



Education Safeguarding Team

WHSG Parents Online Safety



<<< WARNING >>>

- *This is a parents online safety presentation*
- *This presentation is not suitable for children*
- *We will be talking about behaviours that we do not want children to copy*
- *We talk about apps that we do not want children to use*



Ofcom will have powers to take action against companies which do not follow their new duties. Companies will be fined up to £18 million or 10 percent of their annual global turnover, whichever is greater. Criminal action will be taken against senior managers who fail to follow information requests from Ofcom.

In the most extreme cases, with the agreement of the courts, Ofcom will be able to require payment providers, advertisers and internet service providers to stop working with a site, preventing it from generating money or being accessed from the UK.

The Act takes a zero-tolerance approach to protecting children by making sure the buck stops with social media platforms for content they host. It does this by making sure they:

- **remove illegal content** quickly or prevent it from appearing in the first place, including content promoting self-harm
- **prevent children from accessing harmful and age-inappropriate content** including pornographic content, content that promotes, encourages or provides instructions for suicide, self-harm or eating disorders, content depicting or encouraging serious violence or bullying content
- **enforce age limits** and use age-checking measures on platforms where content harmful to children is published
- ensure social media platforms are more transparent about the **risks and dangers posed to children** on their sites, including by publishing risk assessments
- **provide parents and children** with clear and accessible ways to report problems online when they do arise

What else is new?

Online Safety Act 2023

New Offences

Cyberflashing

Illegal to send unsolicited sexual images intended to alarm or distress.

Epilepsy trolling

Criminal to send flashing images aiming to trigger seizures or cause distress.

Threatening communications

Sending threats of serious harm, death, or violence is a standalone offence.

Encouraging serious self-harm

Offence to promote or encourage serious self-harm online, even if harm doesn't occur.

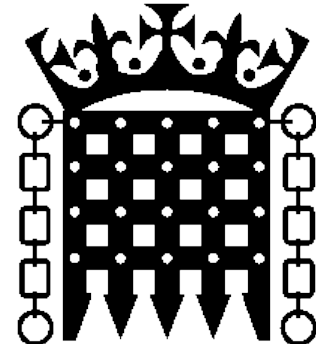
Sharing intimate images (including deepfakes)

Offence to share or threaten to share sexual images without consent, including AI-generated content.

What does the Law say

Communications Act 2003

Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character or sending a false message for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable on conviction to imprisonment.



Computer Misuse Act 1990

You can not impersonate or steal someone else's identity online. This means that writing a status on social media pretending to be your friend, is technically against the law.



Unauthorised access to material stored on an electronic Device

.

The Education Act 2011

Be Aware

The Education Act 2011 makes it an offence to publish the name of a teacher who is subject to an allegation until such a time as that they are charged with an offence. All members of the community need to be aware of the importance of not publishing named allegations against teachers online as this can lead to prosecution.





Department
for Education

Teaching online safety in school

**Guidance supporting schools to teach
their pupils how to stay safe online,
within new and existing school subjects**

June 2019

1. Self-image and Identity
2. Online relationships
3. Online reputation
4. Online bullying
5. Managing online information
6. Health, wellbeing and lifestyle
7. Privacy and security
8. Copyright and ownership

Education for a Connected World - 2020 edition

A framework to equip children
and young people for digital life



4 - 7

7 - 11

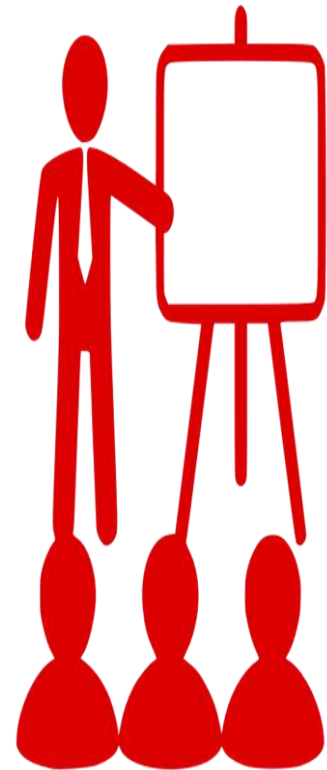
11 - 14

14 - 18

How to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

Schools can help pupils consider questions including:

- is this website/URL/email fake? How can I tell?
- what does this cookie do and what information am I sharing?
- is this person who they say they are?
- why does someone want me to see this?
- why does someone want me to send this?
- why would someone want me to believe this?
- why does this person want my personal information?
- what's behind this post?
- is this too good to be true?
- is this fact or opinion?



