

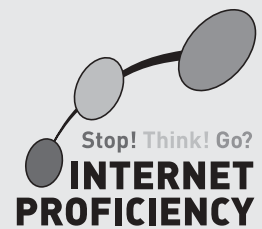
Teachers' Guide



Introduction

- | | | |
|----------|--|-----------|
| 1 | The Internet Proficiency Scheme | 3 |
| | Why have an Internet Proficiency Scheme? How to use this pack Involving parents | |
| 2 | Implementing the Internet Proficiency Scheme | 7 |
| | Profiling pupils | |
| 3 | The benefits and risks of new technologies | 11 |
| | Learning benefits from using ICT The risks Strategies for keeping children safe The future | |
| 4 | Understanding the technologies | 16 |
| | The Internet E-mail Chat Instant messaging SMS MMS | |
| | Lesson plans using the technologies | 31 |
| | Lesson 1 – Using technology to communicate Lesson 2 – Introducing the Cybercafé web site Lesson 3 – Communication and information Lesson 4 – Using e-mail safely Lesson 5 – Responsible use of the Internet Lesson 6 – Chatting with care Lesson 7 – Using text and picture messaging Lesson 8 - Behaving responsibly Extension/refresher activities | |

Introduction



The Internet Proficiency Scheme is designed to help Key Stage 2 pupils learn how to use the Internet and other technologies safely and responsibly.

The aims of the scheme are to:

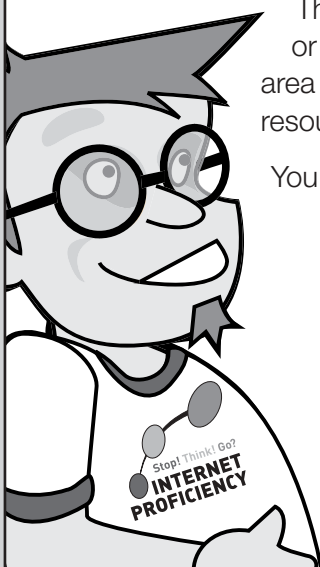
- develop a set of 'safe and discriminating behaviours' for pupils to adopt when using the Internet and other technologies
- provide teachers with easily accessible support materials to help develop safe and discriminating behaviours when pupils are using the Internet and other technologies
- offer pupils a set of activities that allow them to demonstrate what they know and understand about using communication technologies
- ensure that the safe and discriminating behaviours will be directly related to the skills, knowledge and understanding as set out in the National Curriculum and schemes of work for ICT and Citizenship, and the guidance for PSHE at Key Stage 2
- support teachers' own professional development through the information and guidance contained within this pack.

The scheme consists of this teacher's pack and a supporting web site. The pack contains important information for implementing the Internet Proficiency Scheme, including methods of working and integration with the curriculum. You will need to familiarise yourself with much of the teacher's notes before embarking on the lesson plans and activities.

Cybercafé, the accompanying web site (<http://www.gridclub.com/cybercafe>), allows pupils to demonstrate what they have learnt about safe and discriminating behaviours in an interactive and supportive environment. The site also contains an on-line audit of pupils' Internet proficiency skills, which will help you to group pupils according to their ICT experience.

The Cybercafé materials can be used as a whole-class teaching resource or as an ICT activity at school or in the home. There is also a teachers' area of the Cybercafé web site, which provides additional advice and resources for teachers (<http://www.Gridclub.com/cybercafe/teachers>).

You can find details on how to use the pack on page 5.



1 – The Internet Proficiency Scheme

Why have an Internet Proficiency Scheme?

The Internet and other digital information technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. However, alongside the new technologies is a need for new skills to be learnt and applied in the classroom and beyond. While these technologies can have a positive effect, pupils need to be taught about their appropriate and effective use.

Government investment in Information and Communications Technology (ICT) from 1998 to 2002 has been £1,835 million for primary, secondary and special schools for teaching, learning and administration. The ratios of computers to pupils have been increasing year on year since 1998: in 1998, there was one computer for every 17.6 primary pupils, now there is one for 9.7¹.

This huge investment reflects the need for ICT to be embedded into teaching and learning. However, the Internet is by nature 'open'. Open to all, at all times, unregulated and unpoliced. This is an attractive prospect, especially for educationalists who are able to allow pupils to research, explore and create. Unfortunately, this attractive prospect exists also for those wanting to take advantage of young and vulnerable people.

Schools are relatively 'safe areas' for pupils to use ICT. They are likely to have filtering and/or monitoring software, an acceptable use policy that teachers, pupils and parents sign up to, classroom supervision, a firewall and perhaps even a 'walled garden' of web sites that pupils can access. In contrast, pupils' access to the Internet at home may be lacking in all these safety mechanisms. At most, there may be some sort of filtering product that is offered by an Internet Service Provider (ISP) or software developer. If the role of school is to prepare young people for the wider world, then schools ought to be teaching them how to behave safely and appropriately on line – wherever they may be.

The pace of technological change – in schools as elsewhere – has been so fast that there is little material available for teachers to use in the classroom to teach pupils how to employ safe and discriminating behaviours when using the Internet and other technologies. The Department for Education and Skills (DfES) and Becta have been providing advice to schools through the Superhighway Safety pack and web site since 1998 (<http://safety.ngfl.gov.uk/schools>). This pack and the Internet Proficiency Scheme aim to support teachers in this area, by providing practical advice on the teaching and learning of Internet safety in the classroom for Key Stage 2 pupils.

¹DfES Statistics of Education: *Survey of Information and Communications Technology in Schools, 2002* (<http://www.dfes.gov.uk/statistics/DB/SBU/b0360/sb07-2002.pdf>)

How to use this pack

The pack comprises background information for teachers, lesson plans with supporting materials, worksheets for pupils, certificates for schools and pupils, and details of the Cybercafé web site (<http://www.gridclub.com/cybercafe>). The activities are intended to be carried out alongside those on the Cybercafé web site.

While the Scheme is designed to be taught at Key Stage 2, the activities are particularly suitable for pupils aged 9 to 11. Pupils in this age group will be more familiar with the technologies and will have greater awareness of, and ability to debate, the issues.

The scheme is taught using a variety of methods including whole class teaching, pairs, small group and plenary sessions. Before commencing the scheme, it is worth while profiling pupils to determine their level of ICT experience, their exposure to Internet safety advice, and their level of engagement in on-line behaviour which could be deemed 'risky'. This profiling exercise is key to the success of the scheme, and further details and resources are included in Section 2.

Pupils are encouraged to talk about the issues raised by the Scheme, and findings are recorded for whole-class discussion. Once all the activities have been completed the pupils have the opportunity to demonstrate their learning through an on-line quiz and an end-of-unit task. Once pupils have completed the classroom activities, interactive on-line activities and the on-line quiz, they should be awarded a certificate. A photocopy master of this is contained in the pack.

Internet safety should not be seen as an exclusive ICT issue. The pack suggests that you may want to tie this in with other areas of the curriculum, namely Citizenship and PSHE. Children should be taught that how they behave in the 'on-line' world should be the same as the 'off-line' world. Therefore teaching this issue across subjects can reinforce this message.

The Internet Proficiency Scheme was piloted in schools during the summer of 2002, and teachers used the materials in a variety of ways. Colette Cotton, of St Mary's CE Primary School, Folkestone, introduced Internet safety lessons in different ways depending on the age of the pupils. She sometimes discussed issues with them before going into the computer suite. Other times, she would use one computer in the suite to demonstrate a particular web site to the pupils, so that they could see what they would be doing as part of the lesson. Her groups concentrated on Internet safety for two sessions per week. Colette linked this work to PSHE, but had she been using the scheme over an academic year, she would have linked it to other parts of the curriculum as well. "I would plan it in with the general timetable for the year. I might use some of the activities in PSHE, and others in the ICT lesson."

Karl Hopwood, of Greystoke School in Cumbria linked Internet safety issues to activities going on in the school, such as police visits to talk to children on the subject of 'stranger danger'. He also introduced Internet safety as part of the topic of communications and conversations in literacy. In Four Elms Primary School, June Cooke taught 26 Year 5 and Year 6 pupils about Internet safety as part of a special curriculum week. "We did a little bit every day. We worked on the Cybercafé web site throughout the day, and occasionally through lunchtime, with pupils taking it in turns to work individually on the computer". June taught Internet safety as well as the units of work for drug and sex education, citizenship and PSHE: "I could also fit it in with the literacy hour, as part of speaking and listening, and the drama workshop."

1 – The Internet Proficiency Scheme

Involving parents

It is important that the 'safe and discriminating behaviours' taught as part of this scheme are adopted by pupils whenever they are using the Internet and other technologies, not just in the school environment. Parental involvement can help reinforce the messages of this scheme, and extend the learning process into the home environment.

