Surfing Safely -

Your Family's Guide to Internet Safety

family information service warwickshire

Warwickshire County Council

Working for Warwickshire

Introduction

The Internet is a wonderful and diverse place, filled with incredible information resources. Yet for many parents and carers, who often have less knowledge and experience of the Net, it can be a place of concern. We worry about what or whom our children may encounter online, and how we can protect them with our own limited knowledge.

While we use it for booking holidays and answering emails, your children are setting up social networking pages, instant messaging with webcams, blogging, researching school projects, listening to music, playing online games and emailing friends.

Most children use the internet safely and responsibly and we shouldn't therefore lose sight of the Nets' positive aspects. As parents, we need to balance our concerns about their safety online with empowering them to explore and make the most of this wonderfully rich resource, safe in the knowledge that they can talk to us about anything they may run into.

In clear, simple language, this booklet explains to parents what children already know or need to know about the online environment as well as providing advice about how you can protect your family, allowing them to use the Internet safely and securely while having as much fun as possible.

So How Do Your Kids Use The Internet?

Early Primary School Children (ages 5-7)

This is the age when many children are introduced to the Internet. A child's first use of a computer may be at school while others may get their first computer experience at home learning from parents or older siblings.

Young children are often completely engaged by simple games and educational sites, but they quickly learn about new sites from their peers.

Ideally, when your children are this age, you will be actively involved with their online activities in the same way that you are with their homework. For example, you should make sure the computer your child uses is within your view and set up in a family room.

It's a good idea to set the home page of your Internet browser to a child-friendly home page for younger children and consider bookmarking a range of sites which you are happy for them to view. Show them how to access these from a Favourites folder which you can set up with their name. To access these services, click on Tools button at the top of the Browser.

Parental control software can help you by limiting the sites your child can access, even when you aren't around. The controls also limit any information you don't want your child sharing, whether it be their name, age, phone number or any other private information.

Early Primary School Children (ages 5-7) continued...

You should turn on all the filtering and security features in your computer's search engine (such as Google's "SafeSearch" feature, found under "Preferences") to prevent your young child from inadvertently arriving at an adult or other inappropriate site as they do their homework.

Be sure to show your child how to close a browser window and let them know it's always okay to close a site if something surprising or disturbing occurs. Tell them never to chat, type messages or share information with anyone on these sites unless you are with them.

Parents' checklist: what you should do:

- Limit approved Web sites and hours spent online
- Set high security settings with browsers, membership, and social networking sites
- Install and maintain Internet security software and parental controls
- Use parental controls to limit the Web sites your child can visit
- Monitor your child's computer use and sit with them when they're online, wherever possible
- Talk about protecting private information (name, phone number, etc.) and never sharing passwords with friends

Tween Children (ages 8-12)

Tweens are far more social and adventurous in their computer use. They talk to their peers at school and learn about the newest and "coolest" sites.

They might sign-up for their first email and Instant Messaging (IM) accounts. Ask your child about those accounts and what the passwords are, so that you can monitor their activities, and find out who they are communicating with.

Children at this age may also start to check out social networking sites, such as MySpace, Piczo and Bebo that are popular with older teens and adults.

Tweens are also interested in music and the Internet is an easy way to meet others who share their musical interests.

Online video sites, such as YouTube are enormously popular. Many of the videos contain strong language or violent material, so you need to monitor your tween's visits carefully.

Parents' checklist: what you should do:

- Set rules about online communication, illegal downloading, and cyber bullying
- They should know to never click a link in an email or Instant Message - this is a common way people get viruses or reveal private and valuable information to criminals
- Discuss risks and concerns about posting and sharing private information, videos, and photographs
- Watch for signs of obsessive or addictive online behaviours (see Online Gaming and Signs of Addiction)
- Keep computers in a common area in the house
- Encourage open communication and encourage your kids to tell you if anything online makes them feel uncomfortable

Teens (ages 13 – 17)

Teens are developing ever greater independence and this is reflected in their online lives. With that independence comes responsibilities, including being careful in their online world.

