

What is online safety?

Online safety - sometimes called cyber safety - is the safe and responsible use of information and communication technologies. This includes mobile phones, computers, tablets, games consoles and any other electronic device that connects to the Internet. It's important that individuals (such as you as a parent and your child) take the necessary precautions to protect themselves online.

It can be mind-boggling to try to understand every new technology that comes your way, especially if your child seems like an expert!

Technology is incredible. It can open up new worlds and support your child's learning and development, as well as being a fun way to relax and keep in touch with friends and family. However, technology can come with some risks too. It's important to learn as much as you can about how to keep yourself and your child

This parent guide presents some ideas which can support your child's safety and wellbeing online as they move through those first couple of years at primary school (key stage one or years 1 and 2, when they're aged five to seven).

safe online.





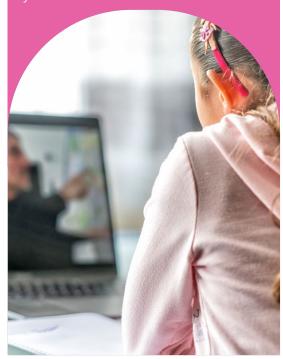




Online Safety for Ages Five to Seven

Online safety - sometimes called cyber safety - is the safe and responsible use of information and communication technologies. This includes mobile phones, computers, tablets, games consoles and any other electronic device that connects to the Internet. It's important that individuals (such as you as a parent and your child) take the necessary precautions to protect themselves online.

Other children their age might be exploring too. Research shows that the age at which children are accessing smart devices and the Internet is getting younger and younger. Did you know that it's estimated that over half of all five-year-olds have their own device? It's never too soon to start good online safety habits with your child.





Why is online safety important?

There are many issues that you or your child could encounter online. For example:

Requests for personal information: These could come from real people in the form of emails or messages. It might also be phishing: this is where an 'attacker' tries to steal information by getting the 'victim' to open an email, a suspicious link or a message.

Computer viruses: These are pieces of code that can copy themselves. This can result in your computer or other system becoming unusable. Viruses can destroy data too.

Requests for money: Sometimes, applications or games require payment information before you can play. If this is stored in the game, it can be all too easy to accidentally authorise a payment in the middle of a game. Requests for money can appear on websites or in messages and emails too.

Dangerous individuals: Unfortunately, there are people who use the Internet to prey upon vulnerable people, including children.

There are many other threats online, which is why it's so important for you and your child to have a good understanding of how to navigate the online world. Without guidance, they are likely to see inappropriate content or come across something unsuitable for their age.





Online Safety Top Tips

What can you, as a parent, do to help your five to sevenyear-old enjoy what the online world has to offer, whilst also protecting them from the dangers? Here are some top tips to help you and your child when using technology.

Explore Together and Talk to Each Other

This is a really simple tip, but it's so important that you make sure you know what your child is doing online and that your child knows they can talk to you. If you keep this dialogue open and non-judgmental, they're more likely to tell you if they encounter anything suspicious or strange. Explore appropriate sites, apps and games together.

Also, talk regularly about the importance of online safety. A good starting point for discussion is this website www.thinkuknow. co.uk which is part of the government Child Exploitation and Online Protection Centre (CEOP). This site also offers support and advice should problems arise.

If your child has an older sibling, talk to them as well. Chat about what they're doing online and what they show to their younger sibling. Encourage them to be responsible and help keep their younger sibling safe.



Use Parental Controls to Tailor Your Child's Online Experience

Set up appropriate parental controls on your home broadband and all Internetenabled devices your child has access to, including mobile phones, tablets and games consoles.

Choose safe, fun and educational sites and apps for your child to have access to. On many websites, applications or programmes, you can choose what content your child will see, which should help protect them from seeing and interacting with inappropriate content. For example, you can set restrictions for some streaming services, so your child can only watch videos that are meant for their age range.

Make sure your child is using child-safe search engines, such as Swiggle or KidzSearch. Activate safe search settings on search engines (like Google) and entertainment sites or applications (like YouTube and iPlayer).



Talk to your child about what they should do if they access something online that is not appropriate. The best guideline is for them to close the screen down immediately and tell you or another responsible adult. Can they identify trusted adults who they can go to?

Manage the Devices

Set up a user account for your child on your devices and set your homepage to a child-friendly one. Keep all devices your child will use in a high-traffic communal area in your home, such as the kitchen or living room. Be with your child when they are online and talk about what they are doing.

If you think your child isn't old enough to have or use a mobile phone or tablet, that's perfectly okay - it's your decision. Stay firm and explain your reasons. Keep the conversation about technology open and honest with your child.







