

# Online safety

information for  
parents and carers

## About this Nutshell

Do you worry about what your children are up to on social media; how long they are online; and whether they should have a mobile phone at all?

The NPFS gets lots of questions about these sorts of issues. So, we've written this Nutshell to help you:

- Think about the benefits, as well as what you're concerned about
- Know what to look out for so that, whatever your children are doing, they are not taking risks
- Encourage your children to tell you if something's wrong, for example if they're being bullied on social media

You can also find sources of information for keeping devices secure in our helpsheet. [npfs.org.uk/downloads/securing-your-devices](https://npfs.org.uk/downloads/securing-your-devices)

Technology and what we can do with it changes all the time. There are some ideas below about where to go for information about latest trends, or if you want to speak to someone about any concerns. There are tips for handling some common issues. And you may find some ideas for helping you stay safe online too. You won't get everything right. But the best way is to take a practical approach based on your child's age and stage, their needs and what they are doing.

One of the best things you can do for your children is to get them to think about online behaviour. You can help your children see the internet as a 'place' with a set of rules. Just like they adapt their behaviour when they are in school, or at the cinema, or even a fancy restaurant, explain that the internet is also a place where there are ways in which they should act properly, and there are consequences if they don't. That applies to all of us.

### See NPFS Clicked materials

<https://bit.ly/2KIYTmh>

## There are pluses and minuses

We live a lot of our lives online: for learning, playing games, shopping, meeting friends, making new friends, doing hobbies, finding courses and jobs, and much more. There are massive benefits to how easy it is for us to connect with others, all over the world. But there are also some downsides. For example, it makes criminal behaviour such as online fraud easier too. The potential for exploitation is even greater as there are so many more people within reach.

The main difference between what we do on and off the internet is that, on the internet, there's a record. It might sound a little scary, but it's important that young people understand that things are kept on the internet, and that there is a trail, which other forms of communication don't necessarily have.

Technology and its applications change constantly. While this can make for better experiences, speedier access to friends and games, and more, it can be hard for parents to keep up with and relate to. It's good if you can keep up to date with the change: the good as well as the bad. In that way, you can help your children get the most out of what's around, and minimise any risk while they do so.

Children and young people's brains also change and grow over time. While they are developing, they don't understand risks or see consequences in the same way as adults. It's the job of parents to help young people make good choices, to allow them to take reasonable risks and to make mistakes. But it's also up to us to give them boundaries so that they are not in real danger. That will stand them in good stead for all aspects of their lives.



## Parents are role models

Parents are role models for children. For example, your children will notice when and how long you spend looking at your screens; how careful you are about sharing details or protecting passwords and privacy settings; and how you behave on social media. If you want your children to stay safe and be internet-savvy (or cyber resilient) you have to do the same. Parents are just as likely to fall for scams, such as online fraud, as children, who might believe that the people they meet online are who they say they are.

What children and young people do online, and how you support them, depends on their age and stage. Whatever their age, encourage your children to be open with you so you can understand them and their world.

## How to keep up to date

**What does cyber resilience mean?**

**What games are children playing?**

**Are there costs?**

**Are there links to gambling?**

**How does grooming happen?**

**How much money are their favourite vloggers making?**

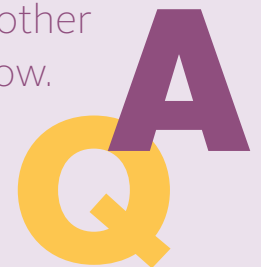
**How are they influencing your child and is that OK?**

**Why is it good to have a positive digital footprint?**

**How can children use Instagram or Tik Tok safely?**

**And what's around the corner?**

You can find the answers to these questions and more at [parentinfo.org](https://parentinfo.org) and the other links below.





## Some tips

### **Respect your child**

If you listen to your child and show that you understand and trust them, they are more likely to be open with you, and to confide in you if they are in difficulty.

### **Take an active interest**

You may not be very interested in Fortnite or Minecraft, but lots of young people are. Show an interest in what they are doing: the games they are playing; apps they are using; who they are following, so you know what they are about and their appeal. Parents tell us that they worry about the amount of time their children spend on games; some of the content (especially when it involves guns and killing); and who else might be playing. Some questions to ask yourself and them are:

- What are they doing online?
- Can you share some of this time with them?
- Can you play or watch with them?
- Do you know how long it takes them to play their favourite game, and is that a problem?
- Do you, and they, know who is playing with or watching them?

### **Do digital things together**

Whether it's watching a film or Skyping grandparents, you can help create good habits by doing these sorts of things with your children.

### **Learn from your children**

If your children are using social media apps like Instagram or Tik Tok, the best way for you to learn about them is to ask your children how they work. Children are often glad to teach their parents. It's a great way to learn about the app itself and also find out how your children interact with their friends and others on social media.

### **Agree the rules for your family: together**

What are the rules for your family? These should cover what, when, where, for how long, and who with. But do these rules feel more like sanctions to your children? If your children are old enough, it's good if you can agree the family rules together. It means that your children are more likely to comply with them. The sorts of questions to discuss are:

- How flexible are the rules?
- Does homework count as screen time?
- At what age can your children use certain technology or apps/games/activities?
- Does this increase as they get older?
- What happens if they break the rules?
- What should they do if something bad is happening to them?

