A Guide to Parental Controls, Common Apps & Websites, and Associated Issues

An e-safety resource for parents, Summer 2022

To return to the main menu click here

Introduction and Contents

This booklet is a curated set of resources from the National Online Safety Hub – further information on a huge rage of safety topics can be found here: https://nationalonlinesafety.com/

The first half of this guide is designed to help you to set up parental controls at home and on devices your child may be using. Parental controls are designed to protect children from accessing inappropriate material and can be tailored to suit the age of your child. It is important however to emphasise that no system is 100% effective so it is important that you talk regularly to your child about their online activity and encourage them to share with you any worrying or concerning content they might come across.

The second half of the guide is information around the most used apps and websites that we see issues with in school, and information regarding the associated issues that occur around the students' use of social media. Although the information regarding issues has been grouped with a relevant app, you will find that most of these issues can occur on any platform.

This guide is not intended to be read as a whole – rather dip into the advice that may be affecting your family as appropriate. The contents table is clickable to take you to the relevant page, and at the bottom of every page you will find a link to return to the menu.

Contents

An e-safety resource for parents, Summer 2022 1

Introduction and Contents 2

What do I need to know about home devices? 4

How to set up Parental controls - Operating Systems 4

- Microsoft Windows 4
- Mac OS 4

What do I need to know about age-inappropriate content? 5

How to set up Parental controls – Internet Service Providers 5

How to set up Parental controls – Mobile Service Providers 5

How to set up parental controls on iPhone & android 6

How to use parental controls to limit age-inappropriate content 7

How to use parental controls to protect privacy 8

How to use parental controls on games consoles 9

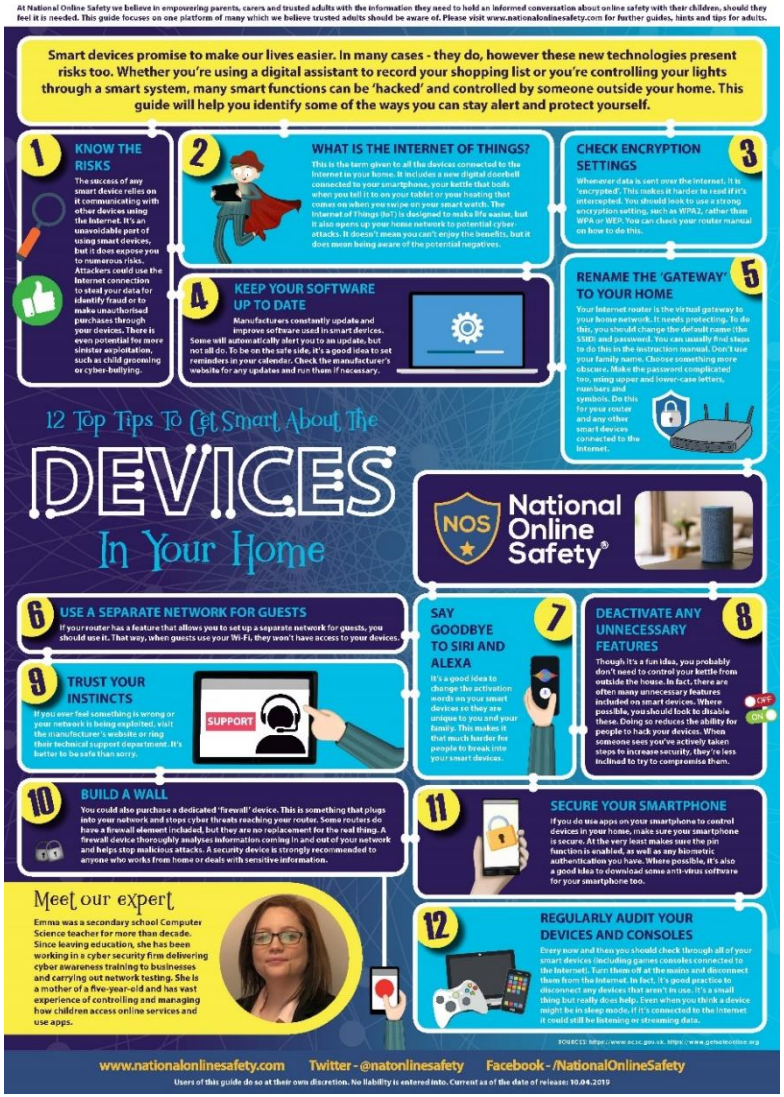
To return to the main menu click here

Setting up parental controls – Games Consoles 9
What do I need to know about screen addiction? 10
Family Technology Contracts 10
Guide to Common Apps and Websites 11
Facebook (13+) 11
WhatsApp (16+) & group chats 12
Instagram (13+) & friends and followers 13
TikTok (13+) & social pressures linked to 'likes' 14
Twitter (13+) & fake news 15
Snapchat (13+) & sexting 16
Discord (13+) & cross-platform sharing of inappropriate content 17
Omegle (18+) & Online Safety Tips 18
Steam & age ratings 19
Find out more! 20

To return to the main menu click here

What do I need to know about home devices?

Smart devices promise to make our lives easier. And in many cases – they do. But these new technologies present risks too. Whether you're using a digital assistant to record your shopping list or controlling your lights through a smart system, many smart functions can be 'hacked' and controlled by someone outside your home. This guide will help you identify some of the ways you can stay alert and protect yourself, you'll find tips on a number of potential risks such as fraud, online grooming and cyberbullying.