In addition to individual pupil certificates, a school certificate is also enclosed in the pack. This is to demonstrate to parents and others that the school is involved in the scheme. You may also want to make parents aware that your school is participating in the scheme by making reference to it in the schools' parental Internet permission form or by mentioning it in your school's Acceptable Internet Use Policy.

Additionally, the teachers' area of the Cybercafé web site (<http://www.gridclub.com/cybercafe/teachers>) provides a presentation that outlines the issues associated with ICT use and highlights how they are tackled through the Internet Proficiency Scheme. Schools may wish to present this at a parents' evening or hold a specific event on ICT awareness.

Involving parents was seen as essential in the pilot schools. Most schools wrote a letter to parents to let them know about the Internet Proficiency scheme. For example, Colette Cotton says, "I asked the children what they would do if they saw something on the Internet at home. They said they would tell their parents, but would parents necessarily know what to do? You've got to make parents aware of the need to have filtered sites at home, because I'm quite sure that many parents are not aware of the problems."

In some respects, the pupils who need to develop awareness of safe practice with the technologies are more aware of the possible dangers than their parents. Taking part in the scheme will not only reinforce their awareness but also help them to develop safety-conscious behaviours. As one of the pilot school teachers remarked, "The Internet Proficiency Scheme has had a huge impact on pupils, as we hadn't broached the subject before.

Pupils are now discussing safety with their teachers, who encourage them in that discussion without being judgemental."

2 – Implementing the Internet Proficiency Scheme



The QCA Schemes of Work for ICT include two units which use some of the technologies. These are Unit 3E – E-mail, and Unit 6D – Using the Internet for Research. These units provide a useful starting point for implementation of the scheme and it is suggested that pupils have had opportunities to use these technologies before they start the IP scheme.

There are eight lessons in this scheme plus extension or refresher activities. The first three lessons focus on generic safety messages which can be applied across the technologies. Lessons 4 to 7 are focused on individual technologies and the issues relating to their use. Lesson 8 seeks to pull together what pupils have learnt and draws out the types of behaviours that could be adopted.

You may feel that, through constraints of time, pupils will not be able to complete the whole proficiency scheme. In this case, you may well select lessons which cover those technologies which pupils are most likely to use, or with which they may be most at risk. It's important, however, to be aware that although pupils' access to certain technologies may be limited at school, they may have unlimited access in the home. An audit of Internet safety practices in schools, for example, which was conducted in June 2002 by Loughborough University, showed that only 5 per cent of schools allowed the use of on-line chat – but recent statistics show that 1 in 10 children between the ages of 7 and 12 use on-line chat elsewhere. While parents and carers naturally have responsibility for how children access technologies at home, you may feel that it is important for schools to address these issues too, so that children learn safe behaviours in all environments.

Profiling pupils

During the pilot phase of this scheme, three groups of pupils were identified. These groups were based upon the level of ICT experience of pupils, their exposure to Internet safety advice and the degree to which they engaged in 'risky' on-line behaviour. Depending on the type of communication being studied or used, pupils could be assigned to different groups. For example, pupils with a high level of experience in using the Internet and risky behaviours may be less experienced and adventurous when confronted with a chat situation.

Children generally fall into one of three broad categories:

Group A: Those with low levels of experience of using the Internet, low levels of prior exposure to Internet safety advice, and poor ICT skills. This group of children generally require guided learning.

Group B: Those with moderate levels of experience of using the Internet, moderate levels of prior

exposure to Internet safety advice, and moderate ICT skills. This group of children can be considered as having a moderate skill and knowledge base.

Group C: Children with high levels of experience of using the Internet, high levels of prior exposure to Internet safety advice, and good ICT skills. This group of children generally has a good skill and knowledge base.

During the pilot phase of these materials, it was found that to derive maximum benefit:

- **Group A** pupils need the teacher to model the experiences and activities and provide appropriate prompts
- **Group B** pupils benefit most from resource-based learning to help them to develop information literacy skills and independent learning skills
- **Group C** pupils need to develop their abilities to reflect and apply their thinking to new situations.

2 – Implementing the Internet Proficiency Scheme

The lesson plans in this scheme try to build on these suggestions and lessons have been differentiated into groups A, B and C.

To help group the children into the above categories, we have developed an on-line auditing tool on the teachers' area of the Cybercafé web site. This asks pupils a series of simple questions which are submitted to the site and the teacher receives a list of pupils grouped into either A, B or C. We strongly recommend that you make use of the on-line audit, as it will help pupils to get the best out of the scheme.

If you are unable to make use of the auditing tool, then Group A children can generally be viewed as those at the lower end of the spectrum, who may need additional support from teachers, classroom assistants or other pupils. Group B children are the 'middle band' and these children will probably make up the majority of the class. Group C children are at the top end of the spectrum and could be used to support pupils who are in Group A. It is important to remember that these groupings are in relation to the three areas outlined above and may not reflect academic achievement in other areas or subjects.

Some pupils will have little or no experience of using some of the technologies. If this is the case, these pupils will need opportunities to have some hands-on experience if they are to understand and gain benefit from this scheme.

Resources

There are a range of resources which can be used in the lessons. Prompt sheets and pupils' worksheets are included as photocopiable print-outs in this pack, and can also be downloaded from the teachers' area of the Cybercafé site (<http://www.gridclub.com/cybercafe/teachers>). In either case, you may wish to modify the examples provided to suit your own pupils.

Presentations which can be used to deliver the lessons, can also be downloaded from the teachers' area of the Cybercafé site.

Methods of working

The scheme is designed to be taught using a variety of working methods, and these are highlighted in the lesson plans. Most lessons begin with whole-class sessions, followed by pupils working in pairs or small groups. Group discussions in plenary sessions are encouraged to allow pupils to feed back their findings, talk about their experiences and decide collectively on safe and appropriate behaviours. Exercises can be tailored to fit available resources, and suggestions are made for homework or follow-up activities.

Duration

This scheme can be taught in two ways:

- As a continuous unit throughout Key Stage 2 (or more likely through Years 4, 5 and 6)
- As a discrete unit during Year 5 and/or 6.

You will need to consider which is most appropriate for your particular situation. Other points you may want to consider include the following:

- Pupils in Years 3 and 4 are likely to match 'Group A' characteristics and will therefore need a lot of structured teaching before they can derive maximum benefit from the scheme.
- Cross-curricular contexts where communications technologies could be used might provide opportunities for pupils to develop their ICT experience and capability in meaningful contexts. However, the thrust of this scheme is to develop an awareness and understanding of potential risks and how to develop appropriate strategies and behaviours to deal with risky situations. To try and combine the two aspects, with younger pupils and over an extended period, may undermine the impact in both aspects.
- Pupils in Years 5 and 6 are more likely to have had some experience of using a broader range of communication technologies and should have had some exposure to safety guidance. In addition, some pupils may have experienced some 'risky' situations and be able to share those with peers.

- Conversely, pupils in Years 3 and 4 might not have been exposed to much safety guidance and therefore be more likely to encounter risky situations without the necessary skills to be able to deal with them. Do we, therefore, try and protect pupils before anything happens but in a relatively abstract context where they have had little or no experience with the technologies or the risky situations? Is school the place to expose pupils to risky situations?

If you decide to begin in Years 3 and/or 4, then teaching the scheme as a continuous unit is likely to be most appropriate. If you decide to commence the scheme in either Year 5 or 6, then teaching it as a discrete unit is likely to be more productive.

Teaching as a continuous unit

If cross-curricular contexts are to be used as the starting points for elements of this scheme, a programme such as the one below might be appropriate:

| Year | Autumn | Spring | Summer |
|------|---|--|--|
| 3 | IP Scheme – introduction | Hi – Tudors ICT – Guided Internet research Introduce the Internet element and raise some of the issues | Gg – Weather around the world ICT – e-mail Introduce the e-mail element and raise some of the issues |
| 4 | Gg – Village Settlers Hi – Case studies of invaders ICT – Guided Internet research IP Scheme – study the safety aspects related to using the Internet | | Gg – How and where do we spend our time? ICT – SMS Introduce the SMS element and raise some of the issues |
| 5 | Gg – What's in the News? ICT – Internet research, chat and IM Introduce the chat and IM elements and raise some of the issues | Gg – Contrasting UK locality ICT – e-mail and Internet Research IP Scheme – study the safety aspects related to using e-mail | Tudor Exploration ICT – Internet research Recap on the Internet safety aspects |
| 6 | Gg – What's in the News? ICT – Internet research, Chat and Instant Messaging IP Scheme – study the safety aspects related to using chat and instant messaging | Gg – A sense of place ICT – SMS and MMS Gg – Connecting ourselves to the world ICT – IP Scheme IP Scheme – study the safety aspects related to using SMS and MMS | Gg – Connecting ourselves to the world ICT – IP Scheme IP Scheme – recap on aspects as appropriate |

2 – Implementing the Internet Proficiency Scheme

Teaching as a discrete unit

If a discrete approach is adopted, pupils will have had hands-on experience of most of the technologies by the beginning of the spring term in Year 5. It should therefore be possible to introduce and teach the scheme by the end of Year 5, still allowing opportunities for pupils to reinforce their problem-solving strategies and appropriate behaviours as their range of experiences and expertise is enhanced through Year 6.

