

A child's face is shown in profile, looking towards the right. A bright blue lightning bolt strikes the child's forehead. The background is a mix of purple, blue, and white, with a grid pattern. The text is overlaid on the left side of the image.

Help...

I want my child to
stay safe on the net

childprotectionuk.net

Safeguarding children and young people

Help...

I want my child to stay safe on the net

Where do I start?

If you have a child of eight years or over, the chances are they have already been introduced to the Internet; at school, through peers, or in a public venue such as a local library or Cyber/Internet café. Many mobile phones now also offer the Internet services we will be describing.

It may well be you are familiar with these modern technologies and are able show your child how to use the Internet sensibly and safely. For many of us however, it can seem like a parallel world where people communicate in mysterious techno-jargon. Added to that, our children appear to be the experts when they talk of 'surfing', 'phishing' (aren't they pastimes engaged in at the seaside?) and 'messaging'.



Whilst the Internet is an excellent resource and effective communication tool, the downside is that there are unscrupulous individuals who use it to gain access to exploit and even harm children. The following pages provide the information you need to know to ensure your child is safe when using this technology.

**Terminologies and Jargon
Uncovered – pages 4 & 5**

What are the risks?

False identities

One of the downsides of the Internet is that a person can pretend to be someone they're not. This is a tactic frequently used by fraudsters to gain access to personal financial details. More worryingly however, is the ease with which a person who is a danger to children can conceal their true identity. There have been several reported instances of sexual/violent offenders entering a chat room under the guise of a child, sending emails or communicating via instant messenger services and then attempting (sometimes successfully) to meet the child with whom they are communicating, who is oblivious to the deception.

Bullying

A child might be sent messages via chat, email or mobile phones that are threatening, demeaning or harassing. Bullying via these Internet services (known as cyber bullying) is typically, but not exclusively, carried out by other children. For further information go to: www.stoptextbully.com

Viruses, hackers and fraudsters

Without proper training and supervision, a child could quite innocently download and open a file containing a virus, or inadvertently allow a hacker/fraudster access to personal information such as credit card details. They could also illegally download programmes such as copyrighted music.

Mobile phones

Many parents are happy for their child to have a mobile phone so they are easily contactable, particularly in an emergency. It is worth bearing in mind however, that apart from chat, children can also use a mobile phone to send/receive text, picture and video messages. 3G (Third generation) phones enable children to access the web and video clips, and they may therefore be vulnerable to contact by fraudsters and those who are a danger to children.



Terminologies and

Anti-virus software

A program that searches a computer for viruses, removes them and can prevent new viruses from damaging the computer.

Bulletin board

An Internet forum (usually on a specific interest/topic) where someone will write a message that anyone can read and reply to.

Chat room

An area (i.e. room) on the Internet, usually dedicated to a particular interest, hobby or group, where people can communicate (i.e. 'chat') with others. A person will type in what they want to say and anyone using the chat room can see what has been written and write their own message/reply.

Cyber cafe/Internet café

Premises, often similar to an ordinary café, where computers and the Internet are available to use for a charge.

Computer file

Information/data stored on a computer.

Download

To copy information (a file) from one computer to another, e.g. information on a web site or information sent with an email (attachment).

Email

Messages sent electronically like writing and sending a letter.

Email Account

To be able to send and receive emails, appropriate software must be installed on the computer (e.g. Microsoft Outlook) and then an electronic connection set up with an ISP.

File Sharing

Where computers are linked to share information/data. P2P (Peer to peer) is an example of this, often used to share music.

Firewall

A security system designed to prevent unauthorised access to a computer, usually through a specialised software program.

Hacking

The correct term is 'cracking'. Someone who 'cracks' gains unauthorized access to computers, usually to do malicious things.

Instant Messaging (IM)

The act of instant communication between two or more people using the Internet via text based messages or using a web cam (camera attached to the computer) and microphone. Users have a contacts list and most instant messenger services indicate whether a person on someone's contacts list is online.

Internet

Computers linked to one another globally, often referred to as the World Wide Web, Cyber Space, or Information Super Highway.

Jargon Uncovered

ISP / Internet Connection

To use the Internet, a computer has to be connected to an Internet Service Provider (e.g. most telephone companies), and there are several ways this can be set up. The ISP can explain and advise on the alternatives available.

Internet browser

Software (e.g. Internet Explorer) that allows Internet users to view (browse) information, images and text typically on websites.

Online

Being connected to other computers to exchange information.

PC

Personal computer.

Phishing

A scam that lures people to fake websites by sending emails claiming to be a bank or similar to obtain personal financial information e.g. bank account numbers, pins, etc. to steal money.

Software

The programmes and procedures required to enable a computer to perform a specific task. Programmes such as Word (word processor) and Internet Explorer are examples of different kinds of software

Spam

Spam refers to electronic junk mail. Spam is unsolicited email sent indiscriminately, often containing

irrelevant or inappropriate messages, especially commercial advertising. Usually sent in mass quantities

Surfing or browsing

Using the Internet and viewing pages of information.

Web-jacking

Gaining control of a computer by a third party to destroy personal information.

Web site

A location on the Internet containing information that can be viewed, downloaded and printed - a bit like an Internet version of a book or magazine. The 'author' or 'publisher' can be an organisation or individual. A web site can also contain interactive content including video, music, and games. Some sites sell products (online shops) or contain reference material (like a library).

Virus

A file containing malicious software code (often transferred via emails) that could damage the computer by deleting programs and documents. A trojan (as in Trojan Horse) is a destructive file often masquerading as genuine that can allow someone to gain remote access to a computer. A worm is a type of virus that replicates itself on a computer affecting the computer's ability to run programs.