How to set up Parental controls - Operating Systems

Whichever OS you are using on your home computer/laptop, you will find built in parental controls for free. You will need to make sure you have your own account, and so does your child for this to be effective.

Microsoft Windows

The free family safety app allows you to set screen time limits that apply to devices, apps, and games. When screen time runs out, choose to add more or not, based on what's right for you and your family.

- App and game limits (Windows, Xbox, Android)
- Device limits (Windows, Xbox)
- Screen time requests
- Activity summaries

https://www.microsoft.com/en-gb/microsoft-365/family-safety

Mac OS

You can monitor and control the time your children spend on the Mac and websites they visit. To set up parental controls for your children, follow these steps:

- Turn on parental controls for each child. If you haven't added a user account for your child to your Mac, see Add a new user to manage with parental controls. If you've already added an account for your child, see Turn on parental controls for a child with an existing account on your Mac.
- Change the restrictions you want for each child. For example, you can decide which websites your child can visit, and how long they can use the Mac each day.
- If you want, copy the settings for one child and use them for another child.
- When you decide your child is ready, you can turn off parental controls for them.

To return to the main menu click here

What do I need to know about age-inappropriate content?

“Inappropriate” means different things to different people. What’s acceptable for one age group, for example, may be unsuitable for a slightly younger audience. Online, young people can chance upon inappropriate content in various way – from pop-up ads to TikTok videos. The increasingly young age at which children become active in the digital world heightens the risk of them innocently running into something that they find upsetting or frightening. Trusted adults need to be able to help children be aware of what to do if they’re exposed to age-inappropriate content. In the guide, you'll find tips on a number of potential risks such as social media, gaming and adverts.

How to set up Parental controls – Internet Service Providers

The vast majority of ISP’s will provide free tools which will allow you to manage the content that can be accessed via your home internet connection. The specific tools will vary by provider but most offer the opportunity to block specific websites, filter content by age and allow/deny access to the network at specific times or to specific devices.

Remember though that these will only apply while a device is connected to your network, and so mobile devices that use 3G, 4G or 5G mobile data connections will need have parental controls set on the device as well. See How to set up parental controls on iPhone & android

Links for some of the main providers are given below:

- Virgin Media: https://www.virginmedia.com/broadband/parental-control
- Sky: https://www.sky.com/help/articles/sky-broadband-shield-start
- Talk Talk: https://new.talktalk.co.uk/broadband/security
- BT: https://www.bt.com/help/security/how-to-keep-your-family-safe-online-with-bt-parental-controls-an
- Plusnet: https://www.plus.net/help/broadband/how-to-use-plusnet-safeguard/
- Now broadband: https://help.nowtv.com/article/set-up-and-manage-broadband-buddy

How to set up Parental controls – Mobile Service Providers

OFCOM regulations mean that all SIM cards obtained directly from the UK’s main mobile providers (Vodaphone, EE, O2 and Three) should come with age restrictions turned on. Unless this has been actively removed, all sites classified as 18+ should be restricted on a mobile device.

This filtering will only apply when using mobile data, and not WiFi so we advise that parental controls should also be installed on the device rather than relying on this alone.

To return to the main menu click here

How to set up parental controls on iPhone & android

Most smartphones allow parents and carers to choose which apps and features appear on their child's device and which ones don't – also preventing young people from buying and downloading anything that's unsuitable for their age. These guides to parental controls for managing apps will help you to reduce the chance of your child using a game or app that might not be appropriate for their age.

To return to the main menu click here

How to use parental controls to limit age-inappropriate content

The parental controls on smartphones allow you to block or restrict certain apps, features, content, downloads or purchases that might not be suitable for young people. Setting limitations around age ratings, Siri and web searches enables you to filter out age-inappropriate content and vastly reduce the likelihood of your children being exposed to potentially upsetting material and information. In the guide, you'll find tips on a number of tips such as sexting, strangers and excessive use.

To return to the main menu click here

How to use parental controls to protect privacy

The privacy settings on your child's smartphone give you control over how the information stored on it can be used. You can turn off location services, for example, to keep their whereabouts private or stop apps from accessing functions of the phone like the camera or microphone. The following step-by-step guides on how to tighten up privacy settings on iPhones and Android phones will give you tips such as how to make changes to the privacy settings and how to prevent changes to other settings and features.

To return to the main menu click here

How to use parental controls on games consoles

Much like a television allows you to watch movies or a radio allows you to listen to music, a game console allows you to play video games. The most modern ones are names you might be familiar with – Sony PlayStation, Microsoft Xbox, and Nintendo Switch – and almost all of them can now connect to the internet and be enjoyed online with friends. In the guide, you'll find tips on a number of potential risks such as the addictive nature of games consoles, inappropriate online content and online chat.

Setting up parental controls – Games Consoles

Games consoles have parental controls too – most will let you manage screentime, filter content based on your child's age and the PEGI game rating, allow or disallow online purchases and review and monitor who they are communicating with online.