At this age teens have usually formed or joined online worlds such as MySpace, Facebook, Bebo and others. With screen names, memberships, blogs, profiles, and other Internet elements that they visit daily, teens communicate the details of their lives with each other.

Web sites are also frequently used for the research and submission of home work for school. Digital traces of their thoughts and activities can be left all over the Web. Often they don't know - or they forget - that everything posted on the Web is there for all to see, and it's probably there indefinitely.

All it takes is a single Google search by a University or college admissions director or potential employer – five, ten even twenty years from now – and all of the photos, opinions and thoughts of your teen are there for all to see forever. Caution is so important!

Parents' checklist: what you should do:

- Reinforce rules of appropriate online behaviours (language, private information and imagery, cyber ethics, illegal downloading, limiting hours of usage, and avoiding inappropriate adult sites)
- Be aware of your teen's online life (social networking sites, photographs, private information, club and sports activities) whether on their site, a friend's site or their school's Web pages
- Review the sites your teen visits; don't be afraid to discuss and possibly restrict sites that offend or concern you
- Ask them not to download files (music, games, screensavers, ringtones) or make financial transactions without your permission
- Teach them to never share passwords and be wary about typing private information when on a shared or public computer, or one they think might not be secure
- Teach them to never click a link in an email or Instant Message - this is a common way people get viruses or reveal private and valuable information to criminals
- Keep computers in a common area in the house and not in your teen's bedroom
- Encourage open communication and encourage your teen to tell you when something online makes them feel uncomfortable. Remember, they are teens but they still need your support, involvement and care
- Remind your teen to take responsibility for keeping Internet security software maintained and up-to-date, as much as for their protection as yours

Follow the Rules

Parents

Remember these top tips for staying safe online:

- Take an active interest in what your children are doing online
- Remember children are accessing the Internet at school, friends' homes, libraries, Internet cafés, etc
- Encourage your children to speak to you if they see anything that upsets them online
- Remind your children never to give out personal information
- Children should never meet up with anyone they've met online without a trusted adult being present
- Encourage your children to be responsible Internet users
- Stick to the fun and positive sides of the Internet

Children and Young People Follow Childnet's SMART Rules

S afe. Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address, or school name - to people who you don't know or trust online.

M eeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

A ccepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.

R eliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.

T ell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at **www.thinkuknow.co.uk.**

Online Safety – The Basics

Safe Browsing

Make sure your browser is set to offer you its built-in security and safety features. For example, Microsoft Internet Explorer (the most popular browser) offers security and privacy settings. These are found under "Tools," then "Internet Options."

Popular search engines such as Google also offer some safety features. For example, Google's "SafeSearch", found in "Preferences" on the main Google landing page, allows you to restrict explicit (sexual) sites and content from appearing in your family's search results. Of course, any knowledgeable user can easily remove the setting, but it's helpful with younger Web surfers.

Protect Your Password

Avoid using easy-to-guess passwords such as dictionary words, names, or dates such as your birthday that your child or an internet hacker might break.

Make sure you have your child's passwords for email, IM, even social networking sites. It's a good idea so you can review who is communicating with your child and in the event of trouble, you'll have important access.

Secure Your Wireless Network

Home wireless networks present other security problems, and there are simple steps to follow to ensure that they are secured from unknown intruders who might use your bandwidth, or worse, host their spam and other attacks from your system.

If you have wireless (or "wifi") at home, make sure you do everything possible to make it secure: reset the router password so it isn't easy to guess; enable wireless encryption to prevent a stranger from spotting your network from the Internet; restrict the access your system shares on the network and make sure your Internet security software is kept up-to-date.

Parental Control Software

Parental control software enables you to choose where your child is able to go online, and to ensure that they don't view inappropriate subject matter.

Parental controls differ depending on the application offering the feature. Usually there are varying levels so you can customise the program according to the child being protected.