Monitoring

Pupils are encouraged to record their findings as they progress through the lessons, and feed these back during group sessions. Once all the activities have been completed, pupils have the opportunity to demonstrate their learning through an on-line quiz and an end-of-unit task.

On completion of the teaching activities, interactive on-line activities and the on-line quiz, pupils will have qualified for a certificate (a photocopy master is contained in this pack, or it may be ordered by e-mail from: internetprof@becta.org.uk).

Learning outcomes and objectives

Each of the lesson plans in Section 5 gives an overview of learning objectives and learning outcomes. Where appropriate, lesson plans are also linked to the National Curriculum Programmes of Study.

3 – The benefits and risks of new technologies



The range of on-line services is growing constantly. Useful information – news, weather reports, sports results, movie reviews, encyclopaedias – and services such as making on-line travel reservations, banking, and shopping are becoming readily accessible. The growth in the numbers of people using technology over the last ten years has been astounding:

- In 200-01, 40–50 per cent of households had a personal computer
- In 2000, around four out of five children surveyed in England, Wales and Northern Ireland had access to a home computer (78 per cent of primary school pupils and 85 per cent of secondary school pupils). Over half were able to access the Internet at home.²
- In 2000-01, 47 per cent of households had at least one mobile phone
- In England, Wales and Northern Ireland in 2000 approximately 20 per cent of children of primary school age and 60 per cent of secondary school pupils owned a mobile phone.³

Future developments in technology are predicted to see a growing convergence between computers and telephones, with Internet access becoming increasingly easy, wherever you are. Education too has seen rapid growth in the use of technology, both in ICT use in the classroom and the availability of teaching and learning materials on line.⁴

Learning benefits from using ICT

Many schools are making use of the technology to dissolve boundaries between the home and the school. Access to school intranets outside school hours and laptop lending schemes help pupils to extend their learning beyond the classroom. By using e-mail, pupils and parents can communicate with teachers outside the traditional school day. ICT has a particular strength for pupils who are unable to attend school on a regular basis. They are able to still feel part of the school environment and retain some continuity.

Research findings suggest that ICT can be beneficial. Becta's *Primary Schools of the Future – Achieving Today*⁵ suggests that ICT is having a positive educational impact. By analysing data from Ofsted reports, Becta found that there is a consistent trend for

pupils in schools with better ICT resources to achieve better grades for English, mathematics and science. Becta also found that at Key Stage 2, schools with 'good' ICT resources deliver better results than schools with 'poor' ICT resources – even when compared with schools of a similar type and taking into account socio-economic circumstances. Becta's research on secondary schools shows similar findings.

The ImpaCT2 study further supports this. A large-scale longitudinal study tracking over 2000 pupils' use of ICT for three years, ImpaCT2 discovered a positive association between individual pupils' use of ICT and their performance in the Key Stage 2 national tests in English and mathematics. Similar positive associations were found between ICT use and national tests for science at Key Stage 3.⁶

² Office for National Statistics, *Social focus in brief: Children 2002* (http://www.statistics.gov.uk/downloads/theme_social/social_focus_in_brief/children/Social_Focus_in_Brief_Children_2002.pdf)

³ Office for National Statistics, *Ownership of mobile phones: by income quintile group, 1996-97 and 2000-01: Social Trends 32* (<http://www.statistics.gov.uk>)

⁴ As footnote 3

⁵ *Primary Schools of the Future – Achieving Today*, Becta, 2001 (<http://www.becta.org.uk/news/reports/primaryfuture/>)

⁶ The full findings from the ImpaCT2 study are available on the research area of the Becta web site (<http://www.becta.org.uk/research/>).

3 – The benefits and risks of new technologies

Apart from the increasing evidence that supports the positive aspects of ICT in education, there is plenty of anecdotal evidence too. For instance, teachers continue to report that pupils of all ages find using ICT to be highly motivating. Sending e-mails and designing web pages provide an audience for pupils which they otherwise would not have. One teacher reported: "They would much rather write an essay for their fellow pupils in our Canadian partner school than they would for me!".

The risks

Unfortunately, alongside the education and social benefits that available through ICT, there are also risks, particularly for young users. As in any other area of life, children are vulnerable, needing adult supervision and the ability to learn sets of safe behaviours. Below is a summary of the kinds of risks that pupils might be exposed to:

- **Exposure to inappropriate material**

One risk is that a child may be exposed to material that is pornographic, hateful or violent in nature or encourages activities that are dangerous or illegal. Schools will provide some sort of protection against this sort of exposure but even the installation of filtering software is not always foolproof and nothing should replace supervision in the classroom. While there is a growing awareness of the dangers to young people of visiting (whether deliberately or by accident) web sites that contain sexually explicit or offensive material, there are other sites that can be equally dangerous. Since the web is open to all, it is attractive to those with extreme political, racist or sexist views. It is natural for children to believe what they read, and the web appears to have as much authority as the

printed word, however undeserved. It's important, therefore, that schools play their part in teaching children to become critical and discriminating users of the web. While this is a challenging area, Lesson 5 offers a framework for helping them to do this.

- **Physical danger**

Although rare, there is a risk that whilst on line, a child might provide information or arrange a meeting that could risk his or her safety or the safety of other family members. This is perhaps the most worrying and extreme risk associated with Internet use.

A criminal minority make use of the Internet, and related services such as chat rooms, to make contact with children with a view to establishing and developing relationships with the sole purpose of persuading them into sexual activity. The techniques used by sex offenders are often known as 'on-line enticement' or 'grooming'.⁷

The relative scale of the risk to children being approached in this way via the Internet is difficult to establish. Evidence from both the United States and the UK provided by actual incidents and supporting research does appear to indicate a growth in criminal activity of this nature over recent years.⁸ In a news story, the BBC report that in the past two years, at least 12 children have been sexually assaulted by people who first contacted them via the internet.⁹ Although their attackers were sent to prison, child protection campaigners say the law needs strengthening. The situation is likely to change under the Sexual Offences Bill, due to be introduced in 2003, which includes a new offence of grooming, based on meeting a child with the intention of committing a sex offence to apply both to the Internet and off line.¹⁰

⁷ Online grooming and UK law: A submission by Childnet International to the Home Office', Childnet International, 2001 (<http://www.childnet-int.org/downloads/online%20grooming.pdf>).

⁸ Chat Wise, Street Wise – children and Internet Chat services. Internet Crime Forum, March 2001 (http://www.internetcrimeforum.org.uk/chatwise_streetwise.html).

⁹ BBC News web site, 16 August 2002 (http://news.bbc.co.uk/1/hi/uk_politics/2196734.stm).

¹⁰ Sexual Offences Bill, Home Office, 2002 (<http://www.sexualoffencesbill.homeoffice.gov.uk/>).

It is important to note, however, that the number of known cases is currently very low in proportion to the rapidly growing rate of Internet use. The danger of children being approached by a stranger on line is thought to be relatively much lower than a child being at risk, off line, from someone known to them.

The concept of danger is a difficult one to establish with young pupils – there is no easy, guaranteed method of identifying an adult who is untrustworthy. Striking the balance between making children aware of potential dangers but at the same time confident enough to express their natural curiosity requires skilled teaching. Teachers will also need to be aware that the activities in Lesson 3 in particular could lead to pupils disclosing personal information, which they will need to address with sensitivity.

- **On-line bullying**

A child might encounter e-mail, chat or text messages that may make him or her feel embarrassed, upset, depressed or afraid. They may not be in any physical danger, but it could affect their self-esteem. Messages from people they can't identify can be particularly frightening. Individuals can receive hoax messages and pupils need to be aware that if they cannot identify who the person is, they should tell an adult.

- **Legal, financial and commercial considerations**

There is also the risk 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 are becoming particular issues which are associated with the Internet especially in relation to the downloading of music or games. Research also shows that children are not able to differentiate between what is advertising and what is not.