More specific information by console is linked here:

- Nintendo Switch: https://www.nintendo.co.uk/Nintendo-Switch/Nintendo-Switch-Parental-Controls/Nintendo-Switch-Parental-Controls-1183145.html
- Xbox: https://www.xbox.com/en-GB/community/for-everyone/responsible-gaming
- PS4: https://www.playstation.com/en-gb/support/account/ps4-parental-controls-and-spending-limits/
- PS5: https://www.playstation.com/en-gb/support/account/ps5-parental-controls-spending-limits/
- Oculus/Meta Quest VR: https://store.facebook.com/gb/quest/safety-center/parental-supervision/?intern_source=blog&intern_content=latest-quest-software-update-makes-your-home-space-more-social-and-adds-important-parental-supervision-tools

If you have reservations about a game your child may want to play, or just want to find out more about what they are playing, the family gaming database at https://www.taminggaming.com/en-gb/home contains key information such as age suitability, description of gameplay, screenshots and associated costs for nearly 2,000 games.

To return to the main menu click here

What do I need to know about screen addiction?

It can be challenging for parents and carers to know whether children are spending too much time on their devices. Furthermore, it's even more of a challenge to know whether a child is addicted to the internet and social media. As technology is becoming more pervasive, children and young people are experiencing tech – related dependencies. Do we as parents and carers have the knowledge to identify and support children and young people who may be developing an addiction to their devices?

In this guide, you'll find tips on a number of potential risks such as health & wellbeing, app addiction and a lack of sleep.

Family Technology Contracts

If you are worried that your child spends too long on their devices, you may find a family technology contract helpful. Family technology contracts help teach proper technology use and set expectations. They allow you to start an open conversation with your child and encourage them to be part of the decision making. By creating a family media contract, your children will know their boundaries and have concrete consequences for breaking them.

There are 4 factors that should be considered within the contract:

- **Time limits** – this may be a maximum time per day, and/or rules around when (and perhaps where) a device can be used.
- **Appropriate content** – this will differ according to the type of contract.
  For video gaming, consider what age ratings are appropriate.
  For phones, what apps are (and are not) allowed to be used.
- **Rules about sharing** – discuss what is appropriate to share online. Some topics to discuss are sharing your location, sexting and what can be posted on social sites.
- **Consequences** – make sure your child will know what happens if they break the rules.
  Make the rules as specific as possible and adjust the consequences based on the item.
  For example, the consequence for sharing inappropriate content might be different from having a phone at the dinner table.

Some example templates can be found here:
https://www.pandasecurity.com/en/mediacenter/family-safety/family-media-agreement-printables/

To return to the main menu click here

Guide to Common Apps and Websites

Facebook (13+)

With 2.9 billion users, Facebook, owned by the recently rebranded Meta, is the world's most popular social media platform. It encourages interaction with other people by (among other things) adding them as friends, reacting to or commenting on their content, sharing images and videos, posting status updates, joining groups and playing games. Facebook is free, and anyone over 13 can join – but with no age verification, younger children can easily create an account: it's likely your child is already familiar with the platform, even if they don't yet use it themselves.

In the guide, you'll find tips on a number of potential risks such as cyberbullying, strangers and the addictive nature of Facebook.