Remember, though, that no software provides perfect protection. Parents need to use a combination of tools and rules to protect children, regardless of their age. The Internet is a rich resource, and it defeats the purpose to lock it down entirely. Parents need to talk with their children to ensure that their beliefs, morals, and values are upheld when their children go online.

Online Favourites

Social networking sites like MySpace, Facebook and Bebo are extremely popular with teens. YouTube is popular but a parental concern because there isn't any filtering for language or adult content. Ask your teens if they have accounts (but always try to check for yourself too).

Whether your kids are teens, tweens, or younger, ask them about which sites are popular with them and their friends. Ask them which ones they've joined and have them show you around. You'll quickly know whether you approve or not. Keep the conversation "impersonal" so they don't feel they are being interrogated.

Online Risks

Internet Predators

It is rare that your child would be approached by a sexual predator online, but there have been enough high-profile cases with tragic outcomes that would make any parent worry about this.

Make sure your children know they must never email, chat, or text message with strangers. It's never okay to meet a stranger offline or online. Make sure they understand that someone they see or meet online is still a STRANGER, no matter how often they see them online.
Children who discuss sex with strangers online have been shown to be more likely to arrange offline meetings. It's very important that you tell your children that it is never acceptable to talk about sex with a stranger online and that they should notify you or a trusted adult immediately or report this if it happens.

You can report suspicious activity towards your children on the Internet to the Child Exploitation and Online Protection Centre (CEOP) **www.ceop.gov.uk** which has a special young person's reporting service called 'Think you Know' - see **www.thinkuknow.co.uk.**

Plagiarism and Cheating

It's very easy to find homework guides to all the popular school textbooks online and many Web sites offer essays and thesis papers for sale. Cheating has never been easier, more available and more tempting to our children. Remind your kids that it's very important to use the Internet for research but not for copying.

Encourage your children to always check the source of information they read on the Internet and explain why user-generated content, such as that found at Wikipedia, can serve as a great starting place for new research but isn't always reliable.

Cyber Bullying and Cyber Stalking

Technology gives our children more ways to connect, socialise, and communicate than ever before. Unfortunately, some kids use email, Instant Messaging, and mobile phone photos and text messages to embarrass or bully other children. Children's digital messages can also be edited to change the meaning then forwarded to other kids to embarrass, intimidate, or insult.

Make sure your children know they must guard even the most casual text message and watch their own written words. They should never retaliate back to the bully, and they should always tell you if and when they are being cyber bullied.

Keep a copy of any bullying message by using the "Print Screen" key on your computer keyboard and copying the message into your word processing program. It's important to help your child know where and how to report if they are the victim of cyber bullying and there is specific advice for schools at **www.digizen.org**

Cyber stalking is a dangerous extension of cyber bullying and used by those who engage in stalking in the real or "offline" world. With awareness of the issue, our older teens can learn to defend themselves and parents should know how to help.

The stalker may hijack an email account and pose as the person whose email they've hijacked. The attacker might deface a social networking page or send hateful messages to the victim's friends, engage in outright identity theft, or try to destroy somebody's credit and reputation.

Cyber stalking is dangerous and should be reported to the police, Internet service providers, and Web site hosts. Keep all evidence of both cyber stalking and cyber bullying.

File Sharing, Music and Video Download

Children quickly learn about the joys of sharing music with each other. And it's often at the tween stage that they discover file-sharing sites, which enable them to swap music or videos online.

Explain to your children the dangers of file-sharing sites and programs, which can let strangers have access to your computer. Using file-sharing sites may expose your computer and information to "bot" software, spyware, keystroke loggers, viruses, and other dangerous malicious code. Additionally, downloading music or videos for free is often illegal. Show your children where they can legally download music and video from sites such as iTunes.

Private Information and Identity Theft

Many children will not automatically know what "private" information is and the importance of keeping this private both online and offline so you need to explain the concept that it's any data that individually identifies them and may allow a stranger access to personal or financial information.
Private information includes real world data such as, names, telephone numbers, addresses, sports club, school, even the name of a doctor.