- **Inappropriate behaviour**

Pupils may get involved in inappropriate behaviour such as bullying. They should be taught how to behave on line and to avoid being

rude, mean or inconsiderate. Pupils should understand that how they behave in the 'off-line world' is the same as they should behave in the 'on-line world'.

- **Bridging the gap between the home and the school**

Schools are relatively protected areas where pupils are able to access different technologies under human and technological supervision and monitoring. In the home, however, there is likely to be minimal technological protection and parental supervision may not be to the same degree as the supervision operated in a school environment. Schools will operate policies which will allow pupils access to certain types of ICT (they may, for example, allow pupils to access e-mail through their network but not via web mail). However, a pupil may go home and access e-mail through the Internet. Therefore it is important that even if schools do not allow the use of a particular technology in school, they still teach pupils how to behave sensibly and appropriately when using it, and educate them about the particular risks associated with it.

Strategies for keeping children safe

The over-arching aim of these materials is to help children to develop patterns of behaviour that will protect them from the risks of certain technologies, and to provide them with strategies for dealing with anti-social behaviour (bullying via text messages, for example).

Given that different technologies may involve different risks, there are some complex messages for younger pupils to assimilate. There are some general rules, however, and these are presented in a simpler, more memorable message as 'SMARTthinking'. Based on the SMART mnemonic developed by Childnet, the SMARTthinking rules are reinforced throughout these materials. It may be helpful to display the colour version of the rules so pupils become familiar with it; a shorter version is also printed on the Pupil Passports contained in this pack.

3 – The benefits and risks of new technologies

The future

The future undoubtedly holds a great deal of promise in terms of technological developments, bringing great benefits and offering new opportunities for education, entertainment and social interaction. Increased integration of technologies will make communication even easier – we will be able to send messages from mobile phones to e-mail accounts and vice versa, picture messaging may become commonplace, and the physical and geographic constraints of using technologies will diminish.

However, with these developments and benefits will also come increased risks. The ease of access to electronic communications, especially to young people, will become more difficult to control, and filtering and monitoring systems will become more complex to implement. Those individuals or organisations with ulterior, untrustworthy or unlawful motives are likely to encompass the multimedia benefits of these technologies for their own personal gain, and ultimately there is a fear that young people will more readily be at risk of exposure to inappropriate materials, content and contact.

Although over time it is likely that technical solutions will be found to minimise some of the risks associated with new technologies, as with filtering systems and similar solutions today, these can never be guaranteed to be absolutely infallible. It is important, therefore, that children are taught, and continue to learn, safe and responsible behaviours to protect them when using any technology, and become discriminating users of the wealth of technology available to them both now and in the future.

SMARTthinking

S

= **Secret**

This is about personal information and whether it is safe to give it out. For example, it might apply to an on-line registration form or someone requesting contact details so they can send you a prize.

STOP and THINK

WHO wants the information?

WHY are they asking for it?

WHAT will they do with it?

M

= **Meeting**

This is about someone you have never met before contacting you on-line or through a messaging service to invite you to a meeting.

STOP and THINK

WHY should you **never** arrange to meet anyone you have only met on-line?

WHAT might happen?

WHO should you tell?

A

= **Attachments**

This is about e-mail and attachments and what you need to think about before opening them.

STOP and THINK

WHO sent it?

WILL it be safe to open it?

WHAT can I do to protect myself and the computer?

R

= **Reliable**

Anyone can put anything on the Internet and anyone can use the communication technologies (such as chat, SMS, e-mail, IM) to contact others.

STOP and THINK

WHETHER I can rely on information on web sites to be true

WHETHER I can rely on someone I can't see telling me the truth

WHAT can I do to check?

T

= **Tell**

No matter how careful we are, sometimes we might come across things that upset us.

STOP and THINK

WHAT can I do when web sites and messages make me feel uncomfortable?

WHO can I tell?

WHAT can I do to stop it happening again?

STOP! THINK! ... GO?

4 – Understanding the technologies

This section highlights the different technologies, how they work and the particular benefits and risks associated with them. Most of the risks that materialise from the use of various technologies are not new and if pupils can be taught to behave sensibly and appropriately, many risks can be eliminated.

The Internet

The Internet is a worldwide system of computer networks, in which users at any one computer can, if they have permission, get access to information made available on other computers.

The Internet enables users to obtain information and resources, to communicate with each other and to publish information. The World Wide Web (WWW) or Web provides easy access to the vast quantity of information and resources available on the Internet and is the facility which people use to 'surf' for information. It is made up of millions of screens, or 'pages', of information. The collection of pages created by one individual or organisation is known as a web site. Each page can include text, images, sound, animation and video and has its own unique address. Any individual or organisation can create and publish a web site. Most Internet Service Providers (ISPs) offer free web space to their subscribers.

To access information on the Internet, you need to use a web browser such as Netscape or Internet Explorer. This allows you to move around web pages just by clicking on words and graphics which are linked to other pages. Sometimes these links will take you to someone else's web site.

Web pages have a unique address or Uniform Resource Locator (URL). For example, if you wanted to go to the DfES web site you would need to type <http://www.dfes.gov.uk> in the address bar of your web browser.

The amount of information available on the web is so vast that it can be daunting, especially when searching for specific facts. To help sift through this huge array of information there are search engines which make it much easier to find what is required.

What are the benefits?

The Internet enables access to a vast range of cultural, scientific and intellectual material which might otherwise not be freely or readily available. It extends the school's resources far beyond the school walls, to museums, galleries, organisations of every kind and displays many of them interactively, so pupils can see how things work. The Internet provides a powerful resource for learning as well as an efficient means of communication.

What are the risks?

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

There is also the question of reliability, credibility and validity of information on some web sites. In a school setting, teachers will also want to check the educational value of a web site, and pupils should be taught to evaluate the material they find.

If children or schools are involved in publishing web pages, there is a risk that personal information about individual pupils is published. Schools need to exercise caution when deciding what information should appear on their web site.

An overview of the Internet as a communication tool is given in Lesson 1; pupils also have an opportunity to explore web browsing, via the Cybercafé web site, in Lesson 2. Lesson 5 tackles the issues in more depth and helps pupils to question what they see and read on web sites.

Avoiding the dangers

General information on safe use of the Internet is available on the Superhighway Safety web site (<http://safety.ngfl.gov.uk/>). There are also some specific issues to consider.

Acceptable use policies (AUPs)

As part of their responsibility for ensuring safe access to the Internet, schools should develop an Acceptable Use Policy. This provides a framework for safe and responsible use of the Internet in school, and guidance for pupils and parents for use of the Internet at home. It will typically outline safe and responsible behaviours for pupils, procedures for reporting unsuitable material, and information on protecting the computer network from viruses.

Acceptable use policies, and pupils' understanding of them, are covered in Lesson 2 of the Internet Proficiency Scheme. Information on acceptable use policies is also available on the Superhighway Safety web site (<http://safety.ngfl.gov.uk/schools/document.php3?D=d39>). The ICT Advice also site provides further guidance and resources for developing an Acceptable Use Policy (<http://ictadvice.org.uk>).

Evaluating web materials

While there is plenty of reliable information on the Web, there is also plenty that is incorrect, out of date and/or seriously biased. Equally, not all educational materials are appropriate for pupils because they are written with adult readers in mind. The evaluation of web resources is therefore necessary to determine the reliability, accuracy and currency of the material, and pupils should be taught the value of this process as part of their core ICT skills development.

When evaluating web materials, pupils might ask themselves:

- Do the headings look relevant for what they need to find?
- Does the content seem up to date?
- Where does the content originate from?
- Is the content easy to read and understand?
- Does it provide everything they need?
- Are the links useful?
- Does it present a one-sided point of view?

The ICT Advice site also provides guidance on evaluating web sites, including some key considerations for teachers, in the 'How to' section.

Evaluating web sites is covered in Lesson 5 of this Scheme, and additional resources are available in the teachers' area of the Cybercafé web site (<http://www.gridclub.com/cybercafe/teachers>).

Internet filtering

Most educational ISPs provide a filtered Internet service. This can help prevent access to undesirable content. Additional filtering software can be used in school or at home to supplement this service.

The Becta Accreditation of NGfL Internet Service Providers enables schools and other educational establishments to make an informed choice of ISP. The standards for assessment have been developed in consultation with partners in education and industry to ensure reliable and relevant information is provided. Through the accreditation process, there is a technical assessment of filtering services provided by ISPs for factors such as browsing of web-based content, web-based e-mail servers, and level of restrictions, for example, a walled garden approach. Assessments of service options such as the ability to filter by age appropriateness and the flexibility to offer site-specific services are also made. Further information is available on the Becta Accredited ISPs web site (<http://ispsafety.ngfl.gov.uk/>).

