



A parent's guide to online safety



A huge 62 per cent of parents with children aged between 12 and 15 feel they know less about the internet than their offspring.

Online safety

Every parent wants to keep their child safe - so we watch them like hawks as they take their first steps, we hold their hand walking them to primary school and we teach them not to speak to strangers.

All too soon it seems they start to assert their independence, wanting to walk to school on their own and have their own mobile phone or tablet so they can chat with their friends after school and research their homework on the internet.

But how much freedom do you give them? And how much does any parent really know about what their son or daughter gets up to online?

A huge 62 per cent of parents with children aged between 12 and 15 feel they know less about the internet than their offspring.

Whether your child goes online to research a school project, visit a social networking site or buy a new pair of trainers, you want them to be protected and aware of what they are doing. So here's our guide to help you keep your children safe in the digital world.

Be interested in what they do online

These days, for your children the line between real life and online life is blurred. Unlike generations before, today they socialise and grow up online. They may start simply on social media sites but as they get older they follow their peers and the trends.

- Talk to them about what they are doing online and reassure them you are always there if they have any concerns.
- Try keeping up to date with new websites and the latest trends. Why not set up your own social networking account so you can understand and advise your children about what is safe – perhaps compile a list of safe sites and chat rooms.

If you find it tricky to chat with your children about their online activities, here are some ideas:

Ask them which sites they like to visit and what they enjoy doing online.

Talk about how they stay safe and if they have any advice for you.

Ask for their help in finding a website or doing something better online.

Find out if they know where to go for help if they need it and how to set privacy settings etc...

Use the internet as a family

Is there anything you could do to encourage the whole family to go online together? Perhaps you could look at the internet together to research your next holiday destination or find local places of interest to visit at the weekend.

Know your gadgets

Nowadays you don't need a computer to go online - most mobile phones, and even some TVs connect to the internet. Ensure you know all the points of internet connection in your home. Think about setting up parental controls for all of them and keep them up to date.

Set some boundaries

It's a good idea to limit the amount of time your child spends online and keep the family computer in a central place so everyone can see what is being looked at.



Chatting online

Text, email and video are just some of the ways today's young people access the online community. Chat to your child about who they are talking to online and encourage them to think before talking to people they don't know.

- Make sure they know not to share personal information including their password, bank details, address, school or any personal details about family members.
- Ensure they understand that, for their own safety, they must never meet up with someone they have met online.
- Ask your child if they know how to block someone whom they don't want to talk to. If they aren't sure, help them to learn how to use the blocking feature.



Sexting

Sexting is sending or receiving sexually explicit images usually via mobile picture messages or webcams over the internet. It's also called cybersex or sending a nudie or selfie.

Many young people don't see sexting as a problem and aren't keen to talk to adults about it because they think they'll be judged or have their phone or computer confiscated. But it's illegal; they have no control over the images and how they are shared and it makes them vulnerable to blackmail, bullying and harm.

How much does any parent really know about what their son or daughter gets up to online?

- Talk to your child about what pictures they feel are OK to send to people.
- Ask them if they would be happy for you or their grandparents to see the image? If they say no, then explain that it's probably not safe to send.
- Make sure your child knows their body is private and that being asked to sext is inappropriate.
- Ask them if they would want a private photo of them shared and remind them how easy it is for someone to forward it on and copy it, possibly for malicious reasons.

Sharing online

Sharing information online, whether it's a photo, video or an opinion, means that other people can access it, and not just people you know. It's so quick to post online - just the click of a button and there it is for everyone to see. Unfortunately it's not so easy to remove.



- Talk to your child about online privacy and sharing content. Do they trust the person they are sending it to? Could it be shared with others or posted somewhere else on the internet? Could it be used maliciously?
- Set clear guidelines about what is OK to share about themselves and your family. Finding examples of cases where it has gone wrong for someone may be a way to open up the dialogue.
- Talk to your child about how easy it is for someone to assume another identity online and lie about anything to get friendly with a young person.

Warn your child they shouldn't email, message or talk to people online who they don't know.

Gaming

Gone are the days when you played a computer game against a friend who was sat next to you in the same room. Now games are played online against opponents your child has probably never met.