On Line Dangers

- Strangers - Fake Profiles & Pictures, Dating Apps
- On line Scams – Financial, Sextortion, ID theft
- Cyber bullying, Trolling
- Grooming/Sexual Exploitation/Radicalisation
- Inappropriate content - Pornography, Suicide, Self harm.
- Gambling, Violence, pro-anorexia,

Inside TikTok

internet
matters.org

*A short form mobile video
platform available in over
150 countries around the world*

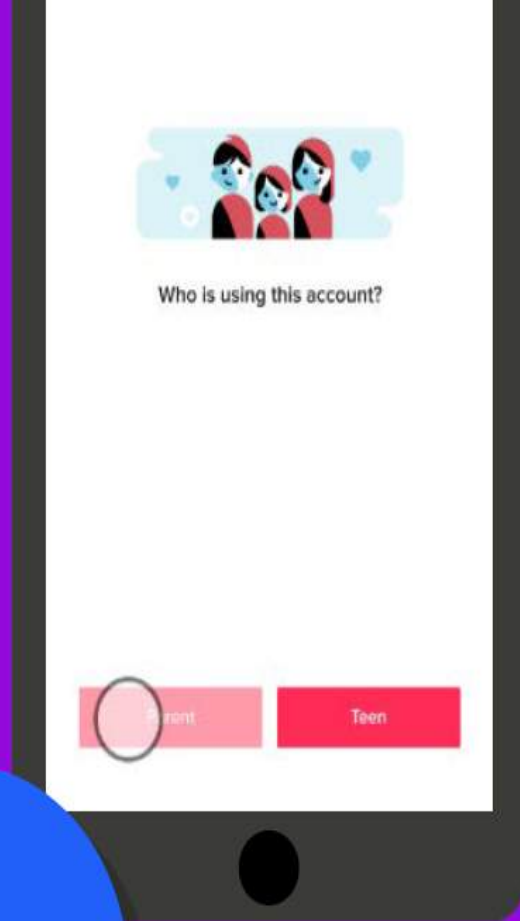
13

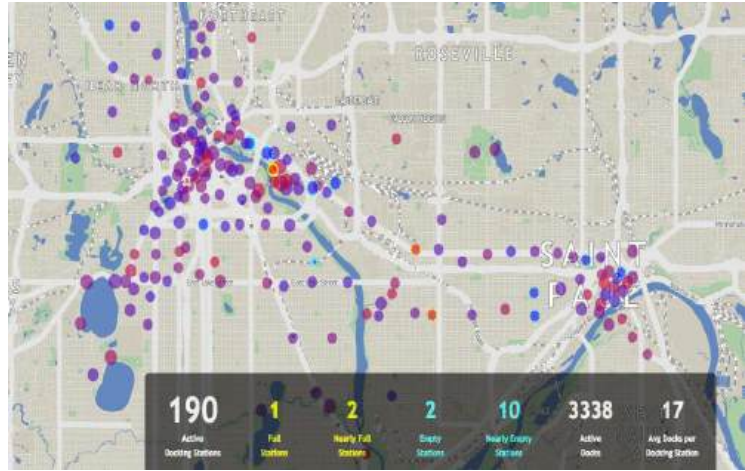
The minimum
age for users
is 13



Family Pairing

Family Pairing links a parent's TikTok account to their teen's and once enabled, they will be able to **control Digital Wellbeing features**, including: Screen Time Management, Direct Messages and Restricted Mode.





