

Online Grooming

What parents need to know

internet
matters.org

Grooming is when someone seeks to build an **emotional connection with a child** to gain their trust for sexual purposes. It happens both online and face to face.



What is online grooming?



Children may often meet people through **social and gaming sites** that aren't who they say they are so it's important to discuss the risks with them.



Once groomers have gained a child's trust they **may encourage them to share** sexual images, or videos of themselves, live stream, or arrange to meet.

XXX

XXX

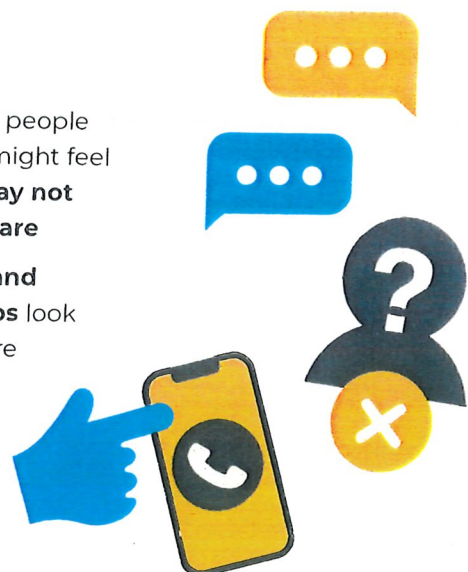
Groomers are **not always strangers** and sometimes children may not be aware that they are being groomed **believing they're in a relationship** with the person.

Ways to protect your child

Talk about it

Although a tricky subject to talk about with your child it is important that you start a conversation

- Show them where to get help if they are concerned and to **talk to you or a trusted adult** for support
- **Spend time discussing** where they interact with friends online and how and what they share with others
- **Explain how easy it is to pretend** to be someone else online, and why an adult may wish to approach them
- Remind them that the people they have met online might feel like friends but they **may not be who they say they are**
- Discuss what **healthy and unhealthy relationships** look like to make them aware



APP SAFETY

catch
22

WHATEVER YOU CHOOSE TO DO, DON'T DO NOTHING.

SOME PARENTS OR GUARDIANS FIND OUT TOO LATE THAT YOUNG PEOPLE HAVE BEEN ACCESSING INAPPROPRIATE PLATFORMS OR CONTENT.

Some devices have built-in controls which can be activated, or you can sync your child's phone to your phone so that you can see which apps have been downloaded;

- Google Family Link is a free android app for under 13s, which can be controlled by the parent's iPhone or Android phone.
- iPhone's iOS 12 offers controls at the operating system level.
- Net-aware.org.uk lets you check out any app before its downloaded and you can see independent reviews of the risks of any app.

Other options include:

	Quastodio	Free or £	Free version or premium plans available from £36 p.a. but no monthly payment option available. Daily reports about phone and laptop use, consoles not covered. Location tracker included. Blocker for certain apps. Requires setting up on each device separately. Good reviews on comparison sites.
	Net Nanny	££	Includes internet filter, scheduled access, activity alerts and reports but does not cover apps. Requires setting up on each device separately
	OurPact	££	Tracks calls, texts, social media use. High degree of parental control, including scheduling access to certain apps at certain times of day. Requires setting up on each device separately. Doesn't cover consoles or laptops.
	Kaspersky Safe Kids	Free or £	Web monitoring, time limits, app management. Laptops also covered but not consoles. Good value option.
	Norton Family Premier	££	Web filters, location tracking, time scheduling and monitoring for unlimited android and Windows devices.

SOCIAL MEDIA CHECKLISTS



Checklist for Snapchat	
Checklist for Facebook	
Checklist for TikTok	
Checklist for Instagram	

Age Restrictions for Social Media Platforms

What is the minimum age for account holders on these social media sites and apps?



Family agreement

A great way to start positive family conversations around safe and responsible internet use, and to agree clear expectations and boundaries.

Things to consider

Getting started

- What do we enjoy doing online?
- What apps, games and websites do we use the most?
- What devices, tech, toys or games do we have with internet access?
- Do we already have any rules about use of tech we want to include in our family agreement?

Managing time online

- How long do we spend on our devices?
- How does it feel when we use tech for too long?
- How do know when our screen use is interfering with family life?
- What can we do to help avoid overusing tech?