Use Strong and Separate Passwords

Password-protect all accounts and chat to your child about the importance of security. Having secure passwords can help protect your personal information online. Pick something that is memorable and that contains a mixture of capital letters, numbers and special characters too. Some services recommend choosing three random words to create a password that is tricky for someone else to crack.

Warn against Sharing Personal Information

Advise your child not to share personal information online, as this can easily get into the wrong hands. It's worth discussing with your child that, although it is safe to talk about general things with others online, they should still be careful not to give too much information away. Be a digital role model for them by never sharing your own personal information online. Personal information includes:

- your name
- your address
- your phone number
- your password
- the name of your school
- a photo of you or your family

Try this: Have your child draw or make a treasure chest as a fun craft activity. Then, ask them what they would keep safe inside the treasure chest. What would need to be protected from everyone else? You can then ask them the same thing, but change this to an online situation. What needs to be kept private and protected online? Use the list of information above to guide this discussion.







Chat about Strangers

Sometimes, we interact with people we don't know online: this is similar to writing a letter to a penpal across the world. Not all strangers are dangerous, but it's important that your child knows what to do and what not to do. Rather than saying, 'Don't talk to strangers!', it's more valuable to create a climate where they can talk to a trusted person (such as you or their teacher) if they feel scared or at risk. In addition, we don't want children to feel like they can't seek help from a police officer or a shop assistant, simply because they don't know that person.

As discussed, there are risks of sharing information online. This is a place where your child is very likely to encounter people that they do not know. Children can be vulnerable to online grooming by adults pretending to be someone they are not. Remind your child that, if they have not met a person, they have no idea if they are who they say they are. Your child can choose to block or ignore people they don't know or don't want to interact with. It's also possible to set strict privacy settings on many platforms.





Try this: Read a story with your child such as Little Red Riding Hood or Snow White. Use this as a way of exploring people who can pretend to be someone else. Explain that this is much easier for someone to do online. You could then write a list or draw pictures of some trusted adults that your child can go to if they are worried, confused or upset.

Avoid Unknown or Suspicious Links

As some general advice, avoid opening up links or messages from unknown contacts. These could be trying to steal personal data. Show your child if you receive an unknown message and model to them what they should do.

Be Wary on the Move

If you're travelling or out in public, you might find you can access public WiFi. Some safety features might not be active, which can mean your child might be able to access things online that you would usually restrict at home.

Some providers are part of family-friendly WiFi schemes: look out for the symbol for Friendly WiFi, which is a government-initiated safe certification standard for public WiFi. They have filters that block inappropriate content. You can find out more about Friendly WiFi by clicking here.



Be Aware of Age Ratings

Games, apps, films and social networks all have age ratings; these can be a good guide to follow. For example, many social networking platforms have an age limit of 13, including TikTok, Facebook and Instagram. Instead, make use of services and platforms that are designed with children in mind, like YouTube Kids and BBC iPlayerKids.



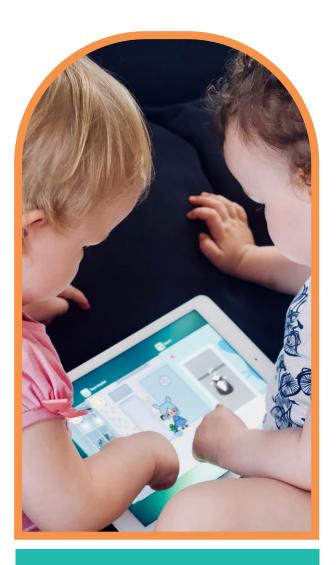


Talk about Social Networking



Social networking is the use of social media websites and applications, like Facebook, Instagram and Twitter, to connect with family, friends and other people who share your interests. Many people use social media daily.

Your child might be aware of social media, either through older children's use of it or perhaps through their peers. Talk to your child about the benefits and risks of social networking. Chat about the age restrictions in place for some social networking platforms and discuss why these restrictions are in place. Do you, as a parent, use social media? What pros and cons do you experience? Be open in these conversations.



It's also important to remind your child that anything they upload, email or message can stay online forever.
For instance, a post on Facebook or Instagram is 'published'. Think about the meaning of that word and the weight it has.

As your child gets a bit older, investigate safe social media sites for children. Internet Matters has some great information about some of the top social networks made for children; find out more by clicking here.





