

E-safety booklet

This booklet is about how to stay safe when using the internet and other forms of electronic communication. It is designed for families, settings like schools or youth clubs and young people themselves. We hope it gives useful advice and information.

The booklet is part of a series of resources covering this issue. It has been produced by the Medway e-safety team at Gun Wharf, Dock Road, Chatham, Kent ME4 4TR.

Contents

Introduction	Page 3
Internet use by young people	Page 4
The potential for harm:	Page 5
Bullying	
Viruses, images and pop ups	
Online predators and grooming	
Social networking	Page 6
Webcams	
Case study	Page 7
Advice for parents and carers	Page 8
Advice for children and young people	Page 11
Advice for schools and clubs	Page 13
Appendix 1: Further help and advice	Page 14
Appendix 2: The law	Page 15

Introduction

The internet has changed the way we live. We use it for shopping, games and leisure. Many people go online to keep in touch with friends and make new ones.

Like everything, the internet has a downside. Reports of fraud and identity theft are common. However, the biggest worry for most people is the threat to children.

There are several ways in which children can be affected by things they do or see online:

- They may be exposed to adult material such as pornography
- They may accidentally give away private family information like names and addresses
- They may encounter adults who encourage them to do things that are not safe or legal
- They may send photographs or messages which can be taken and used by other people
- They may be the victim of bullies who use things like email or text messages to hurt and intimidate.

We should not allow these threats to frighten us or prevent children from using the internet. By following some simple ideas we can protect ourselves and make the internet a safe and fun place.

This booklet covers five topics:

- The type of site used by children and what the risks are for each
- Advice for parents and carers
- Advice for children and young people
- Advice for schools and other places like youth clubs and libraries where children go online
- Where to go for help if you are worried or if you want to know more.

Internet use by young people

It seems odd to imagine a world without the Internet but it has actually only been widely accessible since the early 1990s. Because it is so new, many parents or carers have not really got to grips with everything that is now available online. This section explains a little about the most popular ways in which children and young people use the internet.

Social networking sites are a way of keeping in touch with friends. These are a bit like electronic diaries, in which users can record their day to day lives, post photographs of themselves, join groups and send messages to their friends. Popular networking sites for teenagers include:

Bebo – www.bebo.com

Facebook – www.facebook.com

Flixster – www.flixster.com

MySpace – www.myspace.com

On all of these sites young people can invite others to become their “friend.” Once an invitation to be a friend has been accepted, then both people can see each other’s details.

Younger children enjoy sites like Club Penguin – www.clubpenguin.com or Habbo – www.habbo.co.uk . These are slightly different to social networking sites in that users create cartoon “characters” for themselves, which can then interact with others using the site.

Instant messaging programmes like msn or gmail are sites where young people can “talk” in real time by typing message to one another. These messages appear on the screen and a user then types a reply. In most cases a chat can only happen between people who are members of a contact list – such as friends from a class at school who have shared their email addresses with each other.

Emails are a slightly slower method of messaging in that there is no instant response; instead they have to be opened, read and replied to. All young people in state schools have a school email address but many also have an address with providers like Yahoo, Hotmail, gmail or msn. All of these accounts will allow the user to access instant messenger services linked to the provider – so for example someone using Yahoo email will also be able to use Yahoo Chat.

Using a mobile phone allows people to send **text messages**. These allow people who know a mobile phone number to contact the owner whenever the phone is switched on.

The potential for harm

Bullying

All of these facilities are available 24 hours a day and it is therefore possible for a bully to reach his or her victim whenever they like. Forms of electronic bullying can include:

- Posting offensive or hurtful messages on a social networking site and encouraging other people to do the same
- Sending abuse during instant message sessions
- Creating fake “friends” on social networking sites and encouraging the victim to enter a relationship and send messages which are then made public and mocked
- Sending abuse via email or text message

These are particularly harmful in that they reach the victim in his or her own home, where people generally feel safe. As so many people can view an internet page, the victim can feel exposed and humiliated.