SNAP MAPS

PUT YOUR SETTINGS TO **GHOST** MODE SO AS NOT TO SHARE YOUR LOCATION WITH OTHER PEOPLE



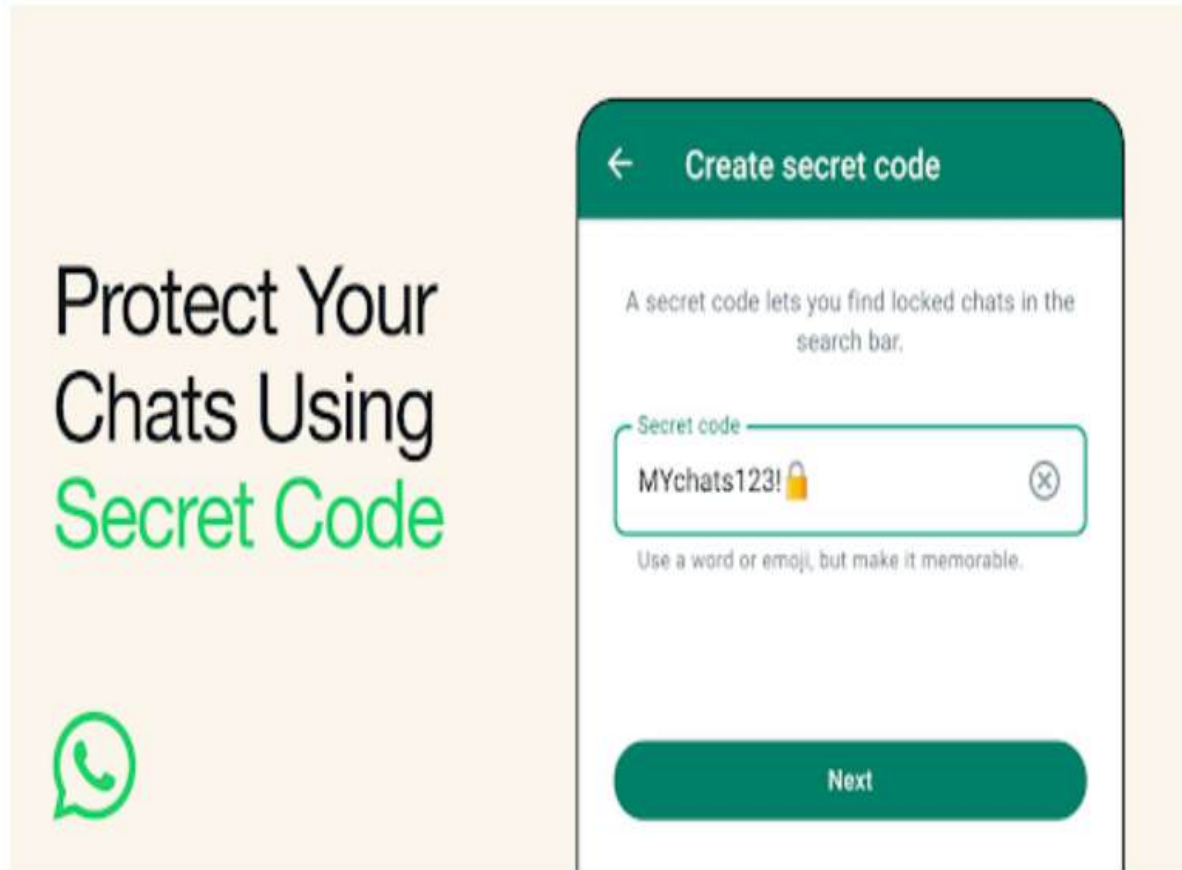
WhatsApp

Six Years ago WhatsApp raised the minimum age to use its service from **13 to 16 across the EU** in order to comply with GDPR.

It's worth noting that on 11th April 2024, WhatsApp changed their minimum age to allow children aged 13+ to use the service (down from 16).



Introducing Secret Code for Chat Lock



Earlier this year we rolled out [Chat Lock](#) to help people protect their more sensitive conversations. Today we're launching secret code, an additional way to protect those chats and make them harder to find if someone has access to your phone or you share a phone with someone else.

Age Restrictions for Social Media Platforms

(Ages specified in terms as of 2014)

Twitter
Facebook
Instagram
Pinterest
Google+
Tumblr
Reddit
Snapchat
Secret



LinkedIn



WhatsApp



Vine
Tinder



Path



YouTube
Keek
Foursquare
WeChat
Kik
Flickr





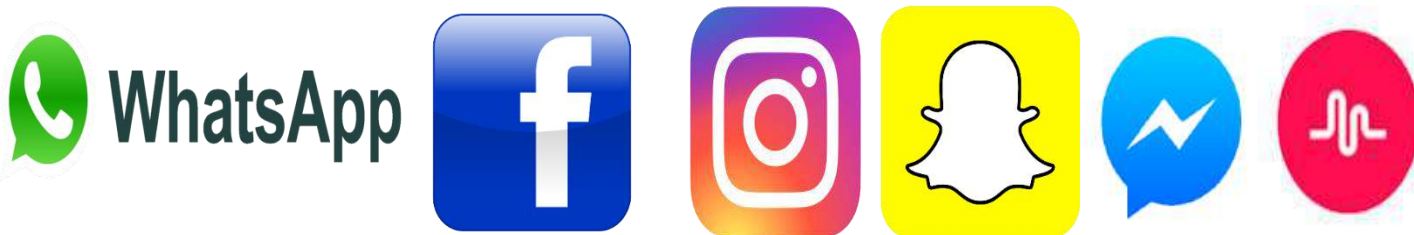
Ofcom research shows that more than a fifth of children aged 8-17 have an adult online profile (i.e., with a user age of at least 18+)

and a third of children aged 8-15 have one with a user age of 16+.