Sharing

- What is or isn't okay to share online?
- What should we check before posting images and videos online?
- How do we keep personal information belonging to ourselves and others safe?
- Do we need a family email address to use when signing up to new accounts?
- Do we know how to use privacy settings and strong passwords, and why these are important?
- How can we use features like livestreaming and disappearing content safely?

Online content

- What can we do if we see something online which seems unreliable or untrustworthy?
- When is it okay to download files, games or apps, or click on a link?
- Do we know what the age requirements, or ratings, on the games and apps we use mean?
- Do we need any restrictions on making in-game or in-app purchases?
- Which websites are okay for us to use?

Communicating online

- Who can we talk/chat/play games with online? Do we only know them online, or offline too?
- How can we keep ourselves safe when communicating with people who we only know online?
- How can we be a good friend when we are online?

If things go wrong

- What can we do if we feel uncomfortable or upset by anything we see or hear online?
- What should we do if someone we only know online asks us for photos, to meet up, or to share personal information?
- Do we know where the report and block buttons are online?

To finish...

- How could parental controls help our family?
- What will happen if one of us breaks the family agreement?
- When should we review our family agreement?

Once you've talked about your family's use of technology and the internet, think about what simple steps you can take going forward. We've given some examples for different ages below...

We agree to... (Under 11s)

I will use my tablet for _____ mins a day.

I will make sure the children's favourite games are bookmarked for them to get to easily.

Who is responsible for this?

Hannah and Izzy

Non

We agree to... (Pre-teens)

I will tell mum and dad when I see something that worries me.

I will put parental controls in place but review it as the children grow up.

Who is responsible for this?

Tom, Ella and Yasmin

Mum

We agree to... (Teenagers)

I will make sure all my social networking sites are private.

I won't post photos of our children without their permission.

Who is responsible for this?

Amar and Yusuf

Dad

Use the questions below to help guide your conversations, focusing on those most relevant for your family.

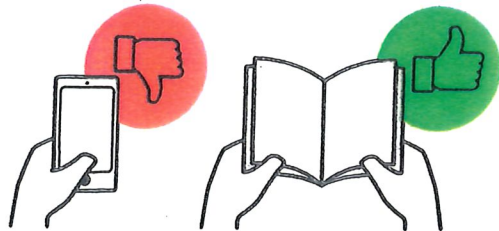
Turn over the page for a template where you can record your agreements and expectations in writing.

Five top tips to manage children's screen time

Help your child make the most of their time on and offline

1 Set a good example with your own device use

Children will tend to model their behaviours on you, so if you start reading a book, they may follow your lead.



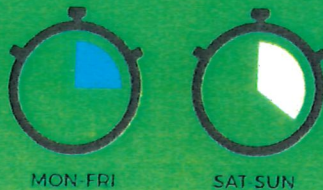
2 Talk together about the time they spend online

Understand what they're doing and explain your concerns.



3 Agree an appropriate length of time that they can use their device

Put in place a family agreement to set some boundaries and don't break them.

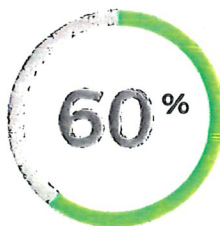


4 Get the whole family to unplug and create 'screen free' zones at home



5 Use technology and apps to help manage screen time

For example, the Forest app enables them to grow a beautiful forest each day they don't use their phone for a set amount of time. The iPad's 'Guided Access' limits the time you can access any given app, which can be great for younger children.



60% of parents are concerned their kids don't have interests outside the web



Parents of 12-year-olds are most concerned about lack of offline interests



Children aged between 11 and 16 post on average 26 times a day

How to create a great environment for kids to talk

1

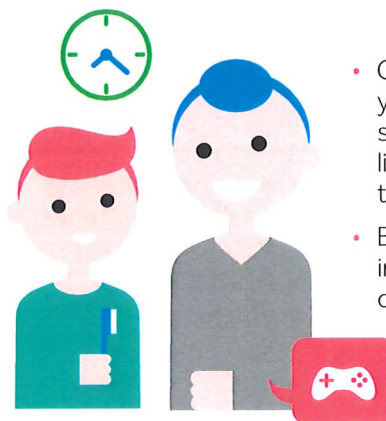
TALK EARLY AND OFTEN



- Talk with children from an early age to make it easier to maintain good communication
- Have bitesize conversations that are relevant to them

