

Know the Jargon:

Authentication - process for verifying that someone/something is who/what it claims to be. Generally done by passwords.

Blog - short for 'web log' or online journal/diary. May contain photos, images and sound and can incorporate comments from visitors.

Chatroom - area on internet or other computer network where users can communicate in real time.

Cookie - small data file on user's local computer which contains info about that user that is applicable to a website, such as preferences.

Cyber bullying - sending or posting harmful or cruel text/images using the internet or other digital communication devices. Examples include:

Flaming - insults which get angrier or more vulgar

Denigration - bully sets up false profile with cruel and false contents

Impersonation - stealing of passwords to send threatening messages

Outing - sending intimate personal information to others e.g. sending photos taken covertly

Filtering - method used to prevent or block users' access to unsuitable material on the internet.

Firewall - network security system to restrict external and internal traffic.

Grooming - the way in which someone who wants to sexually harm children gets close to them, and often their families, to gain their trust. Online grooming occurs by people forming relationships with children and pretending to be their friend. This grooming activity may result in meeting a child with the intention of committing a sexual offence.

Instant Messaging - sending short text messages in real time.

ISP - Internet Service Provider.

Social Networking Sites - places where people create a personalised page on the web related to their interests and views, which links to other users.

Spam - unsolicited junk email.

Continued...

Spoofing - assuming the identity of someone else using an email address. Often used to veil the source of virus-laden emails or to obtain sensitive info without identifying the source of the spammer.

Trojan horse - virus that infects a computer by masquerading as a normal program. They have been known to activate webcams

without the knowledge of the computer user.

Virus - computer program that enters a computer, often via email, and carries out a malicious act. It can corrupt or wipe all data in the hard drive including system software. Users are advised to install anti-virus software.

For further information on e-safety visit the following websites:

Child Exploitation and Online Protection(CEOP) Centre - www.ceop.gov.uk

Childnet International - www.childnet-int.org

Department for Education - www.dfe.gov.uk

Get Net Wise - www.getnetwise.org

Insafe - www.saferinternet.org

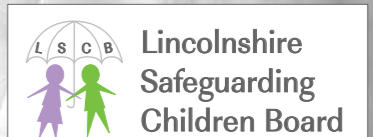
Internet Watch Foundation - www.iwf.org.uk

Kidscape - www.kidscape.org.uk

Online safety for young people and their parents - www.thinkuknow.co.uk

Stop it Now! - www.stopitnow.org.uk

Think U Know - www.thinkuknow.co.uk/parents



A Guide for Parents and Carers Keeping Children Safe in a Digital World

Every Child Matters *In Lincolnshire*



Introduction

'Children are now citizens born into a digital world, growing up surrounded by and immersed in the technology and tools of the digital age.'

While it is clear that technology offers children unprecedented opportunities to learn, communicate, create, discover and be entertained in a virtual environment, there are some inherent risks. And while most children's confidence and

competence in using the technologies is high, their knowledge and understanding of the risks may be low'. (Becta (2008) 'Safeguarding Children in a Digital World')

Parents and Carers can help to keep children safe when they're using technology by having an understanding of the activities their child is engaged in and by helping them to understand the potential risks.

The 3 Cs that may present risks to children using technologies:

Content - children may be exposed to inappropriate content which may upset or embarrass them, or which could potentially lead to their involvement in crime and anti-social behaviour.

Contact - some use the internet to groom children with the ultimate aim of exploiting them sexually. ICT offers new weapons for bullies who may torment their victims, for instance using websites or text messages.

The recent surge in popularity of self-publishing and social

networking sites brings new e-safety challenges, with many young people making available online some detailed – and sometimes inappropriate – personal information, which again raises both content and contact issues.

Commerce - while the internet offers new opportunities for doing business online, it also brings with it many unscrupulous traders to whom children and young people may be particularly vulnerable.

Continued...

Children need guidance in developing their own set of responsible behaviours to keep them safe when online, but equally they should know that, if things go wrong, they can seek

help and support from any trusted adult.

(Becta (2008) 'Safeguarding Children in a Digital World')

How can you help your child to keep safe when using technologies?

- Familiarise yourself with the technology your child uses. Talk to them about the activity they've been involved in (e.g. interactive games) the way you might talk to them about a book they've read or a party they've been to.

- Encourage your child to introduce you to online, instant or text messaging friends as they would with their usual friends.

- Restrict your child to moderated chatrooms. These are supervised either by a person or technology to make sure that the 'chat' is suitable. If your child uses instant messenger make sure that they know exactly who is on their friends list. Teach your child not to reveal their

mobile phone number if they are sending text messages from the internet.

- Teach your children not to give out personal information about themselves, family or friends such as address, name of school or mobile phone number – anything that would enable someone they don't know to contact them offline. Encourage them to use a nickname when they log on and never give their 'password' to anyone else.

- It is vital that children know that some online 'friends' are not who they say they are. Encourage them to consider whether all the information they receive over the internet is as it seems.

Continued...

- Emphasise the dangers of meeting up with anyone they've only met online. No matter who the person says they are they must never go on their own to meet them.

- Bullying online or via text messaging is as serious as any other form of bullying. Encourage your child to block abusive messages, leave the chatroom or report abuse using the 'report button' or by contacting the moderator or ISP customer services. If your child is being harassed contact the Police.

- Use internet filtering software to limit access to unsuitable sites and material, such as content control on Internet Explorer

- Always have oversight of any computer being used by younger children. This will help them to develop safe use of the internet to protect them as they get older and want more privacy.

- Children should always ask your permission before buying anything on the internet. Don't give them your credit or debit card details but help them to fill out any online

forms. Only buy from well-known companies or try to check out the online shop details before passing on your own. Only pay through a secure connection; check for the little padlock or key at the bottom of the web page.

- Let your children know they can tell you if anything makes them feel uncomfortable or concerned when using technology, even if they have done or said something that they are embarrassed about. We all make mistakes.

- If you discover illegal activity this should be reported to the Police. Illegal content should be reported to the Internet Watch Foundation (IWF) and/or Police. If a child is believed to be at risk this should be reported to the Child Exploitation and Online Protection (CEOP) Centre but the Police if a child is at risk of immediate danger.