Further guidelines for Internet filtering are available on the Superhighway Safety web site, and the ICT Advice site also provides a range of guidance on Internet filtering.

Internet search tools

The Web offers users a vast quantity of information, in a wide range of formats. However, having such an extensive resource can also be a major drawback, and locating information quickly and effectively may require the use of a variety of search tools and techniques.

Internet search tools provide a mechanism to search the information available on the Internet. They operate using a keyword search or by a directory structure, with content organised by predefined categories.

4 – Understanding the technologies

Searching the Internet successfully requires careful planning and definition of the exact information needs, and pupils should be taught the benefits of doing this before going on line as part of their core ICT skills development. Whilst typing a keyword or phrase into a search engine will quickly provide a number of links to sites that contain those words, unfortunately the sheer volume of links is often unworkable.

Most search engines now offer advanced searching techniques which allow the user to define their searches more precisely. Although search commands may vary from one search engine to another, the concepts remain the same, and hence the skills acquired are transferable. Many search engines will rank results, placing priority on the first search term, and some search engines may also allow searches to be confined to UK sites only. Common words such as 'of' or 'the' aren't normally recognised for the purposes of the search. However, there will still be occasions when no amount of refining will result in a manageable number of links. In this case, in order to save time, you can probably assume that the first few sites listed will provide the most useful information.

As an alternative to keyword searching, a menu-based search provides a method of finding specific information by gradually narrowing down through predefined categories. The search engine will divide the information on the Web into topic areas, starting with very general topic menus, which are gradually refined through the choices of the user until the relevant information is reached. A menu-based search can provide a structured method of searching the Internet, but will only return results of those sites classified by the search engine provider.

Many search engines will also provide filtering facilities to remove unsuitable sites and advertising from search results. Additionally, there are a number of child-friendly and family-friendly search engines available. Search Engine Watch (<http://www.searchenginewatch.com/links/kids.html>) provides tips and information about searching the web, along with a comprehensive listing of search engines for children. It lists services which are

designed primarily to serve the needs of children, either in focus, or by filtering out sites that some teachers and parents might find inappropriate.

Here are a few examples of child-friendly search tools:

- Ask Jeeves for Kids
Designed to be a fun destination site focused on learning and 'edutainment', which searches using natural language. The service combines editorial judgment with filtering technology to enable children to find both relevant and appropriate answers on the Web. (<http://www.ajkids.com>)
- Family friendly search
Searches Yahoo!igans, AOL Kids, Kids Click and Saluki Search from a single search screen. (<http://www.familyfriendlysearch.com/>)
- Mirago Zone
Uses content filters to provide a special 'family friendly' area where search results are filtered for offensive content. It also provides a 'preference' facility for the user to set their own filtering requirements. (<http://zone.mirago.co.uk>)
- Yahoo!igans
A version of Yahoo, designed specifically for children aged 7 to 12. (<http://www.yahoo!igans.com>)

Further information on effective search techniques is available on the ICT Advice site in 'How to find information on the web'.

Customising web browsers

Most web browsers provide some customisation facilities to allow security, privacy and content settings to be adjusted. The ICT Advice site provides information on how to do this.

Publishing web sites

Many schools are developing their own web site to provide information for pupils and parents, showcase pupils' work and promote the school within the wider community. It is essential that schools protect the identity of their pupils by not publishing personal information, names, e-mail addresses or photographs of individual children.

Guidelines for developing school web sites are available on the Superhighway Safety web site (<http://safety.ngfl.gov.uk/schools/document.php3?D=d27>). The ICT Advice site also provides guidance on publishing web sites.

The importance of keeping personal information private is covered in Lesson 3 of the Scheme.

When children find inappropriate material

When children are using the Internet there is always the risk they will click on a link which takes them to unsuitable content. Children should be taught the appropriate behaviours if they come across inappropriate pages: press the 'back' button on the browser, exit the browser or turn off the computer monitor. This will allow the teacher to go back and check out the pages the child was using, talk through the some of the issues and reassure the child that this was not their fault.

The ICT Advice site contains case studies on safe use of the Internet.

Further information

There are many sources of help and advice for safe use of the Internet:

BBC WebWise (<http://www.bbc.co.uk/webwise>)
The Internet made simple by the BBC, with basic guides to searching, e-mail and Internet safety

Be Safe Online (<http://www.besafeonline.org>)
General information on Internet safety

ChildLine (<http://www.childline.org.uk>)
This contains a safe surfing guide

Childnet International (<http://www.childnet-int.org>)
A children's Internet charity committed to helping make the Internet a safe place for children, this provides safety advice, projects, resources and a section for children

Children's Charities Coalition for Internet Safety (CHIS) (<http://www.nch.org.uk/itok/chis>)
The coalition, which consists of Barnardo's, ChildLine, NCB, NCH, NCVCCO, NSPCC and The Children's Society, works with the government, the Internet industry and others to campaign on a range of safety issues affecting children's use of the Internet

For Kids By Kids Online (<http://www.fkbko.net>)
A site for children which helps them understand more about technology in general, as well as its safe use; it has specific guidance on e-mail, chat and instant messaging, along with advice on defending your system against viruses

ICT Advice site (<http://www.ictadvice.org.uk>)
Information, services and tools for those who use, implement and manage ICT in schools. Advice is given on management issues of Internet access, how to evaluate filtering products, developing acceptable use policies, along with case studies for safe use of the Internet.

Internet Watch Foundation (IWF)
(<http://www.iwf.org.uk>)

The IWF works in partnership with ISPs, software providers, police and others to minimise the availability of illegal, offensive and inappropriate material over the Internet

Kidsmart (<http://www.kidsmart.org.uk>)
A practical Internet safety advice web site resource produced by the children's Internet charity Childnet; it provides sections for teachers, pupils and parents

NCH IT OK (<http://www.nch.org.uk/itok>)
Advice on maximising the opportunities and controlling the risks of ICT for disadvantaged young people; it contains an Internet safety guide, a NetSmart checklist for children and useful guidance for parents on how to deal with spam and offensive e-mail

NSPCC (<http://www.nspcc.org.uk>)
Advice for young people and parents on surfing safely

Parents Information Network (PIN)
(<http://www.pin.org.uk>)
An independent service helping parents to support their children's learning through the use of computers, software and the Internet; it provides information on safety issues and filtering, along with specific guidance on text messaging and childsafe chat

Search Engine Watch
(<http://www.searchenginewatch.com/links/kids.html>)
Tips and information about searching the web, along with a comprehensive listing of search engines for children; it lists services which are designed primarily

4 – Understanding the technologies

to serve the needs of children, either in focus, or by filtering out sites that some parents and teachers might find inappropriate

Superhighway Safety web site

(<http://www.safety.ngfl.gov.uk>)

Information for schools and parents on safe use of the Internet; it provides examples of good practice for Internet use, information on filtering models, advice on developing acceptable use policies and guidelines for developing web sites

Wiredkids.org (<http://www.wiredkids.org>)

An American site dedicated to on-line safety for children and teenagers; it provides games, puzzles, stories and activities to reinforce the messages of safe surfing, and contains specific safety advice for instant messaging. There are also sections for teachers and parents.

E-mail

E-mail (electronic mail) is a message that can be sent over the Internet to someone else. It is one of the services that is offered by an Internet Service Provider (ISP). It is like posting a letter or a postcard, except that it can be sent just about anywhere on the planet in seconds at any time of the day or night. E-mail is great for communicating with people, and just about anything can be attached to, or included in an e-mail – text, pictures, even music and movies. To be able to send or receive e-mail a person must have an e-mail address.

The ISP supplies the school or individual with an e-mail account which can be set up on an individual machine using e-mail software such as Outlook Express or accessed using a web browser. Browser access to e-mail is called web-mail. This means that with the right username and password, e-mail can be accessed from any Internet-connected computer or mobile phone.

Each e-mail address has two parts, the mailbox username and the domain name of the school, separated by an @.

A school e-mail address would look something like **teacher@anyschool.county.sch.uk**.

E-mail addresses used at home would look something like **me@anydomain.com**.

The e-mail is sent and kept on the ISP's mail server until the user logs on to a computer and accesses their mail. The e-mail is then sent to the computer they are working on.

An overview of e-mail as a communication tool is given in Lesson 1 of these materials. Pupils will have an opportunity to explore e-mail, via the Cybercafé web site in Lesson 2, and detailed guidance on using e-mail safely is given in Lesson 4.

What are the benefits?