- Tell your child to avoid sharing personal information with people they meet in an online games room.
- Make sure your child knows how to block people, and if they experience bullying, hacking or racism save the evidence and report it.
- Use parental control on games consoles to disable or restrict access to facilities like voice chat.
- Ensure you are using games from reputable and legal online providers.
- Use PEGI games ratings when you are buying games for your child. They rate video games at various age levels and are designed to protect young people from inappropriate content.



Content online

Young people who have grown up with the internet may believe that everything they see or read online is true. They may also think they can download anything they want without any repercussions.



- Try to encourage your child to double check the information they have sourced by researching and comparing it on other websites.
- Explain that they should only open attachments or click on links in emails if they are expecting them.
- If your child is downloading films and music make sure they know about copyright laws.
- Ensure they understand that if they download from an illegal site or sell copies without permission they are breaking the law and could face serious penalties.
- Research for yourself the legal sites for downloading or streaming music, film or TV content.
- It's also worth explaining that using illegal sites might mean they download viruses that could affect their computer.
- Install reputable antivirus or firewall software and keep it up to date.

Online shopping

Unlike shops on the high street, online shops never close and there are never queues for the tills. But they come with risks and young people need to learn how to shop safely.

- Talk to your child about safe online shopping and oversee younger children. Ensure your child buys from reputable online retailers. Explain to them that criminals can set up online shops that are only there to steal people's money.
- Explain they need to look for the padlock symbol on the payment page.
- Remind your child to use strong passwords when online shopping.



Understanding social media risks

Social networking sites

Most young people have a profile on a social networking site. There are age restrictions for some, for example you have to be 13 years old to have a Facebook account.

These sites can be a great way of keeping in touch and sharing photos and videos with family and friends but there are also risks involved. Your child could befriend or talk with a stranger who may be stalking them, or they could become the victim of cyberbullying, scamming or identity theft.

- Teach your child to be careful of whom they befriend and communicate with online. Most young people want to have as many friends as possible because it makes them feel popular. Warn your child that not everyone is who they say they are.
- Make sure that they understand not to reveal their personal details.
- Encourage them to 'share with care'. Remind your child that once they have posted something on their profile page it can be copied, shared or edited and could turn up anywhere.
- Use privacy settings. Most social networks allow you to limit and control who sees the content that you post. Make sure your child is only letting people they know and trust see what they are posting. Ensure they know how to use the privacy settings themselves and how to block people who are bothering them.



If you are unsure of the risks your child could be taking, ask them these questions:

- Do you know your social network friends?
- Who has access to your posts on Facebook?
- Are you in control of what you share online?
- How does your profile appear?
- Do you know how to use 'Graph Search'?
This enables people to target selected groups such as girls in Swindon who like Taylor Swift - you may suggest your child turns this setting off.
- Do you know how to manage 'Hidden from timeline' changes?
- How do you use your Friends lists?
- Do you know how to deactivate your account?

Understanding social media risks continued...

Cyberbullying

Unlike physical bullying, there can be little escape from cyberbullying as it happens in the victim's home and it's 24/7. Cyberbullying can be anything from someone sending nasty emails or texts to creating a hate page on a social networking site. So if your child says they are being bullied online don't take their computer away from them.

- Talk to them about what's happening and make sure you save the evidence so you have something to show when you report it.
- Resist replying to the cyberbully as they will be hoping for such a reaction. Instead you can block communication and report the bullying to the social sites where it is taking place.
- You can also discuss what is happening with your child's school, and report any unlawful activities to the police.

And finally:

What if something goes wrong

Know who to contact if you want to report a problem. There are many websites dedicated to advising parents and children about using the internet safely, including:

www.getsafeonline.org

www.thinkuknow.co.uk

www.gov.uk/government/publications/advice-on-child-internet-safety-10-universal-guidelines-for-providers

Reference

(1) Samuel Gibbs, Ofcom, One in Three Children under 15 now own Tablet Computer Supplanting TV, Guardian, 09/10/2009.
www.theguardian.com

About BCS, The Chartered Institute for IT

BCS, The Chartered Institute for IT, sets the standards of education for the digital industry.

Our world-class portfolio of digital qualifications is designed to support lifelong learning. From school children and computer novices to IT professionals and CIOs, we're enabling everyone to take part in the digital revolution.

Discover how you can develop your digital skills at bcs.org/ituser