There are good reason for this age restriction to be in place. For example:-

- Inappropriate content,
- Lack of maturity to use the site safely,
- Exposing them to harmful content,
- Risk of being contacted by Sexual predators,
- Creating an online profile which will be hard to remove in the future,
- Placing added pressure on the child to deal with situations beyond their years.

The list goes on but as parents you need to be aware of the safety implications by allowing your child access to Social Media at such a young age.





1

Know your Online Friends, If you do not know them in the real world then they are strangers!!!!

Reques

INTERNET



Sextortion

Tragic toll of nude photos sextortion scandal laid bare: How **'100 children a day'** are falling victim to scammers.

Police forces with the biggest increase in sextortion:

According to an investigation by the Mirror, these are the police forces that saw the biggest jump in sextortion between 2020 and 2023.

- Greater Manchester Police: 2700%
- Gwent Police: 800%
- Bedfordshire Police: 778%
- Cumbria Police: 600%
- Avon and Somerset Police: 524%
- Cambridgeshire Police: 506%
- Northamptonshire Police: 500%
- Kent Police: 469%
- Leicestershire Police: 443%
- West Mercia Police: 431%

Online Grooming Offences Reach Record High

As a result of FOI requests to all police forces across the UK, the NSPCC have obtained data which shows that online grooming offences are at a record high with 7,623 offences recorded from January to March this year alone. Remember, these are the **KNOWN** figures, the real number is likely to be much higher. Where a tech platform was identified, around 40 percent took place on **Snapchat**, 9 percent on **WhatsApp** and 9 percent on **Facebook** and **Instagram**. Where the gender was known, girls made up 80 percent of victims, with the **youngest age being 4**.





According to the Child Exploitation and Online Protection Centre most child sexual exploitation offences take place online. These offences include deceiving children into producing indecent images of themselves, engaging in sexual chat online or sexual activity over a webcam.

Analysis by the centre reveals that 13- and 14-year-olds represent the largest single victim group.

Online Predators using Live Streaming to abuse Children

“This year, NCA analysts have warned there are whole online communities of sexual predators who devote themselves to finding and tracking down children on the internet, so as to bully and coerce them into abusing themselves sexually.

“These criminals can now groom a child who is in the apparent safety of their own bedroom, into making videos of the most serious kinds of abuse.”



SEXTING

YOUTH PRODUCED SEXUAL IMAGRY

- By Children and young people under the age of 18.
- Of Children and young people under the age of 18 that are of a sexual nature or are indecent.
- The images are shared between young people/or adults via a mobile phone, hand held device or website.

Around 1 in 7 young people have taken a semi-naked/naked picture of themselves.

Over half went on to share the picture with someone else.



NSPCC  TM

Cruelty to children must stop. FULL STOP.

childnet.com APP



[Info and advice](#) 

[Get support](#) 

[Toolbox](#) 

[Get involved](#) 

[Your locker](#) 

[Sign in](#)

You are here / [Home](#) / [Info and advice](#) / [Bullying, abuse, safety and the law](#) / [Online and mobile safety](#)

[Search Childline](#) 

REPORT REMOVE

Report Remove is here to help young people under 18 in the UK to confidentially report sexual images and videos of themselves and remove them from the internet.

On this Page

[How Report Remove works](#)

[Make your report](#)

[Help with your report](#)

[Watch: Report Remove](#)

[Get more support](#)



How do I remove a nude image of myself?



If you are under 18 and an explicit or nude image of you has been shared online, we can confidentially help you to get it removed.

Follow these 3 simple steps:

Download Yoti – The easiest, most secure way to prove identity. Take a selfie and then a photo of your ID, like a passport, to verify it's you.

Report: Give details of the nude image and where it could be online (don't worry if you don't know all the details)

Remove: We'll then review the details and the IWF will work to have it removed

The IWF (Internet Watch Foundation) use image hashing technology. This means each photo has its very own ID and using this ID it can identify the image, and have it removed, wherever it is uploaded to the internet.