Keeping it safe

Good communication with your child is a major key. Discussing how the Internet works and safety issues are good starting points. To keep things light and open, you could encourage your child to show you things they've been taught. Alternatively, if they are starting out, you could learn together. It is important if your child's understanding is greater than your own, you find out about the technologies they are using and others that are available. For example, does your child use a free email account such as Hotmail?

Ground rules

Not many of us like rules, particularly children, but boundaries are important when it comes to using the Internet. Discuss and agree these with your child and, depending on their age, encourage your child to type them up and then display them near the computer as a reminder. This way your child will feel involved in the decision-making process and is more likely to comply.

One ground rule may be to restrict the time your child spends on the computer. Apart from the obvious health issues, the excessive and furtive use of online services, especially late at night, might indicate there is a problem. Generally, children should be discouraged from meeting anyone they have been communicating with over the Internet. However, if for reasons such as a shared interest, you decide your child can meet up with another child, always make sure a responsible adult accompanies them because, as

we have said already, an identity on the Internet can be fake.

In view of the move toward combining Internet and mobile phone technologies, these ground rules should also include the use of a mobile phone. Agreeing the content and boundaries of use with your child is important, as well as ensuring what they do is legal.

Location

Whilst your child is entitled to a certain amount of privacy, it is a good idea with young children to locate the computer in a family room where the screen is clearly visible. Activities like 'surfing' can become a social pastime where discoveries can be made and shared together. This may be less acceptable to older children who value their own space and want to use a computer in their bedroom. If this is the case there is nothing wrong with reminding them of the boundaries and explaining potential dangers.



Safeguarding through technology

Your ISP can provide software (or you can acquire your own) that will assist in the management of your child's use of the Internet. The software can block chat areas, newsgroups, and websites that are known to be inappropriate for children (e.g. nudity, sexual, violent or hateful material as well as those advocating the use of alcohol or drugs). Filtering software is also available that allows a parent to restrict access to sites via a rating system, though not all websites subscribe to it at this time. In addition, a filter can be added to your email service to restrict spam. Ensure that you install anti-virus software. New viruses are reported daily so it will need regular updating. It is also wise to install a firewall for security.

Personal Information

Never allow your child to give out personal information such as school or home address, phone number, photos etc. in chat rooms, on bulletin boards and especially not to strangers.

Downloading

Discourage your child from downloading pictures from an unknown source. They may be sexually explicit or contain a virus. Monitor the files your child downloads and consider sharing an email account.

Concerns

Encourage your child to come and talk to you if anything happens whilst they are using the Internet or mobile phone that upsets or concerns them. Reassure them they are not to blame if something unsolicited appears on the screen or if they have made a genuine mistake in logging into

something inappropriate. Make it clear they should let you know straight away what has happened. You can report any concerns to the Internet Watch Foundation (see back cover).

If your child receives a message that is harassing, threatening or of a sexual nature, forward a copy on to your ISP and ask for their help. Instruct your child never to click on any links (files or web addresses) contained in emails from people they don't know.

If someone sends a message or image that is indecent, lewd, sexually explicit or obscene or you become aware of the use, transmission or viewing of child abuse images, immediately report this to your ISP, and either the Child Exploitation and Online Protection Centre (suspicious activity on-line) or the Internet Watch Foundation (websites - see back cover).

Conclusion

This booklet is only a basic overview, so CCPAS recommends that you expand your knowledge. All the organisations listed on the back cover have excellent resources and information available. You could also consider enrolling on a computer course.

The Internet is an essential tool for the 21st century. Computer literacy is part of the National Curriculum and is widely promoted by central government. Used responsibly it provides an ideal forum for children to learn, share and communicate. Parents have an essential role in facilitating the process so that children can do this safely.

Contact organisations

The Internet Watch Foundation

East View
5 Coles Lane
Oakington
Cambridge CB4 5BA
Tel: 01223 237 700
Fax: 01223 235 921

The UK hotline for reporting illegal content (e.g. Child abuse images, criminally obscene and incitement to racial hatred). Reports should be made online at: <http://www.iwf.org.uk/>

The Child Exploitation and Online Protection (CEOP) Centre

33 Vauxhall Bridge Road
London SW1V 2WG
Telephone: 0870 000 3344
Email: enquiries@ceop.gov.uk
Website: <http://www.ceop.gov.uk/>
To report suspicious behaviour online with or towards a child contact the CEOP Centre online by email or the CEOP website.

Childnet International

Head Office
Studio 14 Brockley Cross Business Centre
96 Endwell Road
London SE4 2PD
Telephone: 020 7639 6967
Fax: 020 7639 7027
Email: info@childnet-int.org
Website: <http://www.childnet-int.org/>
Works in partnership internationally to help make the Internet safe for children. Resources also available covering all areas of Internet safety.

childprotectionuk.net

PO Box 133
Swanley
Kent BR8 7UQ
Telephone: 0845 120 45 50 (helpline)
Fax: 0845 120 45 52
Email: info@ccpas.co.uk Website:
www.childprotectionuk.net or
www.ccpas.co.uk

This booklet has been produced by

childprotectionuk.net

Safeguarding children and young people

working in partnership with the CEOP Centre to protect children.



and sponsored by

THE
FORESTERS'
FUND FOR
CHILDREN
Helping Others to Help Children



PO Box 29429, Cumbernauld, Glasgow, G67 9AL
Tel & Fax: 01236 736192
Web: www.forestersfundforchildren.org.uk
Charity Registration no. 327449
Registered in England no. 2128697

(childprotectionuk.net is a working name of the Churches Child Protection Advisory Service. Charity number: 1004490. Company number: 264648)