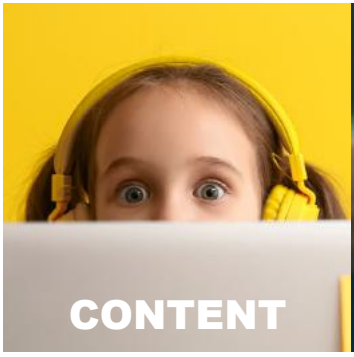
Keeping Children Safe Online

Just like in the real world, the internet is full of wonderful sights, experiences and opportunities. It's a place where people can connect, learn, create and express themselves in new and exciting ways. But just like in the real world, there are also risks to be aware of.

The 3 Cs of online safety

An important step in keeping children safe online is identifying what the potential risks and harms might be. These can be split into three areas:



There is no guaranteed way to ensure a child's safety online. What works for one family may not be workable for another. However, there are certain approaches that have proven generally effective for all. This booklet contains some top tips to help protect children for each of the risk categories.

reducing

CONTENT

risks

Set up filtering

All major broadband providers offer some form of content filtering. This will block access to adult and illegal content before it even reaches your home.

Similar services are also offered by the main mobile networks too. You can find details on how to set this up on your provider's website.

Restrict video streaming

Where available, make use of child-focussed apps and profiles to limit what content your child is exposed to.

Services like Netflix and Disney+ streaming services have a 'child' option that will hide content based on its BBFC rating.

YouTube provides the YouTube Kids app to filter content. Bear in mind, this is primarily filtered via artificial intelligence and cannot be completely trusted.

Avoid social media

The vast majority of social media platforms have a minimum age of at least 13.

No parent has ever said "I wish I'd let them on earlier" when talking about social media.

Keep them off for as long as you can.

Content is anything posted online: words, images, sound or video. Children may see illegal, inappropriate or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

Monitoring their content consumption

Look through your child's browser history to see what sites they are visiting. Check out any you're not sure about.

Check up on what they are watching on video sites. Most streaming services will retain a list of what has been watched.

Take a look at the videos being recommended to your children. The algorithm may expose what they've been watching, even if they deleted it from their history.

As much as possible, have them watching videos in the living room or some other shared space. Encourage them to do it without headphones. So you can casually keep an eye and ear on what they're watching and step in if necessary.

Get to know what your child is watching. Talk to them about it. Watch with them. You will quickly notice if things aren't as they should be.

Use PEGI age ratings

All video games come with a PEGI rating, indicating not only the appropriate age to play the game but an idea of the content it contains.

A lot of games intended for older children are graphically violent and/or feature mature storylines and events. If you wouldn't let your child watch an 18-rated film, you shouldn't let them play an 18-rated game.

reducing

CONTACT

risks

Establish monitoring expectations

Until a child is mature enough to handle the responsibility of online privacy, parents have a right and a responsibility to monitor their online activity.

A big part of reducing contact risks is monitoring who they are talking to and what they are talking about.

This doesn't need to be done surreptitiously. Set up the expectation with your child that you will be checking their interactions now and then, and explain why.

You need to know who they are talking to, what they are saying and what platforms they are using to do so.

Start from a position of silence

Where possible, set all parental controls to their strongest settings when it comes to contacting others. If you can, turn off all chat facility (although it's rare to have that level of control). If there are ways to limit what can be said between players, use it.

New users to a platform are particularly susceptible to being scammed or receive unwanted attention. They are unfamiliar with rules; curious to see what they can do; and eager to make friends – all of which makes them easy to take advantage of.

It is always possible to enable features at a later date, once you and your child fully understand the platform and they have demonstrated they can act responsibly on it.

Contact is about the risk of harm children may face when interacting with others online. Sometimes adults pose as children with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

Keep online access to shared spaces

This is not always going to be possible, especially as they get older. But the longer you can keep children's online activity in shared spaces of the house, the better you can monitor what is happening. The vast majority of online abuse happens in bedrooms, often when parents are still at home.

At the least, keep online devices (including mobile phones) out of bedrooms at night. Or disable their internet access for those time periods. No child needs to be contactable past their bedtime and if they can't get online, you know they can't be receiving inappropriate contact.

The means by which your child can be contacted extends far beyond email and standard messaging apps.

Other means of communication online may include:

- commenting on social media posts;
- participating in live-streaming events;
- using random-connection video conferencing platforms;
- in-game chat facilities (both text and audio);
- online forums and message boards;
- reviews and feedback pages.