Viruses, images and pop ups

Viruses and other electronic problems can all be sent to your computer via the internet. They can be sent in many ways, particularly as attachments to emails. Opening the attachment allows the virus to spread to your machine.

Some website links may look innocent from their titles, but clicking on them brings up explicit images. Pop-ups are just that; little boxes which appear on the screen, often advertising sexual or other illegal services.

On-line predators

It is a sad fact that those adults who have a sexual interest in children can use the internet to find and befriend potential victims. There are several ways in which a predator can do this. Most of them rely on the innocence of children, especially a child’s belief that they can “tell” if someone is not who they seem. The anonymity of the internet also makes it easy for a predator to create a fake identity with which to fool potential victims.

Most people have heard the term “grooming” but may be unclear as to what it means. The Sexual Offences Act 2003 defines grooming as:

“A course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes.”

Predators can also manipulate images of children that are posted online. An innocent photo can easily be turned into something more sinister which is then traded amongst paedophiles.

Once a photograph has been put online it can never be retrieved, no matter how quickly it is deleted. Some predators spend hours simply trawling for random photographs which they download to their own machines and then trade with other people who share their interest in children. A photo of a baby in a bath could be seen all over the world by complete strangers.

Social networking sites are popular with predators as they can learn a great deal about a child just by reading his or her profile. For instance many young people display their full date of birth, thus helping anyone to work out how old they are. A predator can also learn a lot by looking at the friends and hobbies that the child has listed on their page. An adult can then approach the child (often pretending to be another child) by claiming to be of a similar age, background or to share an interest.

There is a craze amongst young people to have the most “friends” on their social network. To get a “friend” a user sends that person an invitation. They will often try to get more friends on their list by sending invitations to people they don’t know. Once the invitation is accepted the new “friend” can see detailed information on the child’s profile, which usually includes their email address as this is needed to sign into the site. Of course this also works in reverse, with young people willingly accepting invitations they have been sent by people they don’t know.

Most sites are **password protected** but in practice this can offer little protection. Most adults are predictable in choosing passwords, and the same is true for children. It can be easy for a predator to guess what a child’s password is, just by reading the profile. For example, a child may write about his or her favourite pop star, making it a reasonable guess that the password is the star’s name.

Once the predator knows a password and username, he or she can assume a child’s identity and log on in their name. The real child will not be able to get online in the meantime. Once logged on under the child’s identity, the predator will be able to contact anyone on that child’s friends list. Other children will not know that it is not genuinely their friend who is getting in touch with them.

Once trust has been built up, it is easy for the predator to manipulate a child into unsafe acts. For example, he or she may suggest meeting the child or persuade the child to strip in front of a webcam.

Webcams allow a child to send moving images of themselves via the internet. Once any image, moving or still, has been put on line it is available for anyone to see and download onto their own machine.

This fictional case study shows just how easy it is for a predator to find out detailed information about a young person.

Katy Jones is 12 and loves her puppy, Fudge. Her Bebo page includes lots of photos of her and Fudge together, plus pictures of her recent birthday party which was held at a local swimming pool. She also has photographs of herself in uniform at her school's open day. Her profile shows that she lives in Chatham and her email address is given as KatyJ1996@hotmail.com. She has pictures of several friends on her page, all of whom are named in the captions Katy has put by each photo.

From this seemingly innocent information a predator could do the following:

- Identify which school Katy attends, and from that guess at the area of Chatham in which she lives
- Use Google Earth to view the area and pick out any distinguishing features
- Download photographs of a 12 year old girl in a swimming costume
- Create a fake identity on Bebo and make friends with Katy by pretending to be another 12 year old girl - using Katy's interest in dogs to strike up a conversation: "I love the pics of you and Fudge! Where do you take him for walks?"
- Use other information (such as the school's website) to build trust – "I live in Chatham too! Your school is the one with the big trees in the playground, do you like Miss Smith the headteacher?" or "I know your friend Lucy, I hope she likes her new house..." (Remember that Lucy's information will also be visible.) From this a predator can lead into more dangerous areas, such as suggesting that he and Katy meet in person
- Most social networking sites use a member's email address as the username. A predator would be able to use personal details to guess at Katy's password – children are predictable and there is a good chance that her password is Fudge. Once logged in as Katy, none of her friends will be able to tell that messages do not actually come from her, which of course makes them vulnerable to exploitation.