### **Create positive environments**

You can and should create boundaries around what children are doing and what they might be exposed to. This includes:

- Knowing how to, and then using, parental control settings on phones, tablets, consoles
- Ensuring that children can't make payments
- Providing a family email address if they are filling in online forms
- Making sure that PCs, laptops and so on are used in the shared areas of your home such as the living room or kitchen
- Not allowing phones and other tech in bedrooms, especially not overnight

### **Minimise unnecessary conflict**

If you're not happy about some aspect of what your child is doing online, think about what's bothering you. Is it to do with being online, or their behaviour more generally? If it's dinner time, and they are busy playing a game, you could find out how long the game will last rather than simply making them stop. It might be a few more minutes rather than hours. It might be very frustrating for your child to end a game, just before it's due to finish.

### **Deal with the behaviour and not the hardware**

When children break the rules or do things their parents aren't happy about, parents sometimes react by taking away their phones and tablets. This tends to be counter-productive. Children are really attached to these items: they are their social life, their link to friends, their music, and more. When these are taken away from them, it can make them feel sad, angry and isolated, as if they've lost part of themselves. And if they're worried about you taking their device from them, they'll be less likely to talk to you about any online concerns. It is better if you can discuss the behaviour with them rather than opting for a sanction that feels to them like extreme punishment.

## Remember the positives

There are many positives about the digital world and it's important to remember what these are. For example, if you live in a very rural place with few activities or public transport, the internet can keep your children connected to their friends and family and to all sorts of opportunities for learning and fun. There are many and growing opportunities for young people who want to work in digital technology of some kind, including cyber security. The opportunities are global and they are well paid.



## Be aware of the problems

The sorts of problems that come up are many and varied and include:

- Being exposed to pornographic material
- Over-sharing personal details and intimate pictures
- Stalking, bullying and harassing others on social media
- Bullying and shaming through 'likes' and 'unfriending'
- Sharing others' personal information without permission, known as 'doxxing'
- Grooming young people for the purposes of exploitation and causing harm
- 'Phishing' scams that trick them into clicking on links that download damaging software, or take them to dodgy websites
- Encouraging young people to take part in gambling

Some of these are illegal; others are deeply distressing. Depending on what's happened, it may be possible to get protection under the law. If abuse involves someone under 16, the police and other authorities would see this as a child protection issue.

## The basics of cyber resilience

There's lots of information around about how to protect children and how they should protect themselves and their tech. Depending on their age, this includes:



**Knowing about passwords and how to make them secure**



**Knowing what and what not to share**



**Not giving out personal details**



**Settings**

This includes privacy, geolocation, parental locks, Wifi in public places. You can find more information on settings, and keeping devices secure, in our helpsheet. [npfs.org.uk/downloads/securing-your-devices](https://npfs.org.uk/downloads/securing-your-devices)



**Spelling out the risks**

People they meet online:

- might not be who they say they are
- might not have their best interests at heart
- might pretend to be other children interested in a game in order to find out things about them



**Warning them never to meet "online friends" in person**

Anyone they have met through the internet should not be met without supervision. Remember that many people meet their partners though online dating so square that up logically with your children and explain how people go about minimising risk



**Knowing about grooming**

Things do go wrong and it's important for your child to know that even if they have taken risks, broken the rules, or done something that made them vulnerable, that doesn't mean that they caused or invited any harm, or wanted to be harmed.



## More information

These websites have helpful information and links, including by the age of the child.

You can also find more information on keeping devices secure in our helpsheet: Securing your devices  
[npfs.org.uk/downloads/securing-your-devices](https://npfs.org.uk/downloads/securing-your-devices)

### Thinkuknow

section on helping your children get the most out of the internet  
[thinkuknow.co.uk](https://thinkuknow.co.uk)

### Parent Info

help and advice for families in a digital world  
[parentinfo.org](https://parentinfo.org)

### Parent Zone

digital family life  
[parentzone.org.uk](https://parentzone.org.uk)

### National Cyber Security Centre (NCSC)

advice for avoiding phishing scams  
[ncsc.gov.uk/guidance/phishing](https://ncsc.gov.uk/guidance/phishing)

### Child exploitation and online protection command (CEOP)

[ceop.police.uk/safety-centre](https://ceop.police.uk/safety-centre)

### Mind Yer Time

advice on safe use of social media and healthy screen time  
[mindyertime.scot](https://mindyertime.scot)

### Childline

[childline.org.uk](https://childline.org.uk)

### Get safe online

[getsafeonline.org](https://getsafeonline.org)

### Internet Matters

step-by-step technical guides and resources by age of child  
[internetmatters.org](https://internetmatters.org)

### Young Scot

general info for young people, including its Digiknow project and podcast  
[young.scot/get-informed](https://young.scot/get-informed)

For help in talking with your children about internet behaviour and safety:

### BBC

[bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online](https://bbc.co.uk/cbbc/findoutmore/help-me-out-staying-safe-online)

### RespectMe

[respectme.org.uk/adults/online-bullying](https://respectme.org.uk/adults/online-bullying)

### See our other Nutshells at

[npfs.org.uk](https://npfs.org.uk)

## If you need to speak to someone about your concerns

Depending on what these are, you could speak to:

### Your child's teacher/guidance teacher

### Parentline Scotland

[children1st.org.uk/help-for-families/parentline-scotland](https://children1st.org.uk/help-for-families/parentline-scotland)

### The police: 101





**npfs.org.uk**

enquiries@npfs.org.uk

 parentforumscotland

 parentforumscot

Created in collaboration  
with Education Scotland