Fraudsters can turn even a small clue into a full record on a child and parent. They, in turn, can trade and sell that private data to make money. It's surprisingly easy for people with such intentions to apply for credit in your child's name and get real world merchandise and money, while ruining the child's (or your) credit rating and good name.

If you do suspect you've been a victim of identity theft, you are entitled to request a report from any of the credit reporting services for a small administrative fee (the UK Data Protection Act credit reporting services are allowed to charge £2 for each request an individual makes for his or her statutory credit report): Equifax, Experian, and Callcredit all follow this.
Once you find evidence of identity theft, you will need to report it to the police. That police report will strengthen your case when you work with the other sites and companies involved.

continued ....
You can also put a "freeze" on your credit record and those of your children to prevent strangers applying for credit in your names. Visit http://**www.ico.gov.uk** for more information.

Social Networking Sites

Social Networking Sites are among the fastest growing phenomena on the Internet for children, young people and adults, but it is tweens and teens who are driving that growth. Among the most popular social networking sites are MySpace, Facebook and Bebo. All of them provide a place for kids to get together online with new and existing friends. When used sensibly, these sites offer great ways for kids to communicate and share their experiences. When used carelessly, however, they can expose your children to identity theft and predators.

Teach your children to set their profiles to private so that only invited friends can view their information. They should not post private information or inappropriate or misleading photographs. This information, once posted, can become public and can be stored on the computers and Internet history files of others. Even if you remove such information or photos, they may still be out there on the Internet and in the hands of other people.

Social networking sites enable kids to form networks of friends who can communicate freely with one another. Make sure your kids don't allow people they don't know to join their networks.

Once strangers are in the network, others in the network will assume a level of trust with them, based upon their relationship with your child. If the stranger is a predator, they may try to take advantage of your child or the friends within the network.

Make sure your child sets the communication features properly so they can approve any postings to their page. This limits even a good friend's opportunity to post an embarrassing but funny photo, or make a remark you and they would prefer not to be seen.

Pornography, Gambling, Racism, Anorexia, & Hate Sites

The darkest corners of the Internet world include some dangerous and illegal elements. Without parental controls or browser filters, it's almost inevitable your child will run into something you and he/she will find upsetting. Make sure your child knows to tell you when and if that should happen and reassure them you won't be angry if it does.

Some children and teens may become curious about sites featuring racist or hate messages, or promoting risky or damaging behaviours such as anorexia and self harm. You may only discover this by regularly checking your computer's browser history. Even a single visit should prompt you to talk to your child about it. Don't assume it was idle curiosity.

Explain your house rules about such sites and ask your child about their motivation for visiting. As you talk, if your child reveals issues, such as depression or self-loathing, don't delay in getting your child professional help to deal with such matters.

Teen Online Privacy

Teach your teens about the Internet. By now, they should know that people online aren't always who they say they are. It's easy to lie about your age, sex, and location online, so many people do it for innocent and not-so-innocent reasons.

Continually remind your teens that they can't trust strangers online any more than they can in face-to-face contacts. They should never allow a stranger to join a buddy list or a chat or IM conversation. And they should never accept free software, ring tones, or screen savers from strangers.

Remind your teen that email addresses, user account names, and Instant Messaging handles should not be their real name, the name of their school, or some combination of the two; they shouldn't be provocative or otherwise inviting to a predator. They should be as anonymous as possible. Also, they should never share a password, even with a friend.

Email and Instant Messaging

Make sure your children's email accounts have the highest level of spam filtering turned on. According to a recent research study, 80 per cent of children report receiving inappropriate spam on a daily basis. Your children should use email account names that can't lead strangers to them. For example, they shouldn't use first and last name combinations. They also shouldn't use suggestive screen names or addresses, even if it seems "cool" to do so.

Make sure they use strong passwords that are never shared, even with friends. You should know your children's email account passwords so you can monitor their activity frequently. Look at who they send email to and receive email from. Do you know everyone? And let your child know you will be doing this to help keep them safe and not because you don't trust them.

