

Safe Online Our responsibility

ensure young people “stay safe”.

Many parents and teachers find keeping up-to-date with children’s use of technology is challenging. Knowing the trends in children’s use of technology and the kind of environment they are immersed in is key to giving them the right advice and guidance in a timely and age-appropriate way.

In schools, e-safety relates to many parts of the curriculum, including ICT, citizenship and PHSE. More broadly, however, because technology can be used in any subject area, it is relevant to all teachers. The Byron Report makes clear the issues and the responsibilities of government, schools and others in the protection of children. Importantly, e-safety is a significant aspect of the Every Child Matters agenda.

This guide will help you to understand the key issues in e-safety. It will help you identify some of the issues and provide starting points for discussion with your children, pupils, students and clients.



*Further help online is available from
Childnet International.*

<http://www.childnet-int.org>

Know IT All

Welcome to Childnet’s Know IT All Website

Know IT All is an **award-winning** set of interactive resources developed by Childnet to educate both young people, parents and teachers about safe and positive use of the internet.

Choose one of the Know IT All resources below to find out more.



Know IT All for Schools



Videos, quizzes, polls and interactive classroom activities help students reflect on their own use of the latest internet and mobile phone

Know IT All for Parents



Know IT All for Parents has been designed to help parents get the most out of the Internet and mobile phone for themselves and their children

Know IT All for Volunteers



Know IT All for Volunteers which is called Getting to Know IT All is a special version of the Know IT All suite of products which was designed especially for volunteers or non

Know IT All for Trainees



Know IT All for Trainees has been designed to help teachers in their initial teacher training become aware of the e-safety issues

SO WHAT ARE THE RISKS?

We categorise the risks for children into three areas; these are: CONTACT, CONTENT and COMMERCIALISM.

CONTACT *Contact from someone online who may wish to bully or abuse the child.*

ONLINE GROOMING

A criminal minority makes use of the internet and related services, such as chat rooms, gaming and social networking sites, to make contact with young people. The intention of these people is to establish and develop relationships with young people with the sole purpose of persuading them into sexual activity. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'. The Sexual Offences Act 2003 includes a grooming offence specifically introduced to combat this abuse of the internet.

JENNY'S STORY

DVD available from Childnet (parents), Becta (schools) and TDA (teacher training)

CYBERBULLYING

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

CONTENT *Inappropriate material available to children online.*

VIEWING INAPPROPRIATE CONTENT

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

PLAGIARISM AND COPYRIGHT

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

INACCURATE INFORMATION

Anyone can write what they want and post it on the internet, and as a result not all the information available online is good information. Inaccurate information can be misleading or even dangerous in some situations, for example when it covers health advice.

USER-GENERATED CONTENT

With the advent of Web 2.0 technologies (web-based technologies that emphasise online collaboration and sharing among users), young people are increasingly creators of digital content and some of it can be very personal. For example blogs or 'web log'. are journals that are available on the web. The activity of updating a blog is 'blogging'. Blogs are a popular part of web 2.0. It is now also simple to create digital content and upload it to the internet or a mobile phone. Children need to know that embarrassing or compromising words or photos of themselves or their friends, once online, could stay there forever and be used against them in the future.

COMMERCIALISM *Aggressive advertising and marketing schemes can invade young people's privacy, both online and via their mobile phones.*

E-COMMERCE

E-commerce continues to grow, and there is a risk that young people may give out financial details, for example the credit card details of a parent, while online. This can result in unexpected consequences and charges. Studies found that children were able to register with online gambling

websites using debit cards issued on youth accounts, which are typically available to children as young as 11.

PRIVACY

Many sites and online services request personal information and data about a user. Protecting one's privacy online is an important issue, because personal information is sometimes misused and passed on to third parties. Pupils need to be taught how to protect their privacy when using the internet.

JUNK EMAIL OR SPAM

Unsolicited emails or text messages containing offers that sound too good to be missed can often contain links to content that is inappropriate for children. Phishing and similar scams may trick young people (and their parents) into revealing personal or financial information which could be used for identity theft.

PREMIUM RATE SERVICES

Premium rate services offer ring tones, logos and competitions. The phone numbers for these services often begin with 090. Information and entertainment is available via landline telephone, mobile phone, PC (by email, the internet or bulletin boards) and interactive digital TV services for a high charge. Some children have been caught out by premium rate subscriptions: they thought they were making a one-off purchase of a ring tone, but were in fact tied in to a reverse-billed subscription (in which you pay to receive rather than send text messages).