Once trust is established, a predator can then lure a child into dangerous behaviours. This may not necessarily involve meeting in person, although this is the most well-publicised outcome. Predators may have an interest in photographs or images of children which they either keep for personal gratification or else trade for other images. So in our example a predator could create a page in the character of "Sally," another 12 year old girl, and as such encourage Katy to send inappropriate photos or webcam pictures. Children are very trusting and predators know how to exploit this. For example, "Sally" could pretend to be worried about her physical development

and ask Katy to reassure her by showing images of her own body. Once Katy has sent these images, she has lost control of them for ever. She could also be persuaded to meet “Sally,” only to find out too late that “Sally” does not exist.

Advice for parents and carers

Get to know the sites your child uses.

You are not alone if this is a daunting prospect! Many adults feel nervous around new technology. The section on page 4 (“Internet use by young people”) should help you understand a bit more about how the internet can be used.

The “Think You Know” website has lots of really good information for parents and carers. You can find it at www.thinkyouknow.co.uk . Click on the section marked “Parent? Carer?” to find out more.

When you feel confident, you could ask your child to show you around his or her favourite sites. Try saying something like: *“I keep hearing about this thing called Club Penguin. It sounds brilliant. Do you use it? Can you show me what it’s about?”*

This approach is good because it puts the child in charge and makes him or her feel that you are treating them with respect. It also avoids the feeling that you are checking up on what they’re doing – instead, you are asking because you are interested. You will also be able to see what your child is doing now, and to understand if they are taking any risks.

Being open and supportive from the start will make it much easier for the child to come to you if they have any worries later on.

Understand the risks

The CEOP site is a great place to look for information on what can go wrong and how you can protect children. The site is split into areas for each age range and features various games and activities designed to help children learn how to stay in control. Looking at the site with your child is a good way to introduce the subject. Remember that adults can be victims as well – crimes like identity theft are increasing, so tell your child that you are learning together.

It’s important to keep things in perspective and not frighten your child. Most of the people they will meet online are fine. As long as we are sensible and take steps to protect ourselves, the internet is a great place to be.

Invest in virus and pop-up protection

Most computer stores sell software that will protect your machine from electronic threats. Some systems can also be downloaded free from the internet.

Make the internet part of the family

If at all possible, have the computer in a main room, not a bedroom. This makes it easier for family members to share in what's going on. It also makes it easier for a child to show an adult if something happens to scare or hurt them.

Webcams are great tools to have but don't have them in a child's bedroom. A child is much less likely to carry out illegal or dangerous acts on webcam if the camera is somewhere public like a living room.

Know what to do if things go wrong.

When your child tells you that something bad is happening, try not to ask too many questions. Let the child tell the story in their own words. Don't praise the child for being brave as this can encourage exaggeration.

Any messages or images should be kept, however upsetting they may be. They will be important evidence.

You need to tell the child that you cannot keep the matter a secret and that you have to tell people who can help. Explain that this is to stop any other children being hurt.

If the problem is bullying messages sent by a classmate, you can take the matter up with your child's school. Every school by law has to have an anti-bullying policy and you are entitled to see it. You could ask for a meeting with your child's teacher or the Headteacher. If you are not happy with the response you can make a formal complaint. All schools have to have a complaints procedure which they must show you on request.

If the messages are either encouraging your child to meet someone or you are suspicious that they are "grooming" your child, you can either report the matter to your local police or else use the "Report Abuse" section of the CEOP website. Reports can also be made from other sites which show the Report Abuse Logo.