Key Recommendations for Parents:

- Teach children not to click on links within emails that they receive, since links can lead to fake Web sites
- Disable the preview function in email. This prevents potential malicious code in the message area from executing
- Kids should not respond to emails or instant messages from anyone they don't know or didn't expect to receive
- Never accept a link or download a file through Instant Messaging
- They shouldn't make their Instant Messaging profile or social networking page public
- Set Instant Messaging preferences to keep strangers at bay
- They should always log out when not using IM or when editing their social networking page to make sure their privacy is protected

Blogging

A blog is an online journal or diary. Often teens have blogs that are more like traditional private diaries - except they are open to everyone on the Internet via the teen's own Web site or on a social networking site - which is like placing their diary online for the world to see.

Children should be careful with regard to the content that they post onto their blogs. Search engines can usually pick up the information that is posted and people such as potential employers or school admissions officers may read your blog, and this exposure may affect other areas of your life as well. For example, people interviewing for jobs have been declined because of items in their personal blogs or in the blogs of friends and family that mention them. Don't let your teen become a blog victim.

Viruses, Worms, and Spyware

Computer viruses have been around for more than 25 years in various forms. But with the popularity of email and file exchange on the Internet, the distribution of these threats has really taken off. These days many of the bad guys are international cybercriminals, motivated by financial gain through their illegal activities.

Spreading via email, Instant Messaging, infected social networking pages, and file-sharing sites, malicious software (malware) such as spyware, keystroke loggers and bots can cause you enormous trouble.

Spyware and keystroke loggers monitor your normal computer activity and then report your private data out via the Internet to the criminals. Bots (short for robots) are forms of software that can sneak into your computer and cause your PC to send out spam and phishing emails to others, without you even knowing. Bots can also be used to steal your personal information and wreak havoc on your credit including the unauthorised use of your credit cards and bank accounts. Help keep your children and your computers safe by installing Internet security software on your family's computers and making sure it's updated with the latest protection files. Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not a safe risk to take.

Digital Photos and Mobile Phones

Many kids have mobile phones that include a camera and many also have their own digital cameras. Talk to your children about the need to protect photographs online from strangers or even from peers who might use them inappropriately. Remind your children that all photos held on a mobile phone or a social networking site can be copied, recorded, shared and they can end up anywhere. This includes images taken from a webcam.

Make sure your child shows you the photos they are using so you can advise them about anything you deem risqué or not appropriate for sharing. If you are using photo sharing sites, such as Flickr, make sure you don't allow others to use your photos, especially photos of people.

If your child is using Bluetooth make sure that its's locked, otherwise anyone in the area can access their phone. Remind your child if they have a GPS feature that it enables all their contacts to see where they are. Finally, if they are receiving unwanted calls you should contact the service provider.

Key Recommendations:

- Don't make private photo albums public
- Require visitors to a photo sharing site to use a password
- Back up photos with backup software because computer crashes can easily wipe out your photos and other computer files
- Use only online photo services that provide security protection

Online Gaming and Signs of Addiction

MMORPG - what is that? It stands for the increasingly popular and potentially addictive "massive multiplayer online role-playing games." Titles such as World of Warcraft, Lord of the Rings, and Everquest are currently popular.

These can be highly addictive for some teens, especially boys. Set rules with your children about the amount of time that can be spent on these sites and any other concerns you might have. Signs of addiction to online gaming can be the same as with real-world gamblers, such as craving, withdrawal symptoms, loss of control and neglect of other activities.

And Finally...

The Internet is a wonderful resource, which offers us education, entertainment, news from around the world, and improves our lives with access to tremendous services such as chat, email, online shopping, and more.

By learning more about online risks and dangers, and using up-to-date Internet security software, you can help your growing child navigate this amazing cyber world with increasing levels of independence. Finally, make sure your behaviour online serves as a role model for your children by engaging in safe Internet practices yourself.