Guidance for Schools – March 2023



Sharing nudes and semi-nudes: advice for education settings working with children and young people

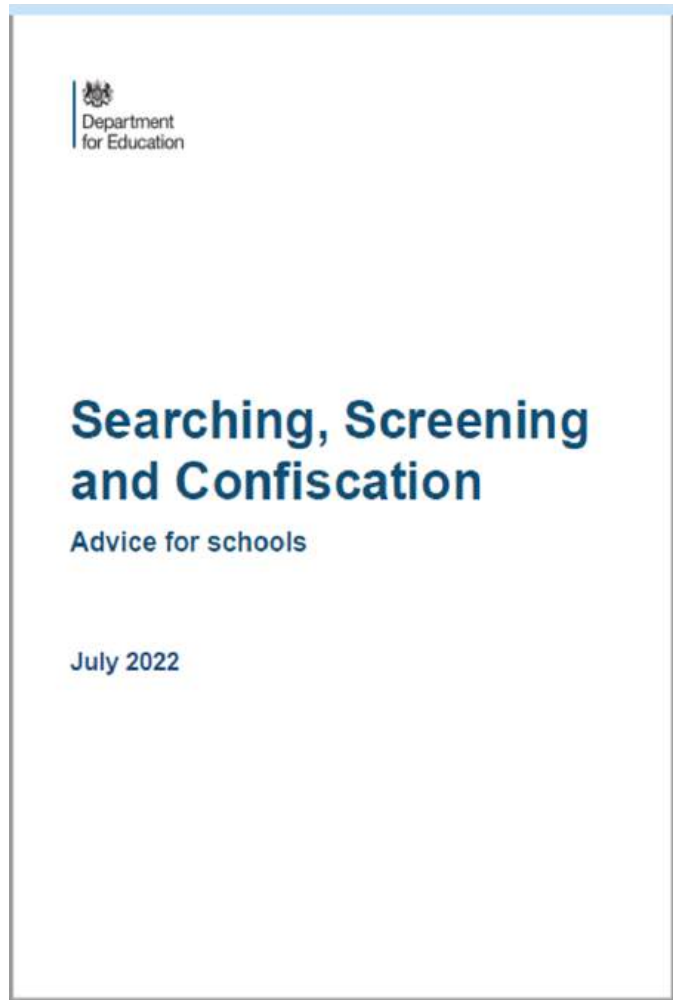
Responding to incidents and safeguarding children and young people

UK Council for
Internet Safety

This advice outlines how to respond to an incident of nudes and semi-nudes being shared, including:

- risk assessing situations
- safeguarding and supporting children and young people
- handling devices and images recording incidents, including the role of other agencies
- informing parents and carers

Searching Electronic Devices



Searching for devices

The Searching, Screening and Confiscation advice for schools highlights how the Education Act 2011 gives schools the power to search pupils for devices, search data on devices. This power applies to all schools and there is no need to have parental consent to search through a young person's mobile phone.

If during a search a teacher finds material which concerns them and they reasonably suspect the material has been or could be used to cause harm or commit an offence, they can decide whether they should delete the material or retain it as evidence of a criminal offence or a breach of school discipline. They can also decide whether the material is of such seriousness that the police need to be involved.

We ALL leave a digital footprint

Once it's on-line it's
virtually impossible
to scrub out

.. and the data
on you will follow
you around for life



Reputation Management

Always be careful when you post something online or upload a photograph

Once it is sent or uploaded it may stay there for ever

If it is copied or resent, then you may never be able to remove it

When you apply for a University or your first job, you will probably be Googled.

Other people will be able to find out what you have said and done on Social Media,

Think before you click





of employers indicate that they are less likely to hire candidates whose social networking profile or tweets evidence unprofessional behavior.





Before You Post
THINK



T - is it True?
H - is it Helpful?
I - is it Inspiring?
N - is it Necessary?
K - is it Kind?

The graphic features a central smartphone surrounded by various social media icons including Twitter, Facebook, and Instagram. The text is presented in a clean, sans-serif font, with 'THINK' in a larger, bold, red font.

- Ollie Robinson set to be dropped by England after offensive tweets resurfaced
- Racist and sexist posts by the bowler from nine years ago have come to light

Before You Post

THINK



T - is it True?

H - is it Helpful?

I - is it Inspiring?

N - is it Necessary?

K - is it Kind?

Think
before
you post!