Talk about online Gamina



Online gaming can take place using a range of devices, including mobile phones, tablets, games consoles and computers. Players can play live with people across the world, which can be a fun, exciting experience. However, there are some risks associated with online gaming. Take a look at these top tips:

- Explore games together with your child. Check if you're happy with the content and the ideas in the game.
- As with all online safety advice, talk to your child.
 Chat about what information they should and shouldn't share. Let them feel that they can come to you if they come across anything that confuses them, upsets them or scares them.



- Be guided by the age rating of the game. Sometimes, games can appear suitable at first glance, but there might be language, themes or images that are inappropriate.
- If your child is keen to try online gaming, make it the norm that they play in a communal area, like the lounge or kitchen where you all spend time together.

 Supervise them.





What is cyberbullying?



Cyberbullying is when someone uses the Internet or a digital device to target, harass or threaten another person or group. It can occur on many platforms, including over text and direct messaging apps, on social media platforms, via email and within the online gaming community.



- sending abusive or threatening messages, both privately and on public forums, such as chat rooms or social media
- sharing embarrassing or upsetting images or videos
- · disclosing someone's personal information online
- posting rumours about someone
- creating fake accounts to impersonate someone online

In very serious cases, cyberbullying can be considered a crime and the police could become involved. Examples of this include making threats of violence or threatening someone's life and harassing someone based on their sexual orientation, gender identity, race, ethnicity or religion.

How can this impact my child?

Sometimes, children find themselves bullying or being bullied online. Issues can also arise between friendship groups at



school or elsewhere when hurtful comments are carelessly posted on social media. Talk to your child about being a good friend online. It's important to remember that our words can still hurt, even if we are not there to see a person's reaction to them.

Experiencing cyberbullying can make children feel very worried, upset and overwhelmed. They may become very uneasy about going to school, have trouble sleeping at night and have unexplained headaches or stomach aches.





Here are some potential signs that a child may be experiencing cyberbullying:

- They appear nervous or upset after receiving a message, text or email.
- They are unwilling to share information about their online activity.
- They suddenly shut off their device or walk away from their computer without warning.
- They experience episodes of unexplained depression or anxiety after using a digital device.

What should I do if I think my child is being cyberbullied?

The most important online safety tip is to create an open and ongoing dialogue with your child about their online activity. Let them know they can trust you and can talk to you about anything they experience online. Here are some steps to take if they are struggling:





- Approach your child calmly, at a time when they will not feel rushed or stressed.
- Listen to your child without judgement and reassure them that you are here to help.
- Ask your child how long the bullying has been happening and if they know who the bully or bullies are. This could be tricky if the perpetrator has used a fake account or is anonymous.
- Take screenshots of any abusive messages or comments as evidence.
- Once you have taken screenshots, encourage your child to delete messages from their cyberbully.
- Show your child how to block people.

- If your child knows their bullies in real life, arrange a meeting with your child's teacher or club leader. Schools are required to have an anti-bullying policy and they will be able to help resolve issues with bullying, even if it is taking place outside of school hours.
- If bullying is particularly serious (e.g. threats of violence or abuse based on race, religion, sexual orientation or gender identity), the bully may be committing a crime.

 Contact the police for more advice.







*Disclaimers: We hope you find the information on our website and resources useful. As far as possible, the contents of this resource are reflective of current professional research. However, please be aware that every child is different and information can quickly become out of date. The information given here is intended for general guidance purposes only and may not apply to your specific situation.

We hope you find the information on our website and resources useful. This resource contains links to external websites. Please be aware that the inclusion of any link in this resource should not be taken as an endorsement of any kind by Twinkl of the linked website or any association with its operators. You should also be aware that we have no control over the availability of the linked pages. If the link is not working, please let us know by contacting TwinklCares and we will try to fix it although we can assume no responsibility if this is the case. We are not responsible for the content of external sites.

We hope you find the information on our website and resources useful. This resource contains potentially sensitive and/or upsetting topics that may emotionally impact on children due to their experiences in their past. It is your responsibility to consider whether it is appropriate to use this resource with your children. If you do use this resource, it is your responsibility to ensure that appropriate support is available for anyone affected.

We hope you find the information on our website and resources useful. This resource is provided for informational and educational purposes only. It is intended to offer general information and should never be taken as professional advice on mental health. As information on mental health is complex and is a developing area, we do not warrant that the information provided is correct. You should not rely on the material included within this resource and we do not accept any responsibility if you or your children do. It is up to you to contact a suitably qualified health professional if you are concerned about your mental health or the mental health of your children.

This resource/information is not intended to encourage social media use and we cannot accept any responsibility for children that sign up to social media sites after using this resource/information.