WHAT ARE THE TRENDS?

SOCIAL NETWORKING AND BLOGGING

Social networking sites, chat rooms, wikis and blogs are places where young people can create personalised web-pages or profiles to express themselves or connect with their friends or social networks. These web-based technologies are part of Web 2.0 technologies.

DOWNLOADING, PEER-TO-PEER COMMUNICATION AND FILE SHARING

A file-sharing network enables people to exchange photos, videos, music, software and games directly between computers using downloaded P2P software. Many young people use these networks to download copyrighted music, films and software.

MOBILE TECHNOLOGIES

Increasingly, all web-based services are becoming available on mobile phones. Social networking, for example, is set to become increasingly mobile: as handsets become increasingly sophisticated, users will be able to upload content to their profiles on the internet from their mobile phones while on the move. Other technologies, such as games machines, also give access to the internet or Bluetooth™.

FURTHER BROWSING

After reading this leaflet, spend at least 20 minutes exploring the online resource Know IT All For Trainees, identifying the relevant and important aspects, making the connections with your own subject, and identifying the implications of e-safety for the Every Child Matters agenda. This site also hosts the Know IT All for Parents CD-ROM produced by Childnet. <http://www.childnet.com/kia>

Becta leads the national drive to improve learning through technology. Becta does this by working with industry to ensure it has the right technology in place for education. It also supports the education sector to make the best use of technology so that all learners in the UK are able to benefit from its advantages and achieve the best they can. <http://www.becta.org.uk>

Childnet's Chatdanger website gives details about the potential dangers of interactive activities like chat, instant messaging, online games, email and mobile phones. Read true stories and find out how to keep safe while chatting online. <http://www.chatdanger.com>

This site from CEOP lets young people learn about e-safety and report abuse which occurred online. It contains lots of useful advice on e-safety, including advice on gaming, blogging and mobile phones. There is an excellent short film clip about grooming. <http://www.thinkuknow.co.uk>

Get Safe Online is a 10-minute internet safety and computer security guide with useful links for both parents and teachers. <http://www.getsafeonline.org>

Childnet's Digizen website gives guidance produced by Childnet for the Department for Children, Schools and Families on cyberbullying. It lists a range of resources suitable for teachers to use with pupils and contains a competition area for young people. <http://www.childnet.com/digizen>

WHERE TO REPORT

In schools, if teachers suspect that a pupil is a victim of physical abuse or you have received any type of disclosure about abuse occurring either online or offline, they **MUST** contact the designated member of staff immediately and make it clear to the pupil that they will have to share the information with a colleague. For their benefit, teachers should make and sign accurate notes of the incident immediately after the disclosure.

REPORTING SUSPICIOUS BEHAVIOUR ONLINE WITH OR TOWARDS A CHILD

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

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

REPORTING ILLEGAL CONTENT

The Internet Watch Foundation (IWF) is the UK hotline for reporting illegal content, specifically child abuse images hosted worldwide and content that is criminally obscene and/or an incitement to racial hatred, hosted in the UK. A prominent link for reporting illegal content is available from the home page of the IWF website. <http://www.iwf.org.uk>

ChildLine is a free and confidential helpline offering general help and advice. Children and young people in the UK can call 0800 1111 to talk about any problem, 24 hours a day. For further information, see the ChildLine website. <http://www.childline.org.uk>

This guide has been written by the children's internet charity, Childnet International, and has been funded by Microsoft, The Training and Development Agency for Schools (TDA) and Becta. Childnet International © 2007 Registered charity no. 1080173 <http://www.childnet.com>



Rome Group is a “safe” application that introduces aspects of esafety relating to passwords, plagiarism and online behaviour. <http://www.youngpeoplesafeonline.com>

Dr John Woollard J.Woollard@soton.ac.uk
Lecturer in Information Technology Education
School of Education, University of Southampton

<http://www.pgce.soton.ac.uk/esafety>

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

Chatdanger <http://www.chatdanger.com>

Child Exploitation and Online Protection (CEOP) <http://www.ceop.gov.uk>

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

Childnet International <http://www.childnet-int.org>

Digizen <http://www.childnet.com/digizen>

Get Safe Online <http://www.getsafeonline.org>

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

Know IT All for Parents CD-ROM produced by Childnet <http://www.childnet.com/kia>

Know IT All for Trainees CD-ROM produced by Childnet <http://www.childnet.com/kia>

Rome Group <http://www.youngpeoplesafeonline.com>

Think-u-know CEOP <http://www.thinkuknow.co.uk>