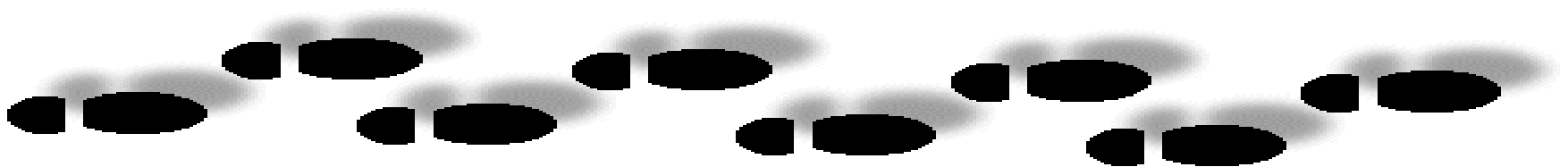
The key thing to remember is to take a moment to think before you post. That applies to comments and messages too! If anything or anyone ever upsets you online, always tell a trusted adult. They can help you feel better and help to find a positive solution to your problem.

So what can we do?



Digital Footprint

- Try googling yourself and your family, this will show your digital footprint.
- Click on images when googling to see what pictures of your family maybe out there.
- If you find something inappropriate then so can someone else.
- Google will remove personal information if requested to do so.





Google is rolling out the ability for Children, teens and their parents to request to have pictures deleted from the company's image search results.

- Anyone under the age of 18 or their parent or guardian can ask Google to remove an image from appearing in search results by filling out this request form.
- You'll need to specify that you'd like Google to remove "Imagery of an individual currently under the age of 18" and provide some personal information, the image URLs and search queries that would surface the results.



www.Commonsensemedia.org

Common Sense Media helps families make smart media choices. We offer the largest, most trusted library of independent age-based and educational ratings and reviews for movies, games, apps, TV shows, websites, books, and music

<https://www.internetmatters.org>

internet
matters.org



0-5



6-10



11-13



14+

Get Age-specific advice

Whatever their age, find simple, practical advice to keep children safe online.



TalkTalk



BBC

Google



Helping parents keep their children safe online

internet matters.org

Advice on Online Grooming

What do I need to know?

Groomers use **fake profiles** on **social networks** to **connect** with **children** and start to **build relationships with them**

Supporting families online

Get expert support and practical tips to help children benefit from connected technology and the internet safely and smartly.

[I need help with an online issue](#)



[I need to report something](#)



New hub to support children experiencing vulnerabilities

Helping them to stay safe online

- Partnership between SWGfL & Internet Matters
- Funded by the Home Office who recognised the risk that vulnerable children and young people face online during the Covid-19 pandemic
- Provides vital support for professionals, parents and young people themselves, with a particular support for children & young people who are experiencing vulnerabilities due to:
 - SEND
 - Care experienced
 - Gender & sexual identity issues (LGBTQ+)

INCLUSIVE
Digital Safety



Inside Inclusive Digital Safety hub: supporting parents and carers

LGBTQ+



Supporting a child identifies as LGBTQ online

Care experienced



Supporting a care experienced child online

SEND



Supporting children with SEND online

For each vulnerability:



Connecting and sharing online

Connecting & Sharing



Staying safe while browsing

Browsing



Online gaming

Gaming

Supporting children and young people with SEND online

Advice for parents and carers to help children with special educational needs and disabilities (SEND) stay safe online.



Connecting & Sharing

Although children and young people (CYP) with SEND are more at risk of contact and contact risks. Risks do not always lead to harm. It is likely that CYP may like to engage online while gaming or in a group chat, or may experience negative comments, but the key thing is to ensure they know how to recognise warning signs to prevent this leading to harm.

What you need to know

How to support your child (CYP) with SEND interacting with others online through social media or other platforms has become an important part of CYP lives and even more so for those with SEND.

The benefits

Connecting, creating and sharing with others online brings a range of benefits which can support a child's wellbeing including:

- Making and maintaining friendships which might be harder to do offline
- Being where they want to be without judgment
- Managing their emotions and seeking support
- Finding their tribe (of like-minded people)
- Being more independent
- Discovering new interests

The risks

Research shows that CYP with SEND experience greater risks when it comes to contact, contact or contact risks.