To return to the main menu click here

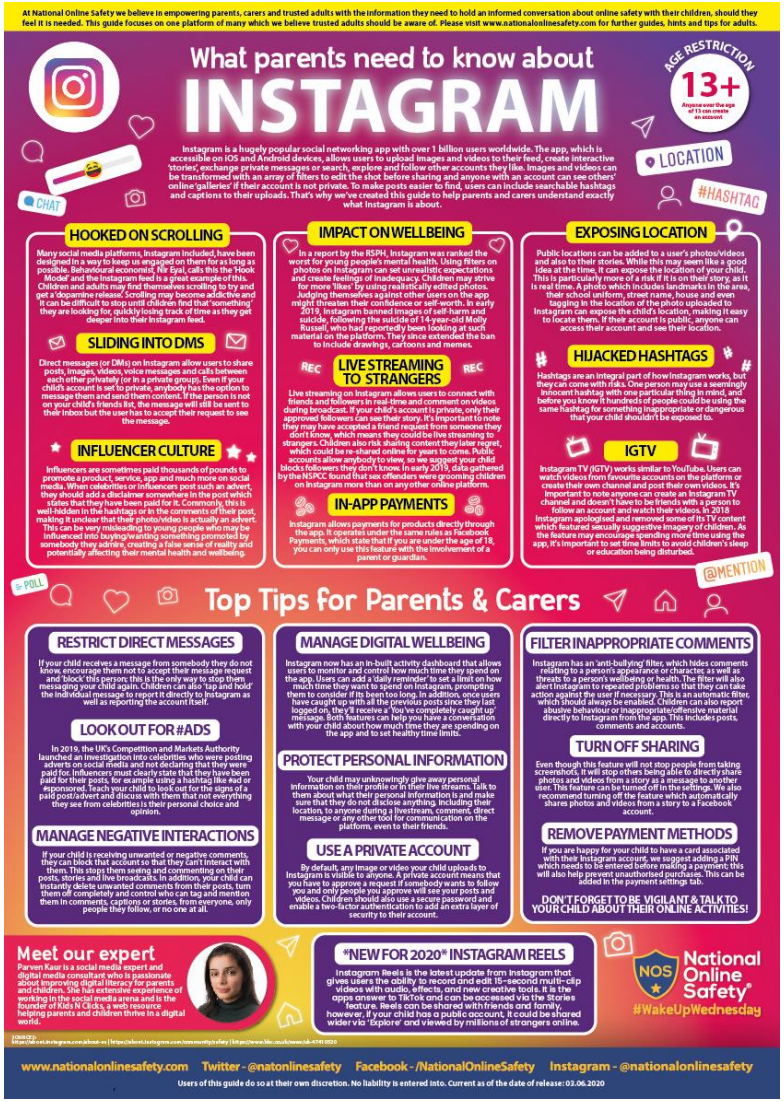
WhatsApp (16+) & group chats

WhatsApp is the world's most popular messaging service, with around two billion users exchanging texts, photos, videos and documents, as well as making voice and video calls. Its end-to-end encryption means messages can only be viewed by the sender and any recipients: not even WhatsApp can read them. Updates to its privacy policy in 2021 (involving sharing data with parent company Facebook) caused millions to leave the app, but the new policy was widely misinterpreted – it only related to WhatsApp's business features, not to personal messages. In the guide, you'll find tips on a number of potential risks such as scams, strangers and location sharing.

To return to the main menu click here

Instagram (13+) & friends and followers

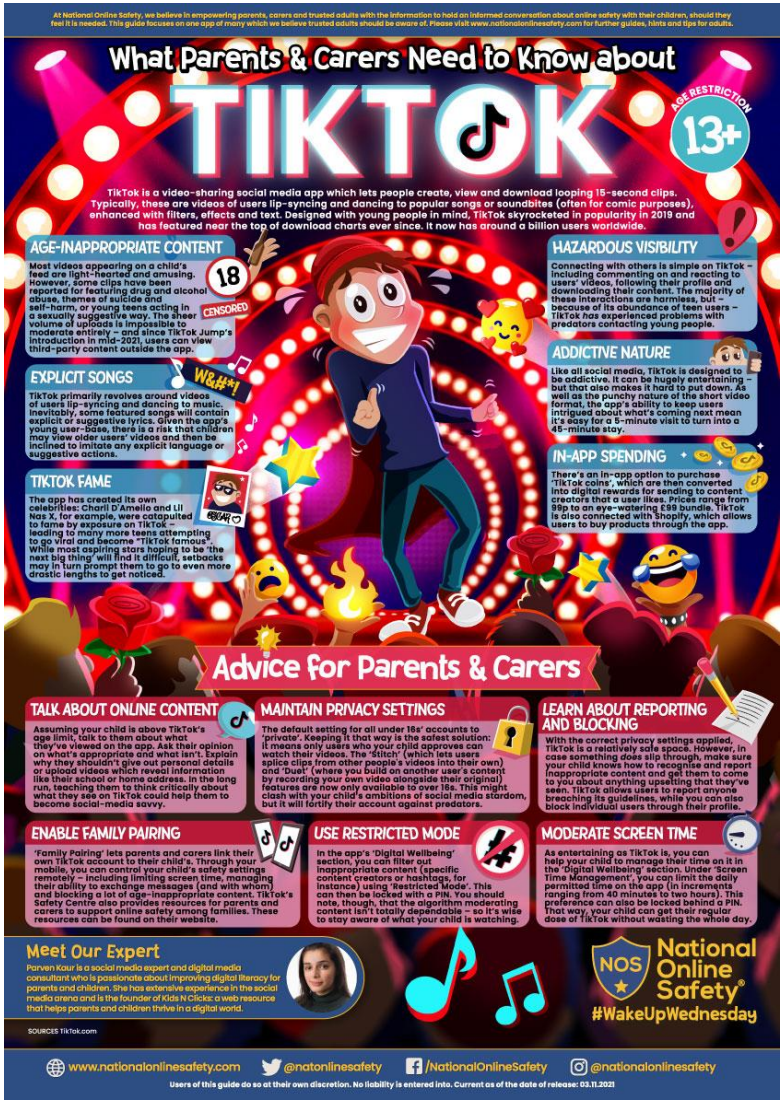
Instagram is a hugely popular social networking app with over 1 billion users worldwide. The app, which is accessible on iOS and Android devices, allows users to upload images and videos to their feed, create interactive ‘stories’, exchange private messages or search, explore and follow other accounts they like. Images and videos can be transformed with an array of filters to edit the shot before sharing and anyone with an account can see others’ online ‘galleries’ if their account is not private. To make posts easier to find, users can include searchable hashtags and captions to their uploads. This guide has been created to help parents and carers understand exactly what Instagram is about. In the guide, you'll find tips on a number of potential risks such as exposing your child’s location, in-app purchases and poor mental wellbeing.