The use of e-mail in a school context can be extremely valuable as it enables pupils to communicate with other people across the world. Teachers have also reported that using e-mail helps pupils to take greater care with spelling (a misspelt e-mail address won't go anywhere) and be more precise with their choice of words, since e-mail encourages brevity and clarity. E-mail can also be particularly rewarding for pupils with special needs: those with physical or cognitive impairments may take a long time to create a message, but no one receiving it would know that they have difficulties, while pupils with severe hearing impairment find it another channel for communication. Examples of good practice of pupils using e-mail in the classroom can be found on the Teacher Resource Exchange (<http://tre.ngfl.gov.uk/>).

What are the risks?

Despite the benefits, e-mail is open to abuse, which may take various forms:

- Spam or spamming – this is unwanted e-mail that has been sent by a source that may be unfamiliar, such as a company trying to sell you a product. Names can be gleaned from discussion groups but there are companies which specialise in creating e-mail distribution lists.
- Flaming – this is the term used for abusive or insulting e-mail sent to people by others who do

not agree with an opinion, usually in news or discussion groups.

- Bombing – a bomb is a program that is intended to crash or damage a computer; a mail bomb is a huge message sent to someone's e-mail address to try and make their e-mail program crash.
- Stalking – it is possible to be harassed with unwanted and obsessive attention via e-mail.
- Viruses – a virus can be sent as e-mail attachments and some even pretend to come from known sources. These viruses can cause serious problems to computers, even allowing hackers to access the hard disk to take or destroy files.
- Inappropriate content – undesirable content such as pornography can arrive as unwelcome e-mail.
- Bullying – e-mail can facilitate on-line bullying between children.

What are the risks?

Even taking into account the dangers, e-mail is still an exceptional and successful way to share information and communicate. But it does require supervision and education about the risks and how to avoid them. Listed below are some specific issues to consider for remaining safe while using e-mail.

Acceptable use policies (AUPs)

In addition to providing guidelines for acceptable use of the Internet, a school's AUP should also provide clear guidelines for e-mail use. These guidelines should also be shared with parents as a framework for acceptable e-mail use in the home.

Acceptable Use Policies, and pupils' understanding of them, are covered in Lesson 2 of this pack.

Attachments

E-mail attachments should be treated with caution. Some viruses can attach themselves to messages without the sender's knowledge, so care should always be taken with an attachment even if received from a known source. A virus checker should always be used before opening any attachment.

E-mail addresses

Most schools will need to limit the use of pupils' e-mail addresses within school for management reasons, but in any case care should be taken to ensure that individual pupils cannot be identified or contacted via their e-mail address. A class or teaching group e-mail address may be more appropriate for use beyond an internal mail system.

The Superhighway Safety site provides guidance and examples of good practice on e-mail addresses at school.

E-mail bullying

Pupils should be made aware of the facts of e-mail bullying, the effects this can have on the recipient, and strategies for dealing with it. Sites such as Be Safe Online (<http://www.besafeonline.org>) and Bullying Online (<http://www.bullying.co.uk>) provide useful resources to tackle the issue.

E-mail bullying is covered in depth in Lesson 4 of this Scheme.

Filtering

In the same way that Internet access may be filtered, e-mail messages should also be filtered for inappropriate material and removal of spam. Although e-mail filtering systems are effective tools, they are not completely foolproof, and so must be supported by a safe and responsible approach to using e-mail.

The ICT advice site has a case study on filtering e-mail.

Mail from unknown senders

Pupils should be taught to recognise when messages come from unknown senders, and exercise caution over opening them. If in doubt as to their validity, pupils should delete the message or seek advice from an adult. If they receive messages that upset them or make them feel uncomfortable in any way, they should tell an adult. If possible use software to filter e-mail into 'real' messages and likely spam.

Strategies for dealing with mail from unknown senders and spam is covered in Lesson 4 of these materials.

4 – Understanding the technologies

Safe and responsible behaviours

When children are using e-mail, there is always a risk that they might receive unsuitable messages. Pupils should be taught the appropriate behaviours if they receive offensive or inappropriate e-mail messages, such as deleting the message, or closing it and seeking advice from their teacher – and never replying to them. This will allow the teacher to go back and check out the message, talk through some of the issues, reassure the child that this was not their fault, and take any other action as appropriate.

Pupils should be taught how to use e-mail appropriately and safely and to develop suitable writing conventions for the technology.

Lesson 2 encourages pupils to explore safe and responsible behaviours when using e-mail, via the Cybercafé site. These behaviours are developed in Lesson 4, and are reflected upon and consolidated in Lesson 8.

Viruses

A virus is a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. A virus is often designed so that it is automatically spread to other computer users, for example as an e-mail attachment, as a file download, or on floppy disk or CD. The sender of the e-mail is often unaware that they have sent a virus. Some viruses become active as soon as their code is executed; other viruses will lie dormant until circumstances cause their code to be executed by the computer. If a virus attacks your computer, it can corrupt or delete all stored information from the hard drive, including system software. All computer users are advised to guard against viruses by installing anti-virus software.

CERT, the Computer Emergency Response Team, provides a wealth of information on viruses, and recommends a simple five-stage test to avoid viruses:

- The **Know** test: is the e-mail from someone that you know?
- The **Received** test: have you received e-mail from this sender before?
- The **Expect** test: were you expecting e-mail with an attachment from this sender?
- The **Sense** test: does e-mail from the sender with the contents as described in the subject line and the name of the attachment(s) make sense?
- The **Virus** test: does this e-mail contain a virus? Always check it using anti-virus software.

Further information on protecting against viruses is available on the CERT web site (<http://www.cert.org>).

Anti-virus software is a program that searches your e-mail messages, hard drive and floppy disks for any known or potential viruses, and either deletes or repairs the problem. Some anti-virus software is free of charge and can be downloaded directly via the web, some you will have to pay for. Anti-virus software offers different levels of protection and the level of protection required should be a key consideration when making your choice.

The UK online centres area of the Superhighway Safety web site provides some useful guidance on viruses, including detailed information on both free and priced anti-virus software. The ICT Advice site also provides information on how to protect computers from viruses.

Viruses are covered in depth in Lesson 4 of the Internet Proficiency Scheme.

Web mail

Using free web-based e-mail accounts has inherent dangers, especially for younger children. Many allow e-mail addresses to be shared with third parties resulting in numerous unsolicited messages. Teach pupils to watch out for stringent privacy statements when signing up for web-based e-mail accounts.

The importance of keeping personal information private is covered in Lesson 3 of this pack.

Further information

Many of the general guides listed in the Internet section will also provide general guidance on safe use of e-mail. Some specific resources are listed below:

Be Safe Online

(<http://www.besafeonline.org/English/e-mail.htm>)

A general Internet safety web site, which also provides detailed information on e-mail; information on e-mail bullying, and strategies for dealing with it, is also included

Bullying Online (<http://www.bullying.co.uk>)

On-line help and advice to combat all forms of bullying, with sections for teachers, pupils and parents; it includes a guide to staying safe in cyberspace

For Kids By Kids Online (<http://www.fkbko.net>)

A site for children which helps them understand more about technology in general, as well as its safe use; it has specific guidance on e-mail, chat and instant messaging, along with advice on defending against viruses

NCH IT OK (<http://www.nch.org.uk/itok/>)

Offers advice on maximising the opportunities and controlling the risks of ICT for disadvantaged young people; it contains an Internet safety guide, a NetSmart checklist for children and useful guidance for parents on how to deal with spam and offensive e-mail

Chat

Chat is a way of communicating with people at the same time by typing messages which then appear on your computer screen, and are sent across the Internet to be read by everyone else participating in the chat at that time. Chat happens in 'chat rooms' – a virtual meeting place, and the process of taking part is known as 'chatting'. Participants are sometimes referred to as 'chatters'.

There are many different chat rooms available on the Internet. They can be a dedicated part of a web site or a service offered by an ISP. Fundamentally they all work in the same way. Users have to register in a chat room of interest by

choosing a username and password; this is often a pseudonym or false name. Normally there will be a list of users currently chatting. These users will be alerted when someone new enters the chat room. To contribute to the chat, the user can type messages into a text box and the message is immediately seen by the others in the chat room so that they can respond. Users can enter a chat room without contributing to the discussion but still be able to read what the others are saying. This is known as 'lurking' which is accepted practice and is a good way of getting to know how to use a chat room.

Some chat rooms are public and can be joined by anyone. Other chat rooms are private and open only to invited chatters or specific groups. Another mechanism that is offered by some chat rooms is 'whispering'. This is where you can go off to one side and have a private conversation with someone.