Think about how to talk to your child

Whenever you need to talk to a child about something important, it can be hard to know where to start. Build up to the subject gradually and at a time when the child is ready to listen. Try not to make a big deal out of it. Think how you'd feel if someone said "Come here right now, I want to talk to you about danger on the internet!" This sort of approach is scary for the child and builds a lot of barriers, because it makes it harder for you to talk about the internet as a place where it's possible to stay safe and have fun.

The next section of this book was written to be used by children and young people. You could try leaving these pages with your child as a reminder of the things they can do to protect themselves online.

There are lots of adverts on television dealing with identity theft. You could use these as a way to introduce the subject – after all, adults are at risk too.

Talking to older children and teenagers

This age group may be defensive when anyone tries to point out the risks. They often feel that they know everything about technology and that they can look after themselves. Try explaining that you are treating them as a young adult by giving them the knowledge they will need to protect themselves, and that you hope they can help other young people who are less mature by sharing the information with them. It can also be helpful to point out that by following simple rules such as not opening attachments they don't recognise they can protect their machine and systems.

Teenagers often feel that they can "tell" if someone is lying to them online. If this happens, ask them to visit Facebook and look at these profiles:

<http://www.facebook.com/profile.php?id=1197268201>

<http://www.facebook.com/profile.php?id=1301412984>

One of these profiles is false and was created for training purposes. Ask your child if they can tell which one is the fake. (Answer on the back page of this booklet.)

Reassure, don't blame

Above all, make it clear that you do not blame your child for anything he or she might have done on-line. Predators are very, very skilled at manipulating young people, who are often drawn into something they don't like and don't realise until it's too late. If your child knows you are going to be supportive they are far more likely to tell you when something is wrong – so you can help them in time.

Advice for children and young people

You might have heard things about criminals, bullies and other nasty people who use the internet to scare or hurt children. This section will give you some ideas on how you can stay safe and still have fun.

Don't be scared about going online. If you are careful you will be able to protect yourself from the bad stuff that can happen. These ideas will help.

Don't give away any personal or private information. If you set up a page on a site like MySpace, don't give lots of detail about yourself. Here are some of the things you should keep secret:

- Your full date of birth – it would help someone work out how old you are. It's okay just to say something like "June 4th" but don't give the year
- Your school – remember that someone could work this out if they saw a picture of you in your uniform!
- Where you live - it's okay to say Medway as that's a big place. Don't say things like "Chatham High Street" as that would make it easier for someone to find you
- Your email address – if you need to show it make sure it doesn't give your name or age away. So instead of Katie.smith1994@hotmail.com use something like Hidemy.name@hotmail.com

Check your privacy settings. Make sure only people you know and trust can see your full profile.

Don't share contact lists. Your details could get passed on without you knowing to anyone in the world – and this person can then see all your friends' details too.

Think about the photos you post. Would you really want a complete stranger seeing them? Remember too that even if you don't mind a photo being posted, anyone else in the photo might not want it to go online. If you're posting a group shot, check with everyone else first.

Think about the messages you send. You might think something is just a joke, but unlike face to face communication, you can't be sure how it's making someone else feel. Your joke might be very hurtful or cruel to the other person.

If something happens that makes you feel scared or worried, tell an adult you trust and ask them to tell the police. If you can't do that, use the "report abuse" on the CEOP website.

If you get friendly with someone online, it's only natural that you will start to think about meeting them face to face. Never meet someone for the first time by yourself – always take a trusted adult with you. If the other person is genuine, they won't mind. It's a sign that something is wrong if they insist that you go by yourself.

Trust your instincts. If you think something might be wrong, tell an adult you trust and ask them to help you. They could:

- Read the messages you get and help you decide if they're okay;
- Help you set your privacy settings or block someone who's been bothering you;
- Help you report things to the police if you decide that is what needs to be done.

Tell your friends about the risks and tell them how to protect themselves like you do. Spread the word by showing them this book, or else go to the CEOP website at www.thinkyouknow.co.uk for more ideas and advice.

Advice for schools and clubs

Children and young people may think that they are safe when using the internet at school or their club. However it's still important to take steps to protect both them and the school or club from potential risks.