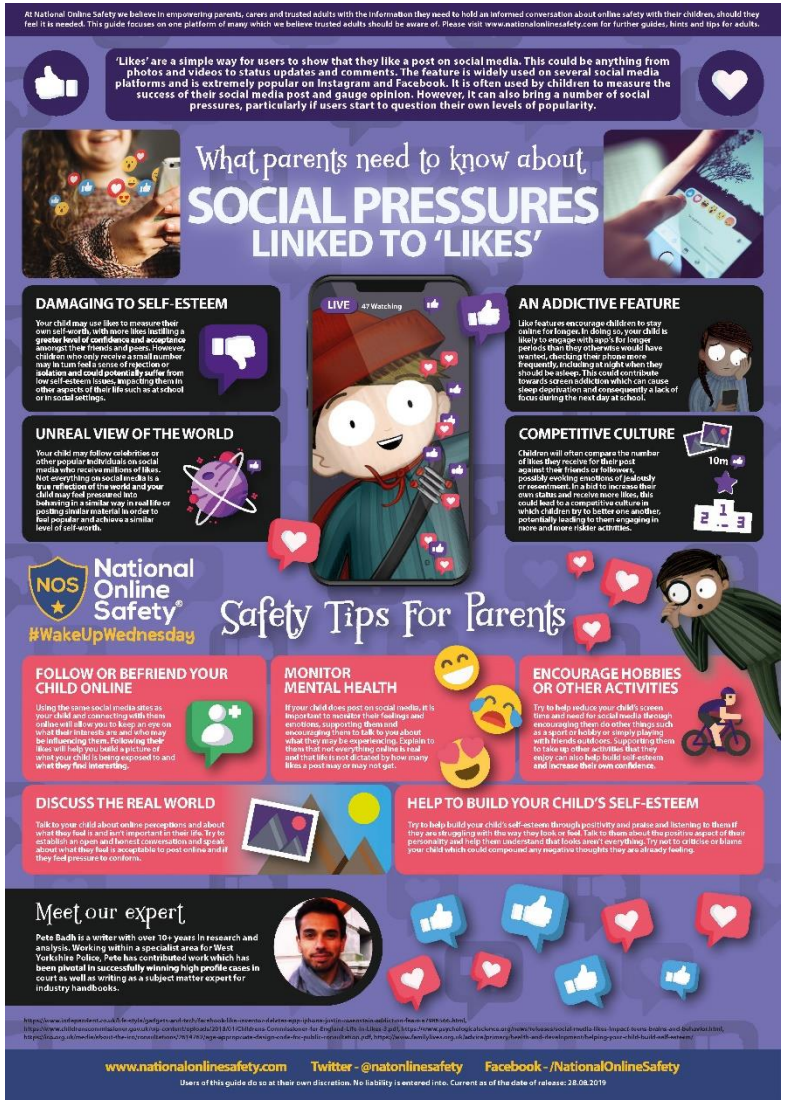


To return to the main menu click here

TikTok (13+) & social pressures linked to ‘likes’

TikTok is a video-sharing social media app which lets people create, view and download looping 15-second clips. Typically, these are videos of users lip-syncing and dancing to popular songs or soundbites (often for comic purposes), enhanced with filters, effects and text. Designed with young people in mind, TikTok skyrocketed in popularity in 2019 and has featured near the top of download charts ever since. It now has around 1 billion active users worldwide. In the guide, you'll find tips on a number of potential risks such as age-inappropriate content, addiction and in-app spending.

