



Internet Safety for Parents

March 2020

Created by Mrs K.Ainley

Internet Safety

A spokesperson for the NSPCC in Northern said:

"The constantly evolving digital world means a steady influx of new apps and games and can be hard for parents to keep track of. That's why it's important for parents to talk regularly with children about these apps and games and the potential risks they can be exposed to."

The NSPCC publishes advice and guidance for parents on discussing online safety with their children, as well as Net Aware - the UK's only parental guide to social media and gaming apps. Some of this information is summarised in this document.

Common signs to watch out for include children who:

- Become very secretive, especially about what they are doing online
- Are spending a lot of time on the internet and social media
- Are switching screens on their device when approached
- Are withdrawn or angry after using the internet or sending text messages
- Have lots of new phone numbers or email addresses on their devices

If adults are concerned or have any questions on how to approach the subject with their children, they can contact the NSPCC Helpline on 0808 800 5000 or **visit the NSPCC website**.

Parental Controls

The 4 big internet providers in the UK – BT, Sky, TalkTalk and Virgin Media - provide their customers with free parental controls which can be activated at any time by contacting them or via your online accounts.

Alternatively there are a range of software packages available. The following websites provide information on protecting your family online and available software packages:

<https://uk.pcmag.com/parental-control-monitoring/67305/the-best-parental-control-software>

<https://www.internetmatters.org/parental-controls/smartphones-and-other-devices/>

Don't forget if your child uses their device away from home, then they'll be able to connect to public WiFi which might not have the same settings.

If your child accesses the internet through 3G or 4G rather than using WiFi then they won't be subject to the parental controls.

Remember that filtering is only part of the solution

No filter or parental controls tool is 100% effective, and many of the risks that young people face online are because of their own and other's behaviour. It is therefore important to talk to your children about staying safe online and make sure they know that they can turn to you if they get into any difficulty.

Devices that connect to your home internet

In addition to content filtering offered by your internet provider, many devices such as games consoles, smartphones and tablets have their own parental controls, for example to limit spending or restrict access to apps based on age rating. Likewise, many web browsers have built-in tools and features to help you control the kinds of content users can view.

Staying safe when out and about

If children are taking their devices out of the home, it's worth bearing in mind that they could connect to public wifi, for example, in a shop, cafe or restaurant. Look out for the Friendly WiFi symbol:



which shows that the wifi has filters in place to limit access to pornographic content.

Settings on Apps and Game Consoles

- **TV and music settings** – Smart TVs and services like Netflix, iTunes, BBC iPlayer and YouTube have settings that allow you to control who sees what.
- **Search Engines** – Make sure the content that your child sees online is age appropriate by using the controls available in search engines like Google and Bing. You can set up filters like Google SafeSearch or use child-friendly search engines like Swiggle and Safe Search Uk.
- **Snapchat** – For ages 13+. This app will share the user's location unless the 'ghost mode' is enabled. You can enable this in Settings.
- **Instagram** – For ages 13+. Instagram has developed a filter that will block certain offensive comments on posts and in live video. All other comments will appear as they normally do and you can still report comments, delete comments or turn them off. To access it click the Settings Menu from the Profile, Privacy and Security, Comment Controls.
- **Facebook** – For ages 13+. Look at the privacy settings on Facebook accounts by clicking on Settings and Privacy, Privacy Shortcuts.
- **Twitter** – For ages 13+. Twitter allows you to mute words to help filter inappropriate content from your timeline and notifications. Tap Settings, view Content Preferences, Muted then Muted Words and simply add the words you would like to block.
- **WhatsApp** – For ages 16+. You can hide personal information on WhatsApp. Features like 'Last seen', 'Profile photo', 'About', 'Status' and 'Live location' can be hidden via Settings, Account, Privacy. There are additional settings under Security.
- **YouTube** – Officially, YouTube forbids children under the age of 13 to create their own accounts, and children between ages 13 and 17 are only allowed to open accounts with parental permission. To implement the Restricted Mode, go to YouTube.com and click on the Settings symbol, change Restricted Mode to 'On'.
- **TikTok** – For ages 13+, the minimum age limit to host a live stream is 16+ and only users aged 18 and over can purchase and give virtual gifts as well as receive them. Users can control who can see their uploaded content, follow them, and send them messages by making their account private. Please remember: Even with a private account, profile information – including profile photo, username, and bio – will be visible to all users. Counsel your teen not to reveal personal information such as age, address, or phone number in his/her profile.
- **Game Consoles** – Like with Mobiles and Tablets, the controls on your games console help you manage what your child can and can't do. Some devices allow you to set up different profiles for each family member, deactivate the internet, turn off chat functions to stop your child from talking to stranger.