 2.0 technologies, such as social networking tools. The notion of appropriate writing conventions for electronic communications could also be introduced here. Pupils should be taught to critically evaluate materials found online.
Communicating	Use email securely and efficiently for short messages and supporting materials. Know how to protect personal details and why this is important.	As with 'fitness for purpose' (above), the notion of appropriate writing conventions for electronic communications could be reinforced here. Pupils should also be aware of the immediacy and permanency of any communications they make using ICT, and should learn the importance of protecting their personal information and that of others. Issues relating to Web 2.0 could also be discussed here.

ICT Key Stage 3 National Strategy – Year 8

Teaching objective and area	Specific teaching point	Relevance to e-safety issues
Finding things out		
Using data and information sources	Understand how the content and style of an information source affects its suitability for particular purposes, by considering: • its mix of fact, opinion and material designed to advertise, publicise or entertain • the viewpoint it offers • the clarity, accessibility and plausibility of the material.	Pupils should be aware of tone, bias and context in the materials they find online, and should be aware that some web publishers deliberately aim to mislead users. Pupils should be taught digital literacy skills, learning to critically evaluate any information they find, and should consider any copyright restrictions on its further use.
Searching and selecting	Extend and refine search methods to be more efficient (eg using synonyms and AND, OR, NOT).	Again, digital literacy skills are important here. Pupils should be taught to search effectively using online tools within the context of e-safety issues such as using 'safe' search engines and filtering tools.
Organising and investigating	Understand potential misuse of personal data.	Pupils should learn the importance of protecting their personal information and that of others, and be aware of issues such as identity theft and online fraud.
Exchanging and sharing information		
Fitness for purpose	Devise criteria to evaluate the effectiveness of own and others' publications and presentations, and use the criteria to make refinements.	Pupils should be taught to critically evaluate materials found online.
Communicating	Understand some of the technical issues involved in efficient electronic communications	Pupils should be aware of viruses and measures they can take to prevent their machines from becoming infected.

ICT Key Stage 3 National Strategy – Year 9

Teaching objective and area	Specific teaching point	Relevance to e-safety issues
Finding things out		
Using data and information sources	Select information sources and data systematically for an identified purpose by: • judging the reliability of the information sources • identifying possible bias due to sampling methods • collecting valid, accurate data efficiently • recognising potential misuse of collected data.	Pupils should be aware of tone, bias and context in the materials they find online, and should be aware that some web publishers deliberately aim to mislead users. Pupils should develop effective digital literacy skills, learning to critically evaluate any information they find, and should consider any copyright restrictions on its further use.
Exchanging and sharing information		
Communicating	Understand the advantages, dangers and moral issues in using ICT to manipulate and present information to large unknown audiences (eg issues of ownership, quality control, exclusions, and impact on particular communities).	This is a good place to consider many of the legal issues of using the internet, such as copyright and intellectual property legislation, the Computer Misuse Act (relating to hacking and unauthorised access to computing facilities, both hardware and software), and data protection issues. There is also the issue of accuracy and reliability of content on the web. This is also a good place to discuss issues relating to Web 2.0 technologies, such as social networking tools. The more risky aspects of communicating over the internet, such as grooming within chat rooms, should also be considered.

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 young people and their parents to learn together, and e-safety is an excellent topic for encouraging home–school links.

Additionally, schemes such as Computers for Pupils,[30] which aim to put computers into the homes of disadvantaged secondary children to help improve their education and life skills and benefit the whole family, will place even greater importance on schools sharing e-safety information and guidance with parents to raise general awareness and achieve consistency between safety guidelines in the home and the school.

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 get the most out of the internet and mobile phones for themselves and their children. It is currently available to parents through schools. The CD-ROM contains videos of experts giving safety advice as well as an interactive section to help families create and print internet use agreements. It also contains activities that parents can do with their children to prompt discussions about safe use of ICT. Sections of the CD-ROM are in Bengali and Urdu. Schools can order sample copies from the Childnet website [**http://www.childnet-int.org/kia**].

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**].

[30] See Teachernet website [**http://www.teachernet.gov.uk/computersforpupils**].

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 33 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:[31]

- 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.

[31] 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 practitioners develop their awareness of e-safety issues. These include:

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

The Child Exploitation and Online Protection (CEOP) Centre offers the interactive Thinkuknow programme and training to teachers and educational professionals. This describes online issues, outlines necessary child protection information and includes training on how to deliver the CEOP presentation.

Children and the Net
[**http://www.nspcc.org.uk/Inform/TrainingAndConsultancy/Training/TrainingPacks/ChildrenAndTheNet_ifega42365.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 secondary schools – ICT
[**http://www.tda.gov.uk/partners/supportstafftraining/inductionmaterial/induction_ta_secondary.aspx**]

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 mailing list

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 below). 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.

Safetynet

[**http://lists.becta.org.uk/mailman/listinfo/safetynet**]

Safetynet is a mailing list specifically for anyone who wants to discuss and share information to support the development of e-safety good practice within educational organisations. This forum is for teachers 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.

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 1 and 2

Signposts to a selection of resources to help teachers of Key Stages 1 and 2 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**].

Millburn Hill Road
Science Park
Coventry CV4 7JJ
Tel: 024 7641 6994
Fax: 024 7641 1418
Email: becta@becta.org.uk
URL: http://www.becta.org.uk

03/DD06-07/098/BX/4k