Adults looking to connect with young children are always seeking new ways to make contact, even exploiting seemingly harmless features like shared playlists on Spotify, or signposts on Minecraft.

reducing

CONDUCT

risks

Set up a family agreement

A family agreement is a way to start a conversation with the whole family about how you all use the internet, and to start discussions together around how to behave in a positive way when online, whether this is at home, at school or at a friend's.

The agreement involves generating promises, positive statements about how your family want to look after each other online and how you should treat others online. It might include things like screen time, no mobiles at the dinner table or what to do if something goes wrong.

It needs to be clear both in terms of what you expect from the children and what they should expect from you. The idea is that it is created in collaboration with young people, rather than them being told what to do. When children understand the reasoning behind a rule and have helped formulate it, they are more likely to abide by it. Model how this will work by including your own conduct. Perhaps you'll agree not to post images of them online without their consent.

Technology changes and children age, so you should regularly review the agreement. Change things that better reflect your child's maturity and introduce or remove what needs removing.

Limit screen time

Young people find it difficult to track their own consumption of online content, so it is a good idea to configure Parental Controls to limit their screen time.

Time controls are available on most devices under a range of names: "Screen Time", "Digital Wellbeing", "Free Time" or general "Parental Controls".

Conduct means the way people behave online. Some online behaviour can increase the likelihood of a child experiencing harm, or being the cause of harm to another.

Keep Devices Out of Bedrooms

In a shared space, children are less likely to behave inappropriately and you're more likely to spot problems.

Generally, if you wouldn't be comfortable with your child being with a potential boyfriend/girlfriend in their bedroom with the door closed, you shouldn't feel comfortable with them having online devices there.

This advice also goes for games consoles, online or not. Children find moderation difficult and have a poor sense of how long they spend on a device. Playing video games can often replace much needed sleep with some children.

Honour minimum ages

All social media platforms and multi-player games come with a minimum user age, typically 13. Allowing a child to bypass these age checks gives them access to environments not intended for them and sets a dangerous precedent that rules designed to protect them can be ignored as they wish.

If you MUST allow your child on a platform before they are of age, do the process yourself. Have the discussion about why you're allowing it and your expectations on their behaviour. Make overriding the age limit seem a significant action so they don't feel they can do it themselves next time.

USEFUL LINKS

Internet Matters
https://www.internetmatters.org/
From age-specific online safety checklists to guides on how to set parental controls on a range of devices, you'll find a host of practical tips to help children get the most out of their digital world. This includes help for setting up Family Agreements.

Common Sense Media
https://www.commonsensemedia.org/
Since 2003, Common Sense Media has been the leading independent source for media recommendations and advice for families. Their advice covers movies, TV, books, apps, games & YouTube channels.

Childnet
https://www.childnet.com/
Childnet is a UK-based charity who work with others to make the internet a great and safe place for young people. Their website has some help on how to have conversations with your children about the internet.

YouTube Kids
https://www.youtubekids.com/
YouTube Kids provides a more contained environment for kids to explore YouTube and makes it easier for parents and caregivers to guide their journey.

Rate My YouTuber
https://natterhub.com/rate-my-youtuber
Searchable list of many (but not all) of the most popular YouTube channels. It offers insight into their content and suitability based on first-hand experiences.

PEGI
https://pegi.info/
PEGI provides age classifications for video games in 38 European countries. Their website allows you to look up the classification and brief details for any published game across all platforms.

UK Safer Internet Centre
http://www.saferinternet.org.uk/
This site contains advice on how to use the internet and new technologies safely and responsibly as well as a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies.

Childnet International
http://www.childnet-int.org/
A non-profit making organisation working with others to help make the Internet a great and safe place for children. You can access Jenny's Story, Becky's Story and Let's Fight It Together (the cyberbullying DVD) in addition to other online resources from this site.

Digizen
http://www.digizen.org/
A site about recognising and dealing with online hazards, setting up safe profiles on social networking sites and understanding how to manage personal information.

Think U Know
http://www.thinkuknow.co.uk/
Provides the latest information on the sites young people like to visit, mobiles and new technology. It's separated into different age groups: 5-7 years, 8-10 and 11-16 years. There is also a 'parent/carer' and 'teacher/trainer' section. It discusses what's good; what's not so good about the internet; about online risks and what you can do about them.

Google Family Safety Centre
http://www.google.co.uk/familysafety
Provides parents and teachers with practical tools to help them choose what content their children see online. Look out for the video tips on how to set up safe searching on Google and YouTube.

BBC - OWN IT
https://www.bbc.com/ownit
A site designed to teach younger children about some of the pitfalls of the internet in a fun-way; using cartoons, quizzes and games