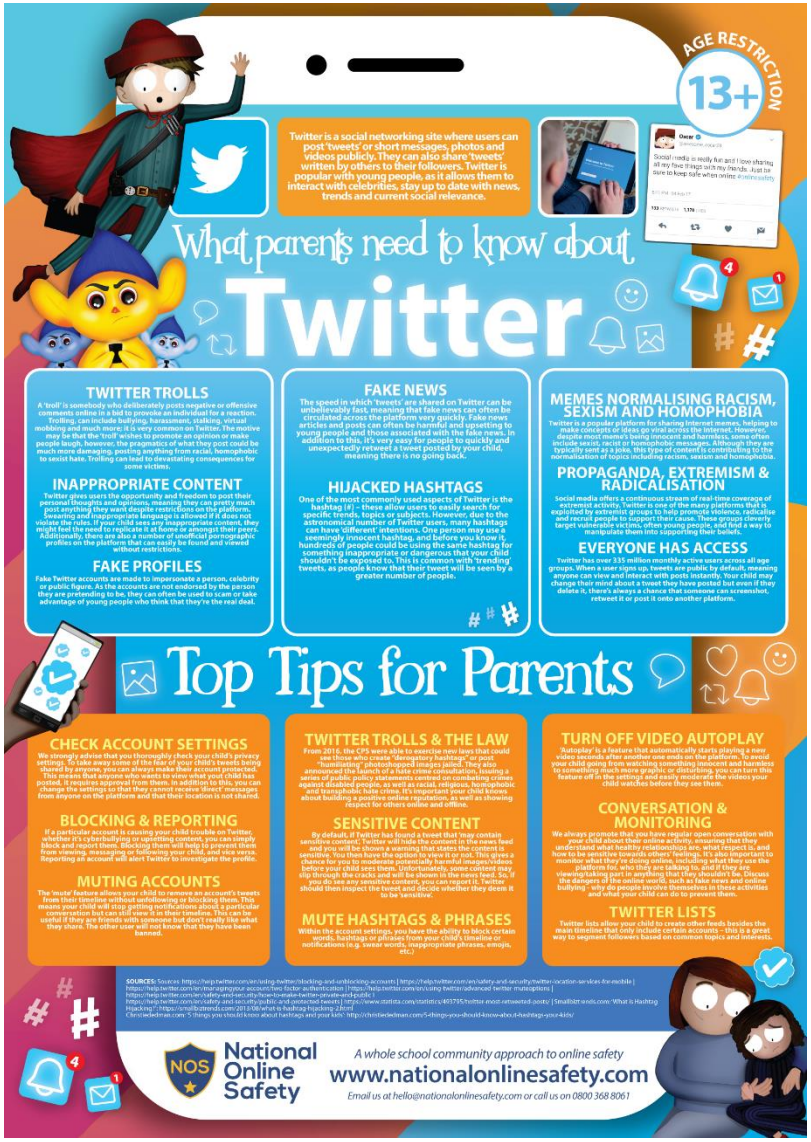


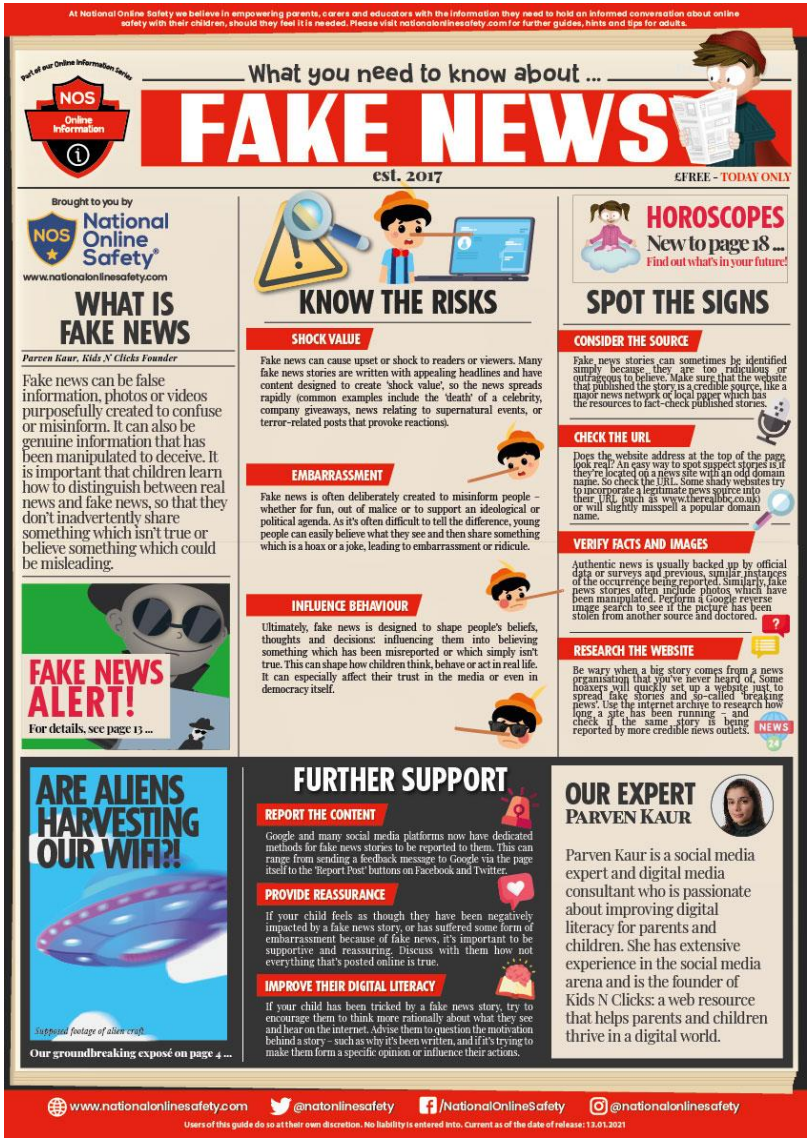


To return to the main menu click here

Twitter (13+) & fake news

Twitter is a social networking site where users can post ‘tweets’ or short messages, photos and videos publicly. They can also share ‘tweets’ written by others to their followers. Twitter is popular with young people, as it allows them to interact with celebrities, stay up to date with news, trends and current social relevance. In the guide, you'll find tips on a number of potential risks such as trolls, fake news and propaganda.