- **Contact** – being exposed to harassment or harmful content which may include bullying and abuse or harmful images, e.g. pornography, self-harm, etc.
- **Contact** – meeting strangers and being invited to high-risk situations online
- **Contact** – when a child receives a message or contact at the recipient of harmful content online

It is important to be aware that:

- CYP with SEND are **more likely** to experience online risks compared to those without any difficulties, particularly contact risks
- Examples of this include seeing under pressure and coercion. They appear to be **groomed upon and singled out**
- CYP with communication difficulties are **more likely to experience contact risks**
- Experiencing contact risks is also associated with a **greater risk of seeing harmful content and experiencing more aggressive behaviour** from their contacts

- Getting help to manage the risks that they may face
- What are they sharing with others?
- Why are they using or their sharing status a factor for them to experience online risks, to social apps made for under 18s

Key steps to protect CYP

Children are exposed to social media and the internet.

Digital family agreement – create a set of rules for what you expect your child to do and what they can do.

Digital safety – is a parent or carer's role to ensure that their child is safe online and that they are protected from harm.

Consent – most of the popular social media sites have a number of privacy and settings that you can set to control what your child can interact with online.

Wellbeing – both Android and iOS have a large range of accessibility features that you can use to help CYP get the most out of their experience online.

Checklist – schools regularly check up on what they do online and how they use the internet. It is important to have a checklist together.

Spending time on social media – a number of social apps and tools have been created to help CYP spend less time on social media and more time on their schoolwork.

Family & friends group – it is important to set up their social accounts together so they can have a family and friends group and they can help each other if they are having any difficulties that they are not sure how to deal with.

Where do young people go to be social?



Helping children experiencing vulnerabilities stay safe online

Visit www.internetmatters.org/inclusive-digital-safety-hub



Guide to Monitoring apps

With children accessing the internet on a range of devices, the job of protecting them from things they may not be ready for online can be a challenge.

In recent years, a wide variety of monitoring software solutions have appeared to allow you to see what children are doing online and set digital boundaries.

With the help of Pocket-lint's Andy Robertson, we've given tips on how best to use them and reviewed the top apps available.



Inside the guide

- What do monitoring apps offer families?
- What to consider when choosing monitoring apps?
- What are the top monitoring apps available?
- How can I make sure it's the best option for me and my child?

What do monitoring apps offer families?

Companies producing technology are making huge strides to empower and equip parents to play a crucial role in guiding children to digital health. Whether they are games consoles offering automatic parental controls based on PEGI ratings, routers providing apps to show you exactly who's doing what online, or even smartphone add-ons that let you track where your child is, there has never been more help for parents.



Epic Games Store parental controls

Controls & Settings guide

The Epic Games Store is a digital video game storefront for Microsoft Windows and macOS. Users can also use it to play games. Exclusive games include the very popular [Fortnite](#), [Fall Guys](#) and [Rocket League](#).






Manage cabined accounts for under-13s and learn how to use a PIN in the Epic Games Store to manage inappropriate game content based on age ratings.

[DOWNLOAD PDF](#)[EMAIL ME PDF](#)

What do I need?

An Epic Games account and access to gaming device

Restrictions you can apply

-  Chatting
-  Game Ratings
-  In App purchasing
-  Inappropriate content
-  Online games
-  Parental control
-  Privacy and identity theft
-  Purchasing





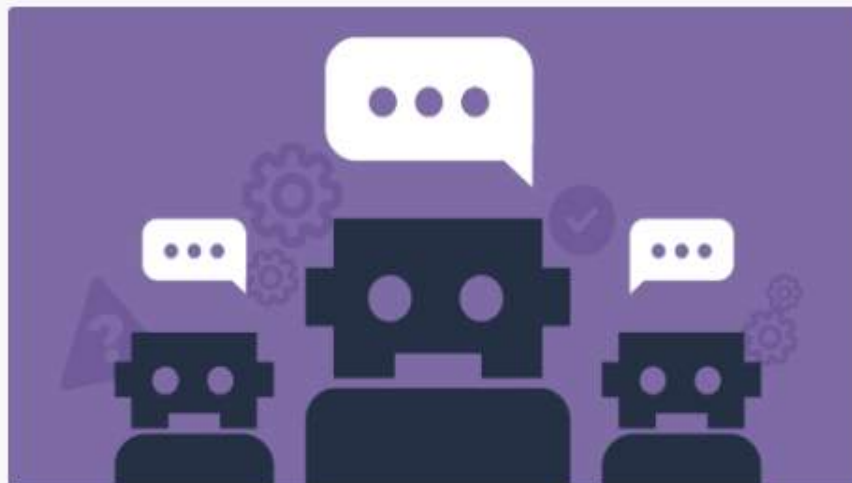
You are here: [Home](#) > [Resources](#) > Making the most of artificial intelligence – A parent's guide to AI tools

A parent's guide to using AI with kids

How to get the most out of AI tools

In this guide to AI, learn about the different AI tools like ChatGPT that are currently available. Then, explore how to support learning, creativity and even bedtime using AI at home.