- Ensure that filters are set to high security
- Don't allow access to networking sites (eg MySpace) via your system
- Make sure that all children or young people in your setting are aware of the CEOP "report abuse" symbol. Show them how to find www.thinkyouknow.co.uk
- Ensure that you are following safer recruitment procedures
- Review your anti-bullying policy to ensure it covers electronic bullying
- Review your IT policy to ensure it covers staff use of the internet. Members of staff need to know what is acceptable usage of school/club computers. Remember that downloading adult pornography is not illegal. What would you do if you found it on a colleague's laptop?
- Ensure staff know that they should not take personal information off-site – for instance on laptops, data sticks or CDs
- Ensure staff know what to do if they encounter abusive or indecent images of children or young people. These should not be printed off as this is technically possession. Instead, use the Report Abuse button to report the matter to CEOP.

Appendix 1 - Further sources of help and advice

- Internet watch – www.iwf.org.uk - this is a general site which offers advice and guidance, together with a chance to report illegal web content. Although abuse can be reported here, the IWF also investigate other crimes such as spreading obscene material or content that is likely to incite hatred.
- CEOP – there are two strands to the CEOP site: www.ceop.gov.uk is the formal area, in which details of their work are available together with information for parents, carers and teachers. Their other site is www.thinkyouknow.co.uk which is where children and young people can play interactive games and learn how to take control of their technology.
- National Society for the Prevention of Cruelty to Children – www.nspcc.org.uk is the site for this child welfare organisation, which offers advice on a range of issues, including abuse, neglect and online safety.
- Childline – www.childline.org.uk is a site where children and young people can get advice about topics like body image, bullying and divorce. There is a section on online safety and children can use the site to report anything which is scaring or harming them.
- School Child Protection co-ordinators can be contacted via the school office. There may also be a Home School Support Worker, or Family Liaison Officer, who will be a further source of help.

Appendix 2 - The Law

Many young people (and indeed some adults) use the internet regularly without being aware that some of the things they do are illegal.

The law is developing rapidly in this area. The main pieces of legislation at the time of writing are shown below but please note that this section is not professional advice. If you have any questions about the law, you should speak to a solicitor.

The Sexual Offences Act 2003

This introduces new offences of grooming (see page XX for a definition). In relation to making/distributing indecent images of children, this Act raised the age of the child to include anyone up to 18 years of age.

An adult who makes a child under 16 watch a sexual act (including looking at images such as videos, photos or webcams) for his or her own gratification, is committing an offence.

It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. "Position of trust" covers people such as teachers, social workers, health professionals, and Connexions staff.

Anyone who has sexual intercourse with a child under the age of 13 commits the offence of rape.

The Racial and Religious Hatred Act 2006

This Act creates new offences involving stirring up hatred against persons on religious grounds.

The Police and Justice Act 2006

This extended the reach of the Computer Misuse Act 1990 making denial of service attacks (ie hacking) a criminal offence.

Communications Act 2003 (section 127)

This Act covers using the internet to send messages or other matter that is offensive, obscene or indecent. The exact wording is: *Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.* This wording is important because an offence is complete as soon as the message has been sent. There is no need to prove any intent or purpose.

Data Protection Act 1998

The Act requires anyone who handles personal information to protect data relating to any living individual. The Act also grants people the right to see their personal data, to compensation if it is misused, and to prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of anyone's motives, the Act makes it a criminal offence to do the following:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a criminal act (such as fraud); or
- impair the operation of a computer or program (for example spreading viruses).

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. It is illegal to adapt or use software without a licence or in ways prohibited by the terms of the software license.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing threatening written material. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers "fake" photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not harass another. A person whose behaviour causes another to fear, on at least two occasions, that violence will be used against him or her is guilty of an offence.

The Regulation of Investigatory Powers Act 2000

This act regulates the interception of communications. It is an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.

Answer to the Facebook profile question on page 9: Both profiles are false and were created for training purposes.