To return to the main menu click here

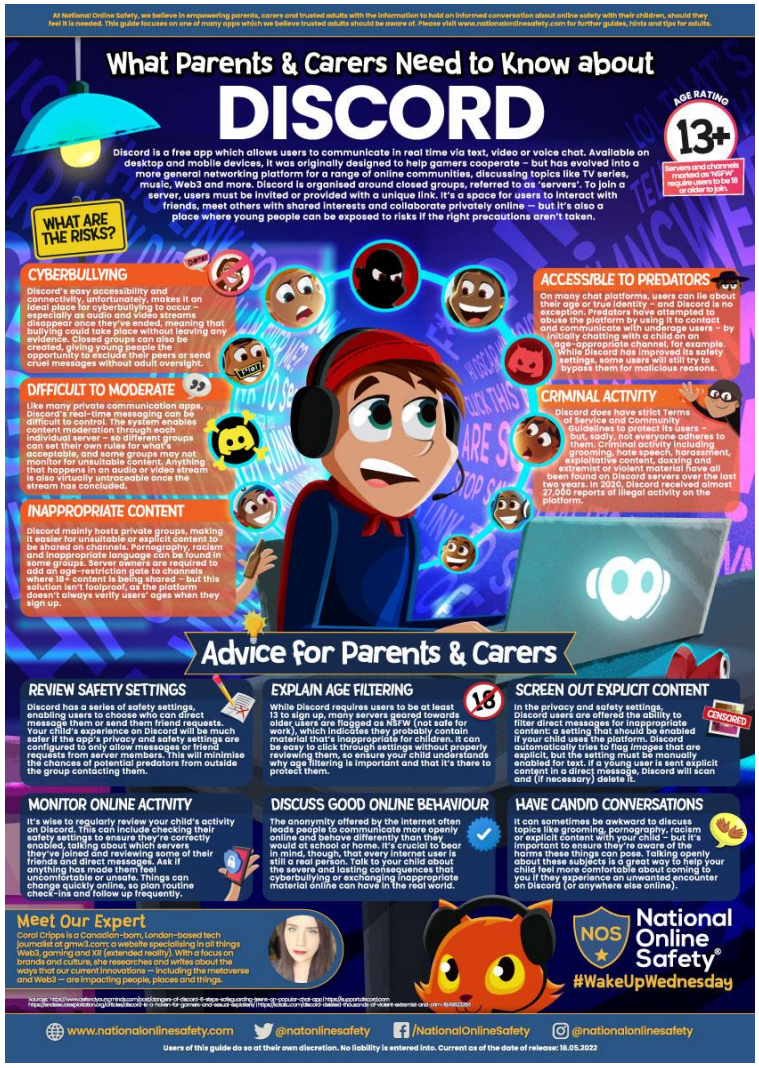
Snapchat (13+) & sexting

Snapchat is a photo- and video-sharing app through which users can chat with friends via text or audio. Images and videos can be shared with specific friends, or as a 'story' (documenting the previous 24 hours) that's visible to a person's entire friend list. Snapchat usage rose during the lockdowns, with many young people utilising it to stay connected with their peers. The app continues to develop features to engage an even larger audience and emulate current trends, rivalling platforms such as TikTok and Instagram. In the guide, you'll find tips on a number of potential risks such as sexting, visible location and strangers.

To return to the main menu click here

Discord (13+) & cross-platform sharing of inappropriate content

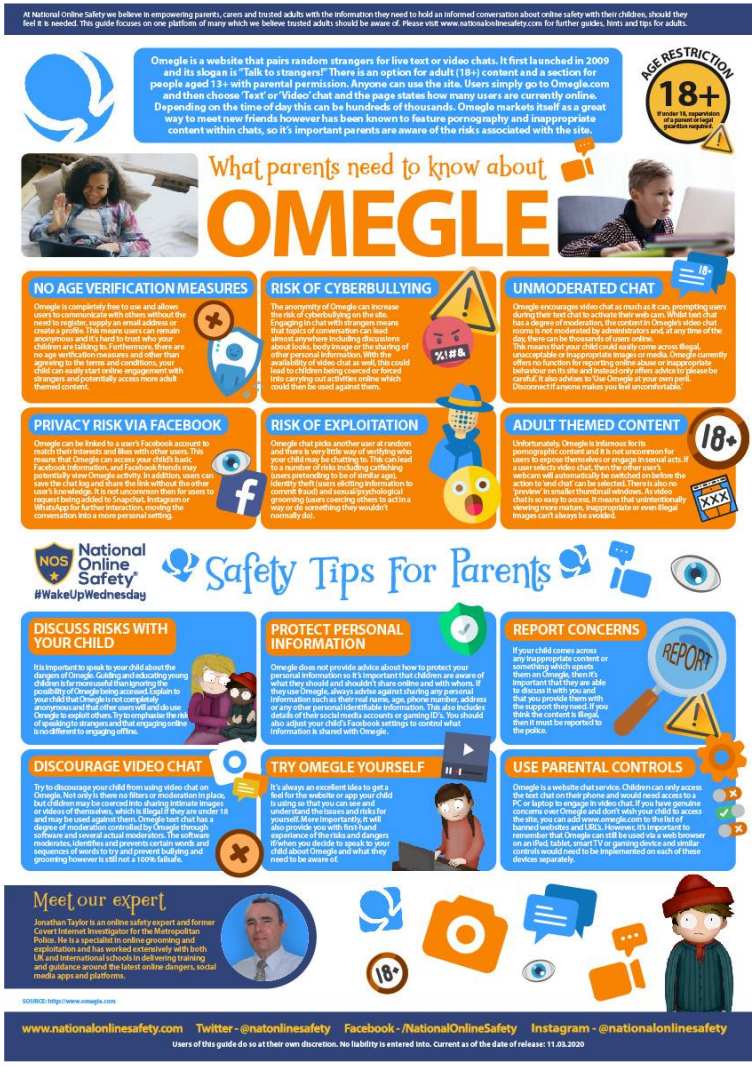
Discord is a free app which allows users to communicate in real time via text, video or voice chat. Available on desktop and mobile devices, it was originally designed to help gamers cooperate – but has evolved into a more general networking platform for a range of online communities, discussing topics like TV series, music, Web3 and more. Discord is organised around closed groups, referred to as 'servers'. To join a server, users must be invited or provided with a unique link. It's a space for users to interact with friends, meet others with shared interests and collaborate in private online — but it's also a place where young people can be exposed to risks if the right precautions aren't taken. In the guide, you'll find tips on a number of potential risks such as cyberbullying, predators and inappropriate content.