Watch this space for more updates and guidance on the potential risks and benefits to AI coming soon.



[DOWNLOAD PDF GUIDE INSTEAD](#)

What's in this guide

53 likes

[SHARE](#)

- [What is artificial intelligence \(AI\)?](#)
- [Guide to AI tools](#)
- [Interactive parents' guide to AI tools](#)
- [AI words to know](#)
- [Other resources](#)



You are here: [Home](#) > [Resources](#) > [What is WhatsApp?: A safety how to guide for parents](#)

What is WhatsApp?

A safety how-to guide for parents and carers

With over 2.7 billion monthly users, WhatsApp is one of the most used messaging apps.

Find out what features you can use to help keep your child's personal information private.

[DOWNLOAD GUIDE](#)[SHARE](#)

The Thrive online resources



Teaching about digital wellbeing (SEND)

Teaching resources including video on digital wellbeing for young people with Special Educational Needs and Disabilities aged 11-17 years old.



Teaching about healthy online relationships (SEND)

Teaching resources including video on healthy relationships online for young people with Special Educational Needs and Disabilities aged 11-17 years old.



Teaching about online pornography (SEND)

Teaching resources including video on online pornography for young people with Special Educational Needs and Disabilities aged 11-17 years old.



Supporting young people with SEND

Advice for parents and carers of young people aged 11 and over with Special Educational Needs and Disabilities covering healthy relationships, digital wellbeing, online pornography and nudes. Part of the Thrive Online resources.



[Resources](#) [Blog](#) [Who we are](#) [W](#)

[Teachers & professionals](#) [Parent](#)

Our Projects

Thrive Online

Helping educators, parents and carers to support young people aged 11 and over with Special Educational Needs and Disabilities (SEND)

CEOP EDUCATION



Education from
the National
Crime Agency

Welcome to CEOP Education

The National Crime Agency's CEOP Education team aim to help protect children and young people from online child sexual abuse.

We do this through our education programme, providing training, resources and information to professionals working with children, young people and their families.

I am:

**A professional working with
children and young people**

**A parent
or carer**

**4-7
years old**

**8-10
years old**

**11-18
years old**

GUIDANCE

CyberFirst: How to stay secure online (11-14 year olds)

Interactive online security resources for 11-14 year olds.

What can you do now

- **Search yourself and your children online**
- **Check your and your children's privacy settings**
- **Use strong passwords**
- **Update software**
- **Think before you post**
- **Review apps and remove any you are not using.**
- **Ensure your child is creating a positive reputation.**
- **operate online in a way which would not cause embarrassment in the future or limit their life chances.**

TIPS FOR PARENTS/CARERS

When you buy a game console/Mobile phone/interactive toy, make sure you ask the vendor about its online capabilities. **Know what the equipment is capable of.**

Think about the location of the game console. Keep it in a common area if possible. A family room is best for monitoring and supervision. **Don't allow children to have internet enabled devices in their bedroom until they reach an age and maturity to keep themselves safe.**

Discuss the risks with your child. Don't wait for something to happen before you talk to your child about the potential risks of gaming online. **Ensure they have privacy settings activated and help them to understand why this needs to be done.**

Gaming sites/Social Media often have ways of reporting abusive chat and blocking unwelcome contact from other users. – **You should know how to do this.**

Ask your child what they are playing or what Social Media they are using. **Take an interest in your child's on line life** – just as you would if they were in a football team in the real world. Watch them playing and always keep lines of communication open.

Parents need to play their part

Educational settings and professionals should encourage parents to discuss online safety at home and to talk to their child about what they do online. Useful websites to signpost parents/carers to include:

thinkuknow.co.uk/parents

childnet.com

saferinternet.org.uk

parentinfo.org

internetmatters.org

nspcc.org.uk/onlinesafety

commonsensemedia.org

<http://www.iwf.org.uk>

www.askaboutgames.com

swgfl.org.uk



Have that Conversation



Keep that Conversation going



Cognus

No Limits on Learning

**Thank you for Listening
Have you any questions?**

Education Safeguarding Team