To help speed up the flow of conversation in a chat room, acronyms have been invented. Some examples are listed below:

LOL – laugh out loud

BTW – By the way

j/k – just kidding

An overview of chat as a communication tool is given in Lesson 1 of this pack. Pupils will have an opportunity to explore chat, via the Cybercafé web site, in Lesson 2 and the topic is covered in depth in Lesson 6.

What are the benefits?

Chat rooms can have real educational benefits. Pupils are able to chat with peers anywhere in the world, in real time, sharing experiences, comparing lifestyles or working collaboratively. Frequently, on-line chats are hosted with notable figures, such as a successful business person, a television presenter or a pop idol, giving children access to a wealth of information and experience in a way that would not be possible in the real world.

Examples of schools using chat in the classroom can be found on the Superhighway Safety web site (<http://safety.ngfl.gov.uk/schools>) and the ICT Advice web site (<http://www.ictadvice.org.uk/>).

4 – Understanding the technologies

What are the risks?

Chat rooms have an element of anonymity, so children often talk about things they may not have the confidence to say face to face. They can pretend to be someone else: older, smarter, and more popular. Taking on a pseudonym is an accepted and encouraged practice in chat rooms.

Anyone who uses a chat room has to be careful about how much personal information they give out to the people they are chatting to. This is particularly difficult with young people, who may feel that they know the people they are chatting to very well, especially if they are talking about intimate or sensitive subjects with them. Unfortunately, for those who want to attract children, using chat rooms is an excellent means of doing so. They are able to win their confidence by appearing to be 'on their side'. This is known as 'grooming', as already discussed under risks earlier in this section. It is important that young people understand it does not matter how well they think they know someone on line: they never know who they really are. Young people should be told that they should never arrange to meet anyone they have met on line, no matter how well they think they know them.

Groups are often formed just like at school, with an invented set of acronyms as a way of keeping conversations private or excluding others from the 'in crowd'. Bullying can also happen in a chat room.

Potential risks of chat and chat rooms are a topic of discussion in Lesson 1 of these materials. The importance of keeping personal information private, particularly in chat rooms, is covered in Lessons 3 and 6.

Avoiding the dangers

There are a number of strategies for helping to keep children safe.

Acceptable use policies (AUPs)

In addition to providing guidelines for acceptable use of the Internet, a school's AUP should also provide clear guidelines for use of chat, both in school and beyond. These guidelines should be shared with parents.

Acceptable Use Policies, and pupils' understanding of them, are covered in Lesson 2 of this pack.

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 the conversations stay on topic or there is some sort of software that monitors the conversations and alerts a moderator should there be any unsuitable 'chat' going on. This is known as proactive or reactive monitoring. Proactive is the best type in an educational context as the moderator is able to step in if things are straying off topic. All good chat rooms should have clear policy and privacy statements, an archive of previous conversations and an outline for forthcoming topics.

Young children should always use moderated chat rooms. GridClub (<http://www.gridclub.com>) is a good example of a moderated chat room for Key Stage 2 pupils. It is moderated by trained professionals and all members have to be verified through their school. GridClub can only be used by pupils in this age group and they can gain access at home or at school.

The ICT Advice site provides information on how to use chat in the classroom safely.

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

Moderated chat rooms are covered in Lesson 6 of these materials.

Safe and responsible behaviours

While chatting, children should never give out personal details that would identify who they are, such as surname, address, phone number or school, or arrange any face-to-face meetings with anyone they have met in a chat room (unless their parents or carers agree and go with them).

Children should also be taught not to rely on strangers they meet in a chat room for important advice. If there is bad language or if anyone writes anything that makes a child feel uncomfortable

should not reply to the message but instead tell a teacher, parent or carer. The chat room moderator can be told of this and the perpetrator removed from the chat room. Children should also be aware that their actions in a chat room will affect others and be taught to behave responsibly with respect for all.

If a situation occurs where a child is suffering abuse in a chat room they should be taught what to do. One method that they can apply is to save the conversation. Some chat rooms allow users to 'log their chat', or alternatively users can use the 'save as' function, copy and paste, or print screen. Instructions on how to do this along with other useful tips are detailed on the For Kids By Kids Online web site (<http://www.fkbko.net>). The charity Childnet also has some useful information for pupils on how to stay safe in chat rooms (<http://www.chatdanger.com/>).

Further information

Many of the general guides listed in the Internet section will also provide an overview on safe use of chat, in addition to the specific resources below:

Be Safe Online

(<http://www.besafeonline.org/English/chat.htm>)
A general Internet safety web site, which also provides detailed information on chat

GridClub (<http://www.gridclub.com>)

General information on Internet safety, with fun activities and a moderated chat room for Key Stage 2 pupils

Chatdanger

(<http://www.chatdanger.com/home/index.htm>)
Information on how to keep safe in chat rooms, including sections on using chat in schools, and a parents' guide to using chat at home

For Kids By Kids Online (<http://www.fkbko.net>)

A site for children which helps them understand more about technology in general, as well as its safe use; it has specific guidance on e-mail, chat and instant messaging, along with advice on defending against viruses

Parents Information Network (PIN)

(<http://www.pin.org.uk>)
An independent service helping parents to support

their children's learning through the use of computers, software and the Internet; it provides information on safety issues and filtering, along with specific guidance on text messaging and childsafe chat

Yahooligans! (http://www.yahooligans.com/Arts_and_Entertainment/Chat/)

Yahooligans! web guide for kids provides a list of safe chat areas for children

The main Yahooligans! area also provides guidance for teachers and parents on safe communication on line (<http://www.yahooligans.com>).

Instant Messaging (IM)

Instant messaging is a form of on-line chat but it is private between two people. It is not moderated and cannot be joined by others. When you send an instant message it goes straight to the person you sent it to and appears on their computer screen almost immediately. Some services also allow the sending of files to one another. Internet messaging is also known as IM, IMing, Internet Relay Chat (IRC), or ICQ ('I Seek You').

Instant messaging is a service offered by Internet Service Providers (ISPs) and other web companies. To use instant messaging you will need to install a piece of software on your computer. The person you want to talk to will need the same software installed on their computer. When a user logs on to the Internet, their computer registers them as being on line with the instant messaging service. When another user registers and connects, they will know that he or she is logged on. Many services now also offer the facilities for users to 'appear' off line if they don't wish to be disturbed.

Using the service usually requires registration, giving a username and e-mail address. Instant messaging allows the user to maintain a list of people that they wish to interact with. They can send messages to any of the people in their list, often called a buddy list or contact list, as long as that person is on line. They are then able to send notes back and forth with friends who are on line or create their own customised chat rooms.

4 – Understanding the technologies

An overview of instant messaging as a communication tool is given in Lesson 1 of the pack. Further information is provided in Lesson 6.

What are the benefits?

Instant messaging is quick and effective when used in the right context and can be a very easy way of communicating with somebody instantly. In an educational context instant messaging could be used to work collaboratively with a friend when doing research on the Internet, although typically it is used in a social context.

What are the risks?

Instant messaging notifies others when a user signed up to the service goes on line. This is the reason instant messaging works so well. The downside is that they could be added to someone else's buddy list and be contacted by a total stranger. There is also an issue of privacy. To use messaging you need to register on line to an instant messaging service. These are usually free, but when registering providers usually ask for a lot of personal information. This information could potentially be made publicly available to others.

Avoiding the dangers

Many schools will block access to instant messaging and so the following issues may be more associated with home usage than school. Nevertheless, it is important that pupils are made aware of the safe use of IM as part of their general ICT skills development.

Attachments

Care should be taken when sending or receiving attachments via instant messaging. Similar caution should be exercised with e-mail attachments, and attachments should always be virus checked.

Automatic login

Many instant messaging programs automatically log on registered users when they access the Internet. This could be an issue, particularly when computers are shared, meaning that a 'buddy' who is apparently on line may be a brother, sister or other family member of the person with the IM account. Children should always check that the person they are instant messaging with is who they

think they are, perhaps by using a simple password and response as the first message of the IM session. It may also be possible to adjust privacy settings in the instant messaging software to always ask for a password before signing a user in.

Buddy lists

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

Harrassment

If a child is harassed by IM, the service's system administrators should be informed giving the nickname or ID, date, times and details of the problem. The system administrators will then take appropriate action, which could involve a warning or disconnection from the IM service. It might also be worth re-registering for instant messaging with a new user ID.

Registering

When registering for an IM service, pupils should ensure that they give as little personal information as possible and only use services that have clear privacy policies that state that they will not make information publicly available. Many services also provided members' directories – it's always best to decline an entry in such directories, as any details provided may be made publicly available, and hence available for any members of that community to see.