Top Tips for Protecting Your Family Online

- Keep the computer in a common room
- Establish rules for using the Internet
- Understand social networking
- Help your children keep their personal information protected
- Protect your children's passwords
- Frequently check your computer's Internet history
- Spend time with your children online
- Teach your children cyber ethics
- Teach your children to tell a parent, teacher, or trusted adult if they feel uncomfortable about anything they've seen on a computer

Acknowledgements:

Much of the information published in this booklet has been reproduced from information provided by the Symantec Corporation, the makers of Norton Internet security and anti-virus software. We would therefore like to thank them for granting us permission to do this.

Free downloadable software to protect your family

Warwickshire County Council is offering all parents of 80,000 school age children a free, groundbreaking e-safety product to make surfing the internet safer for children.

CyberSentinel, made by Forensic Software and already used in over 1500 UK schools will be made available to download free for parents by the county council allowing children to thrive online at school and in the home.

CyberSentinel recognises and monitors keywords that signal danger, providing extra protection for instant messaging, chat rooms, social networks and much more. It is the first time that a product has offered protection spanning subjects such as cyberbullying, gambling, suicide, self-harm and grooming.

The key product features include:

- Time management and access control
- Filtering of web sites (white and black lists)
- Logging of web sites (recording all visited)
- Monitoring chat usage (all sides)
- Word and phrase analysis (from the black list)

A weekly summary is produced for the parent to see all internet activity that has been visited by each child.

Reporting can also be accessed remotely by parents 24/7. This means they can log to their control panel remotely from any PC with internet access and see what their children are doing online at home at any moment – with the ability to change the settings immediately.

For more information about where you can obtain your free copy of the software visit **www.warwickshire.gov.uk/cybersentinel**

Useful Websites:

www.childnet.com
Childnet International's website offers internet safety advice and links for young people, parents, teachers etc.

www.childnet.com/kia
Resources to help educate young people, parents and teachers about safe and positive use of the internet

www.childnet.com/sorted
A website entirely produced by young people for young people and adults on the issues of internet security including how to protect your computer against viruses, phishing scams, spyware and Trojans.

www.digizen.org
Provides information about using social network / social media sites creatively and safely, including advice and guidance on cyberbullying.

www.ico.gov.uk
Provides information and advice on how to protect you and your family's personal information.

www.iwf.org.uk
The Internet Watch Foundation website is the UK's hotline for reporting illegal online content, including child abuse images and racial hatred content.

www.ceop.police.uk
The Child Exploitation and Online Protection Centre's website provides information on how to stay safe online, including a link to the Virtual Global Taskforce that enables parents and young people to make reports of actual or attempted abuse online which the police will investigate.
Thinkuknow.co.uk the CEOP Centre's on line saftey site provide advice and tips to adults and children of all ages.

www.wpthezone.co.uk
Warwickshire Police website offering advice and information on issues such as cyberbullying, internet safety and mobile phone safety to children, adults and young people.

Notes

Other titles in this series include:

Choosing Childcare and Early Years Education
Starting School
Moving on to Secondary School
Encouraging Good Behaviour
Your Child's Learning – Getting Involved
Tackling Homework and Revision
Talking to your Children about Relationships and Sex
Talking to your Children about Alcohol and Drugs
Life with a Teenager
Dealing with Bullying – A Parent's Guide
Dealing with Discrimination - A Parent's Guide
Dealing with Separation and Divorce
Why Dads Matter

If you are looking for any further information or advice for your family the Family Information Service can help you. We offer a free and impartial information and signposting service for parents and carers of children and young people aged 0-20 on a range of topics such as; childcare, benefits, health, leisure and much more. If you don't know who to ask, ask the Family Information Service!

Tel: 0845 090 8044 or 01926 742274
Email: fis@warwickshire.gov.uk
Web: www.warwickshire.gov.uk/fis

follow us on twitter **@WarksFIS**

Like us on Facebook **Warwickshire Family Information Service**

family information service warwickshire

families first

12_12_WM