To return to the main menu click here

Omegle (18+) & Online Safety Tips

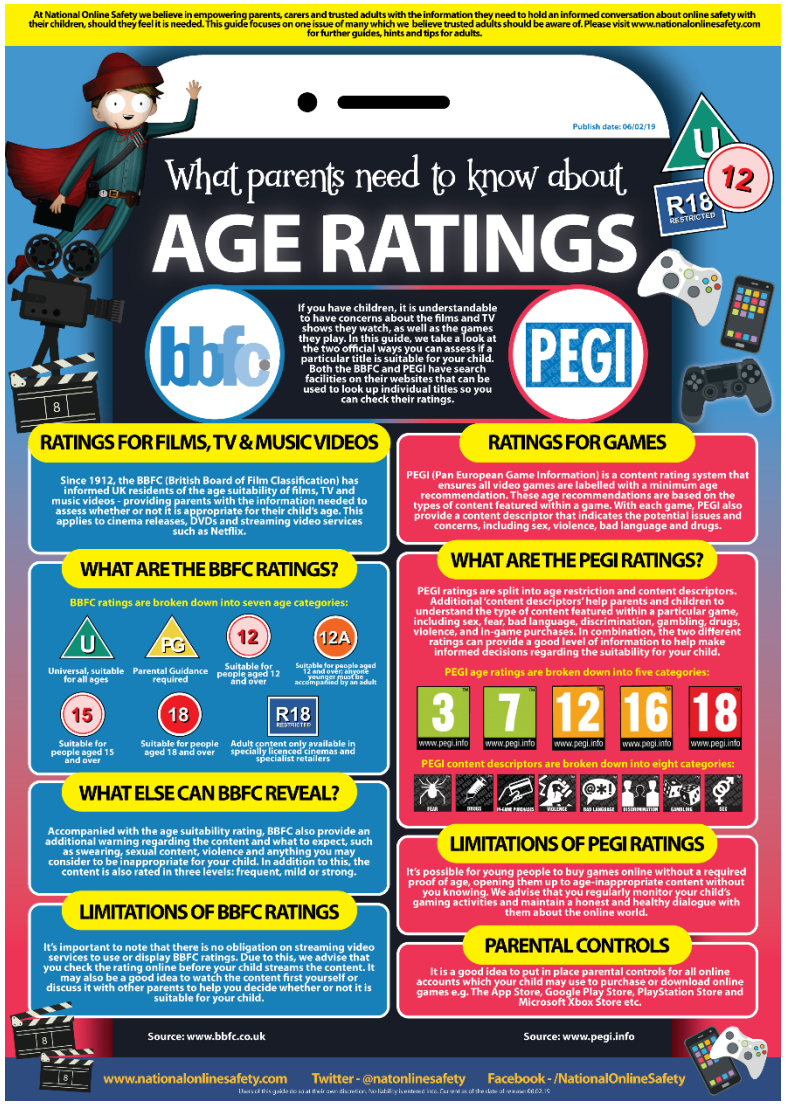
Omegle is a website that pairs random strangers for live text or video chats. It ¬first launched in 2009 and its slogan is “Talk to strangers!” There is an option for adult (18+) content and a section for people aged 13+ with parental permission. Anyone can use the site. Users simply go to Omegle.com and then choose ‘Text’ or ‘Video’ chat and the page states how many users are currently online. Depending on the time of day this can be hundreds of thousands. Omegle markets itself as a great way to meet new friends however has been known to feature pornography and inappropriate content within chats, so it is important parents are aware of the risks associated with the site. In the guide, you'll find tips on a number of potential risks such as pornographic content, cyberbullying and the chats being unmoderated.



To return to the main menu click here

Steam & age ratings

Steam is a computer gaming digital distribution platform and storefront. It is the biggest platform for desktop- or laptop-based gaming, with a range of more than 30,000 games available. The platform has become a lively social environment for many gamers, and allows people to trade, sell and buy gaming items for real money. Valve, the developers behind Steam, have also released different hardware that works with the platform, including the Steam Deck – a hand-held console that lets users play their favourite games while away from their computer. In the guide, you'll find tips on a number of potential risks such as potential scams, contact with strangers and in-app purchases.



To return to the main menu click here

Find out more!

Useful links for more safety information:

CEOP provide information for both parents and young people

- Parents: https://www.thinkuknow.co.uk/parents/
- Young people: https://www.thinkuknow.co.uk/11_18/

Their #AskTheAwkward campaign helps you to prepare for regular conversations with your child about online relationships and related topics. It also offers advice on how to keep conversations positive and what to do if your child tells you something that worries you. https://www.thinkuknow.co.uk/parents/ask-the-awkward/

You can also report concerns around grooming and sexual abuse directly to CEOP. https://www.thinkuknow.co.uk/parents/Get-help/Reporting-an-incident/

Seen child sexual abuse content online?

If you have come across child sexual abuse images or videos online, report to the Internet Watch Foundation (IWF). Reporting is quick, easy and anonymous. It can lead to the removal of criminal content and even the rescue of a child from further abuse.

An under 18 year old worried their nudes have been shared online?

If an under 18 year old has had a nude or semi-nude image of themselves shared online, they can report to IWF and Childline's Report Remove tool. They will work to try and remove the image.

Does your child need someone else to talk to?

If your child needs someone to talk to because of anything which has upset them, it could be that they are being bullied or that they have seen something online which they wish they hadn't, they can speak free and confidentially to Childline. Children can ring Childline on **0800 1111** and speak to trained counsellors about any problems they may face. Childline is run by the NSPCC and is there to help your child.

The Childline website also offers excellent help and advice on a whole range of issues.

Want to know more about keeping you and your devices safer?

Get Safe Online gives practical advice on how to protect yourself, your computers and mobiles device against fraud, identity theft, viruses and many other problems encountered online.

Find out more at: Get Safe Online.

To return to the main menu click here