Safe and responsible behaviours

As with any form of electronic communication, pupils should be taught safe and responsible behaviours when using IM. They should never give any personal information when instant messaging, or any other information which might make them identifiable. If at any point during an instant messaging conversation pupils are made to feel uncomfortable, they should end the conversation, and seek advice from an adult.

Further information

Many of the general guidance in the Internet section will also apply to instant messaging, but some specific resources are also listed below:

Be Safe Online (http://www.besafeonline.org/English/instant_messagin.htm)

A general Internet safety web site, which also provides detailed information on instant messaging

For Kids By Kids Online (<http://www.fkbko.net>)

A site for children which helps them understand more about technology in general, as well as its safe use; it has specific guidance on instant messaging

Wiredkids.org (<http://www.wiredkids.org/safety/im/>)

An American site, providing general on-line safety information with guides on instant messaging safety for both children and their parents

Short Message Service (SMS) or Text Messaging

Short Message Services (SMS) enable users to send and receive text messages via mobile phones. Messaging is usually short and often replaces a full conversation with someone, particularly if the other person is not available to take a voice call. It's also known as text messaging, mobile text messaging, texting or g-mail.

In order to send and receive SMS, the user usually has to pay a monthly fee to their service provider or a small fee for each text message. Some companies offer SMS free of charge. Text messages can also be sent from some web sites that offer to send messages to mobile phones.

The text can comprise words or numbers. Typically messaging is used to say hello, arrange a meeting, provide snippets of information or prompts. Messages are usually created using button combinations from the mobile phone keypad.

As typing messages with the limited keys on the phone is time consuming, many words can be written as abbreviations:

AFAIK – As far as I know

CUL8r – See you later

Gr8 – Great

ILBL8 – I'll be late

LOL – Laugh out loud

NMP – Not my problem

THNQ – Thank you

What are the benefits?

As messages are delivered to mobile phones and can be stored for later reference, SMS is often more convenient than e-mail to communicate with groups of people. Once familiar with reading, sending and replying to messages, SMS is a useful way of exchanging information and keeping in touch with friends. Almost three quarters of a billion text messages are sent every day.

What are the risks?

Young people aged 14 to 16 are the biggest users of mobile phones. Almost two thirds of young people in that age group have access to a mobile phone. Of all of the technologies this is the one that pupils are most likely to be familiar with. Therefore it is imperative that they use it effectively and safely, and avoid any risks.

Texting is more casual than a phone call as messages can be sent and received at times when other communication is not convenient. It is also perceived as being more anonymous, particularly if the message is sent via a web site. Sometimes text messages are sent to embarrass, threaten or bully someone. This can be particularly upsetting as the message can arrive when the receiver least expects it and if the person's number is not listed in the receiver's address book then the receiver will not know who has sent the message. There have also been instances where a message has been sent out to various random numbers. These messages can be flirtatious in nature. If receivers respond, it lets the sender know that the number is in operation and they can be bombarded with inappropriate messages.

The use of texting for unsolicited advertising is becoming more common, often with promises of free offers for responding, or notifying of a competition 'win'. If an offer sounds too good to be

4 – Understanding the technologies

true, it generally is. This is just another form of spam and so should be ignored. Texting can also be used inappropriately, such as during a test.

An overview of SMS as a communication tool is given in Lesson 1 of these materials. Pupils will have an opportunity to explore SMS, via the Cybercafé web site, in Lesson 2, and detailed guidance is given in Lesson 7.

Avoiding the dangers

There are a number of ways of avoiding problems.

Abusive text messages

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

Bullying by text message

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

Sites such as Be Safe Online (<http://www.besafeonline.org>) and Bully Online (<http://www.bullyonline.org/schoolbully/mobile.htm>) provide detailed advice on tackling the issue of bullying by text message.

Safe and responsible behaviours

As with any form of electronic communication, pupils should be taught safe and responsible behaviours for text messaging. As with any personal information, mobile phone numbers should never be given to an unknown source, such as an on-line registration form. It is also important to give and type mobile numbers accurately as messages can go astray to be read and replied to by unknown parties.

Lesson 2 of the Internet Proficiency Scheme encourages pupils to explore safe and responsible behaviours using SMS, via the Cybercafé web site. These behaviours are further developed in Lesson 7, and are reflected upon and consolidated in Lesson 8. The importance of keeping personal information private, such as mobile telephone numbers, is covered in Lesson 3.

Spam by text

Text messages received from an unknown number are likely to be spam. The message should be deleted or if in doubt, pupils should be encouraged to ask an adult for advice.

Further information

Be Safe Online (http://www.besafeonline.org/English/bullying_online.htm)

A general Internet safety web site, which also provides information on bullying by e-mail, over the Internet and by text messaging

Bully OnLine

(<http://www.bullyonline.org/schoolbully/mobile.htm>)

A general guide to bullying, which provides specific advice on tackling bullying by text messaging for children

Office of Telecommunications (OfTel)

(<http://www.oftel.gov.uk>)

Guidance and further links on dealing with unsolicited text messages

Parents Information Network (PIN)

(<http://www.pin.org.uk>)

An independent service helping parents to support their children's learning through the use of computers, software and the Internet, the site provides specific guidance on text messaging



Multimedia Message Service (MMS) or Picture Messaging

Multimedia Message Service (MMS) is the latest development in mobile messaging, and like the short message service (SMS), multimedia messaging provides automatic and immediate delivery of personal messages using mobile phone technology. Unlike SMS, however, MMS allows the sender to incorporate sound, images and video into their message. It's also known as multimedia messaging, mobile multimedia messaging, picture messaging and enhanced messaging service (EMS).

Whereas most modern mobile phones incorporate SMS facilities, MMS requires an MMS-enabled mobile phone. Whilst at present these are expensive, over time prices will undoubtedly fall and their use will become more widespread. The user usually has to pay a fixed monthly charge for multimedia messaging facilities, or a charge per message depending on the service provider. Unlike SMS, MMS is not yet available to users who pre-pay.

Many MMS phones feature integrated cameras allowing users to take photos to incorporate with their message, although this is not standard. Messages are sent as multimedia presentations in a single entry, as opposed to text files with attachments as many other forms of electronic communication. MMS technology provides support for e-mail addressing, so that messages can be sent from phone to e-mail and vice versa.

What are the benefits?

Like SMS, MMS is set to become more convenient than e-mail to communicate with groups of people, providing automatic, immediate delivery of personal multimedia messages from phone to phone, or phone to e-mail. With its enhanced ability to send audiovisual files, some predict that MMS will revolutionise mobile communications.

What are the risks?

Whilst the costs of MMS phones are probably prohibitively expensive at present, it is thought that young people will provide a key market in the future.

MMS will present all the same risks as SMS, but with its multimedia capabilities, and ease of sending

images there is real concern that children will either be exposed to inappropriate materials, or be asked to send photos of themselves via their MMS phones. This is of particular concern if friendships formed on line, in chat rooms for example, progress to texting as a means of communicating. MMS will undoubtedly also be used for unsolicited advertising as the market matures.

The full extent of the risks posed by MMS, however, are still to be seen.

Avoiding the dangers

Various strategies can be adopted to minimise risk.

Abusive multimedia messages

As with SMS, any abuse of MMS should be reported to the mobile phone service provider and details logged. Mobile phone numbers should not be passed to any unknown source, and caution should be exercised before opening any multimedia message from someone unknown to you. If in doubt, delete the message.

Bullying by MMS message

Bullying by MMS message will probably become inevitable. As with bullying by SMS, children should seek immediate 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, the time, the caller ID, or whether the number was withheld or not available. Sites such as Be Safe Online (<http://www.besafeonline.org>) and Bully Online (<http://www.bullyonline.org/schoolbully>) provide detailed advice on tackling the issue of bullying by text message, but the basic advice will equally apply to picture messaging.

Safe and responsible behaviours

As with any form of electronic communication, pupils should be taught safe and responsible behaviours for multimedia messaging. It is also important to give and type mobile numbers accurately as messages can go astray to be read and replied to by unknown parties. As with any personal information, mobile phone numbers should never be given to an unknown source, such as an on-line registration form.

4 – Understanding the technologies

Spam by MMS

Spam by MMS is also likely to become inevitable.

The message should be deleted, or if in doubt, pupils should be encouraged to ask an adult for advice. Children should not be tempted to respond to spam in any form, even if wild promises and incentives are offered for replying.

The importance of keeping personal information private, such as mobile telephone numbers, is covered in Lesson 3. Safe and responsible behaviours to adopt when using MMS are covered in Lesson 7, and these are reflected upon and consolidated in Lesson 8.

Further information

As yet there is little available information on MMS, but this is likely to develop over time. Sources of information and advice for SMS will generally apply to MMS also.