2

CHOOSE THE RIGHT TIME



- Choose to talk when you are due to spend some time together, like over a meal or during their bedtime routine
- Bring digital experience into normal, everyday conversations

3

OPEN UP AND SHARE TOO



- Model the behaviour you want them to show by sharing about your day
- Be open and encouraging to make them feel supported

4

CREATE A SAFE SPACE FOR YOUR CHILD



- Ask open-ended questions
- Ensure that your child feels listened to rather than cornered
- When they start talking, hold off with questions and really listen
- Be prepared, calm and patient with them

Further resources

www.commonsensemedia.org

www.thinkuknow.co.uk

www.nationalonlinesafety.com

www.lucyfaithfull.org.uk

www.internetmatters.org

Google family Link-

Family share. www.apple.com/uk/family-sharing/

Facebook –Derbyshire Police Online safety

Twitter -@DigitalPCSO

A PARENT'S GUIDE TO:

Moving to secondary school

Online safety tips to support children



internet
matters.org

InternetMatters
internetmatters
@im_org



What are kids doing?

- It's a time when children are beginning to **make deeper social connections** for the first time and learning how to **interact with each other online** which can be overwhelming.
- **The Smartphone becomes a status symbol** and an important tool to stay connected to their friends but it also puts them under **pressure to interact**.
- School interactions with friends **cross over into the online world** and at times it can be challenging to balance this with school work and other activities.

Online activities

- **Socialising online** on a range of social apps
- **Watching TV online** through YouTube
- Building their digital footprint by **sharing details about their day to day life** with friends and family or people they've met online
- **Gaming online** with friends regularly
- **Doing homework** through video chats with friends
- **Taking part in online challenges** with friends

What risks and challenges do they face?

As they become more active online, the probability that they will face an online issue increases.

60% of children in early years of secondary school experience a range of peer-to-peer online threats from being ridiculed in a group chat to harassment on social media*.

*Source: University of Suffolk Online peer-to-peer abuse report – June 2018



Screen time

'Everything in moderation' applies to the screen time debate when it comes to 'how much is too much screen time'.

Research tells us that children's brains, behaviour and sleep can be affected by how much time they spend on screens.

What can you do to help?

The challenge is helping children to be able to focus on what they are meant to be doing online

- **Discuss how** screen-time is affecting their overall wellbeing
- Set some **digital boundaries** and help them be in control of their tech

- **Make them aware** that most apps, games and devices are designed to keep them watching and playing
- **Stay engaged** in what your child is doing to help them use a wide range of media from safe sources

20
HOURS

the amount of time 12 - 15 year
olds spend online in a week

Support from schools

Schools can follow a framework that guides children on issues around wellbeing, health and as part of this they give children strategies to manage screen time to avoid the negative affects.



SIMPLE STEPS TO PROTECT YOURSELF, YOUR INFORMATION AND YOUR MONEY



Keep up to date!

Quite simply, our first line of defence against cybercrime, are the devices we use to access internet and email. So whatever devices, operating systems, software or apps you use, always ensure you are running the most up to date versions. Updates include security patches to fix vulnerabilities! If you can, select 'Auto Update'. Windows 8.1 users, this will become unsupported from January 2023 – you need to start planning your upgrade.

Antivirus

Make sure, as a minimum, you have any default AV running and make sure you are always running the most up to date version running. If you can, select 'Auto Update'. Mobile devices do not need AV installing.

Passwords

In a nutshell, you need to have a different password for everything you log in to. Make sure you're using [#ThreeRandomWords](#) to create a strong, separate password for each account, adding uppercase letters, numbers and symbols for complexity. Consider installing a Password Manager App. You can save passwords in browsers, but this should only be where you are the only person using that device.

<https://www.ncsc.gov.uk/cyberaware/home#action-2>

To help with the problem of remembering passwords, we advise considering downloading a "Password Manager" App. If that's not for you, consider noting down your username and a hint/reminder of your password. If you need to note this down in full, it's very important that this is kept safely, away from your devices and not accessible to others.

