



## More things to consider

- **Protect your personal information and identity**

Use the privacy features on social media sites to choose who can see your profile and your posts, and avoid publishing information, such as your telephone number, address or date of birth.

- **Protect yourself when buying things online**

Make sure that you're using a secure website before entering any personal details. There are ways to spot that a website is secure. Look for addresses that start with 'https', this means they are secure. A padlock symbol will also appear in the browser where the website address is. But be aware that a padlock symbol is not an absolute guarantee of safety. If you ever have doubts it's best to leave the page.

- **Protect your computer**

There are a few simple steps you can take to protect your computer, which include installing security software, updating your computers operating system and protecting your wireless network.

- **Stay safe**

Please remember overloaded sockets, damaged cables and wiring, blown fuses and misused appliances could all be a fire risk so keep an eye on your devices. Watch out for danger signs such as hot plugs and sockets and always follow the manufacturer's guidelines.

## Useful resources

- [www.lincolnshire.gov.uk/lscb](http://www.lincolnshire.gov.uk/lscb)
- [www.internetmatters.org](http://www.internetmatters.org)
- [www.ageuk.org.uk](http://www.ageuk.org.uk)
- [www.getsafeonline.org](http://www.getsafeonline.org)
- [www.nspcc.org.uk](http://www.nspcc.org.uk)
- [www.lincolnshire.gov.uk/lfr](http://www.lincolnshire.gov.uk/lfr)
- [www.lincolnshire.gov.uk/lsab](http://www.lincolnshire.gov.uk/lsab)



# Staying safe online

# Top tips for children and young people

- **Be aware of your digital footprint**

Every time you go online you leave a 'digital footprint' which shows others where you are and what you have been doing. So while posting pictures and videos is great for sharing and being creative, remember that once something is online it's likely to stay there forever!

- **Think before you post**

The internet can be great for airing your opinions and making the world a better place. However, be wary of writing negative posts. Ranting on the spur of the moment might feel good at the time but you may regret it later. Always remember that when you respond to something someone's said, there's a person at the other end who has feelings, just like you do.

- **Know who you're dealing with**

Lots of people only play or chat with people they know in person, and that's a sensible approach. But if you do meet people you don't know, use the same caution you would offline. Remember people may not be who they say they are, so be mindful about what you say about yourself. Keep chat general and if you are concerned that someone's asking for personal details, then stop contact and tell a trusted adult. Never arrange to meet someone you only know online.

- **Protect your identity**

When using the internet never give out personal information, such as your number, where you live or what school you go to – it's a big no-no. If you are using social media check your privacy settings and make sure only friends can see your posts.

- **Keep a healthy balance**

The internet is amazing, but make sure you take regular breaks away from the screen. If you find yourself spending a lot of time online and even thinking about it when you're offline then maybe it's time to back off a bit. There's a whole world out there – and while the internet can be fun, creative and social, you could be missing out on real life, like hanging out with your real mates. It's all about striking a good balance.

# Top tips for parents

- **Set some simple rules**

Agree where devices can be used – living room, dining room, not in bedrooms! Agree on what apps can or can't be installed, or agree to discuss any new apps before downloading. Even agreeing to keep social media accounts private can go a long way towards being safer online

- **Agree rules on age limits**

All app and game stores use the PEGI rating system which shows you, at a glance, how age appropriate a game or app is – either 3, 7, 12, 16 or 18 rated. Devices such as tablets and consoles allow you to set a maximum age.

- **Make sure you manage their screen time**

Mobile devices will now help you keep track of what games and apps are being used, and how long they are being used for – some apps let you set reminder to take a break. Make sure they always take regular breaks from technology and make sure you discuss pressure to be constantly connected to others – there is no prize for who replies the quickest!

- **Set up some Parental Controls**

Parental controls allow you to stay in control of the technology. Whether you want to filter their internet or limit what features they can use, parental controls keep you in charge. Nearly every internet ready device will come with these features – games consoles, tablets, phones, even Smart TV's!

- **Keep talking about it**

Children and young people often feel anxious talking to adults when things go wrong online, but keeping technology as an open discussion in your household can make them feel more comfortable talking about both the bad and the good they experience. Even if they've made a mistake, just talking about what upsets us, or what we don't like online, can help us all feel a little less isolated.



# Top tips for older people

- **Copycat websites**

Ordering new passports, booking driving tests and renewing car tax discs are just some of the ways people are being conned by fraudsters who operate 'copycat' websites. These are designed to trick people into parting with their cash by charging for services that are provided cheaper or free through official government channels. Search on GOV.UK to find official government services and phone numbers.

- **Protect your password**

Ensure you use strong passwords, and do not disclose them to anyone else. Visit [www.getsafeonline.org](http://www.getsafeonline.org) for more information.

- **Phishing**

These are emails and harmful links designed to deceive people into revealing personal/financial details. By spoofing emails, email addresses, websites and payment services, scammers can trick people into believing they are dealing with genuine banks, traders and authorities to send money. These are often in the guise of non-existent goods and services – or to collect lottery "winnings."

- **Health scams**

False and misleading claims may be made about medical-related products, such as miracle health cures, and fake online pharmacies offering cheap medicines. The medicine delivered to you can turn out to be poor quality, and harmful to your health.

- **Relationship scams**

Scammers use social networks such as dating websites and chat rooms. Once they've gained your trust, they'll start asking you for money, often by telling you an emotional or hard luck story. Trust your instinct. If something feels wrong, it probably is.