Protecting your online accounts

www.haveibeenpwned.com – check to see if your details have been compromised in known data breach incidents. Click on the three lines and opt for 'notify me' – you will be contacted anytime your passwords are found to be available in a new breach, allowing you to immediately change your passwords to protect your online accounts.

#2FA Turn it on!

Most email accounts, shopping and social media accounts will allow you to choose 2 Factor Authentication (2FA) in the security settings. It means you'll need to carry out an extra step to log in if you are using a different device or from somewhere new, but it means that ONLY you will be able to log in to your accounts!

For step by step instructions on how to set this up for different platforms, visit www.2fa.directory

If the worst should happen, here is some advice on recovering a compromised account

<https://www.ncsc.gov.uk/guidance/recovering-a-hacked-account>

BEWARE of phishing emails and text messages!

ALWAYS #TakeFive and REMEMBER! – emails, texts and phone calls can all easily be spoofed. NEVER assume any contact is genuine until you have verified that it is. **Don't click** on links in emails or open attachments unless you are certain they are safe.

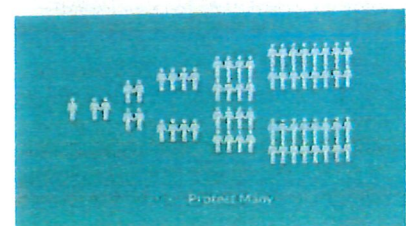
If an email relates to an account issue of ANY sort, always log in via a browser or an app – **NEVER** click on a shortcut in a text or email to log in or "resolve" an issue to ensure you avoid fake, copycat websites.

Did you know that you can forward ANY suspected phishing emails to report@phishing.gov.uk; and suspicious texts can be forwarded to 7726 (spells SPAM on your keypad)

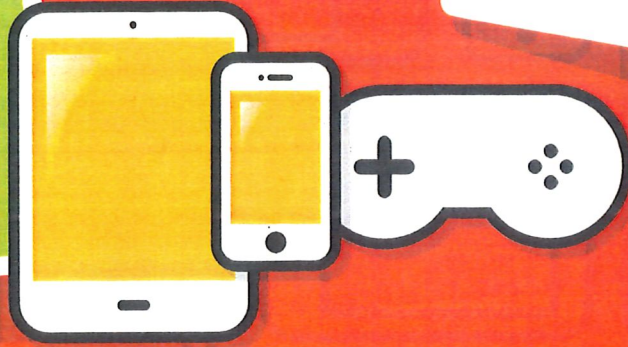
Courier Fraud

Neither the Police nor Banks will ever contact you to:

- transfer money to a safe account;
- withdraw funds for safekeeping;
- assist with a covert investigation;
- purchase high value items or jewellery;
- OR collect cash, bank cards or PIN numbers



BE SMART ONLINE



S

SAFE

Keep your personal information safe. When chatting or posting online don't give away things like your full name, password or home address. Remember personal information can be seen in images and videos you share too. Keep them safe to keep yourself safe.



M

MEET

Meeting up with someone you only know online, even a friend of a friend, can be dangerous as this person is still a stranger. If someone you only know online ever asks you to meet up, for personal information or for photos/videos of you then tell an adult straight away and report them together on www.thinkuknow.co.uk

THINK
U
KNOW
CO.UK

A

ACCEPTING

Think carefully before you click on or open something online (e.g. links, adverts, friend requests, photos) as you never know where they may lead to or they may contain viruses. Do not accept something if you are unsure of who the person is or what they've sent you.



R

RELIABLE

You cannot trust everything you see online as some things can be out of date, inaccurate or not entirely true. To find reliable information compare at least three different websites, check in books and talk to someone about what you have found.



T

TELL

Tell a trusted adult if something or someone ever makes you feel upset, worried or confused. This could be if you or someone you know is being bullied online. There are lots of people who will be able to help you like your teachers, parents, carers or contact Childline – 0800 11 11 or www.childline.org.uk



BE SMART WITH A HEART

Remember to always be smart with a heart by being kind and respectful to others online. Make the internet a better place by helping your friends if they are worried or upset by anything that happens online.





Use a **strong password**



Change settings to **private**



Use an **alias** and avoid **personal pictures**



Consider the **minimum age**



Don't include date of birth and other **personal information**



Don't accept **friend requests** from strangers



Switch off **location services**



Show your child how to **block** and **report**



Tell them to think before they **post**