Cyber Safety

The online world is part of everyday life for many children and young people. It is packed with great information and resources for playing, learning and socialising, but there are real risks too. The best way to keep children and young people safe is by staying actively involved in their digital world. You don't have to be an expert. Knowing where to find things out is what's important.

Keeping children safe

Children and young people are accessing the internet through more devices than ever – phones, tablets, smart TVs, games, computers, laptops or wearable devices. It is accessible 24 hours, often from devices they carry with them. It is important they learn safe use as you won't always be there to guide them.

The best way to keep children safe is to talk with them about what they are doing and show your genuine interest. Discuss how things work and solve problems together. This builds trust and they will be more likely to come to you if something worries them.

Don't let the online world shape children and young people's values. They need balanced information and guidance from you.

Family technology use

As with other areas of life, children need boundaries and limits that help keep them safe as they learn. You could discuss as a family how you will use technology and agree on things like:

- using devices only in open areas of your home – children are safer when you know what they are doing
- keeping devices out of bedrooms after 'lights out' – they can interfere with sleep and increase online risks
- no phones at mealtimes or other social occasions
- having regular technology-free time
- balancing screen use with plenty of physical activity, socialising and other interests.

Remember to model safe and healthy use of technology yourself. Children are quick to see a double standard.

Setting up safe use

One way to have safer and healthier use is through software and settings for devices that filter unsuitable content and let you choose when and for how long the device can be used.

For example, you can enable Google SafeSearch on all devices (including smart TVs) and parental controls on gaming consoles and streaming services such as YouTube, Netflix or AppleTV. If you decide to enable these controls, be up front and explain your reasons. Not telling children may encourage them to hide things from you.

> Remember, no software can completely guarantee children's safety. Your involvement and a trusting relationship is still the best option.

Learning safe skills

Children and young people need to learn and practise safe online skills. Make sure they:

- learn to question what they see online and realise not everything is real. Critical thinking is an essential life skill. You might ask 'Why are they doing that?', 'What would happen if they did that in real life?
- understand that people online may not be who they say they are
- never share private information such as full name, address, phone number or date of birth without your knowledge
- realise that what they put online is not private and may be seen by people they do not intend – family, friends, current and future employers
- are kind and respectful in every communication
- pause before they post anything to ensure it is respectful – they are still learning self-regulation
- know it is better to have difficult conversations in person
- know that sharing sensitive personal information, even with a friend, could make them more vulnerable to bullying. They lose control over who sees it, even if it is deleted
- know how to screen or block unwanted contacts
- use a PIN or access code on their devices so if these are lost or stolen others can't send texts or images to contact lists
- use complex passwords, change them often and never share them with friends
- know the risks of 'geolocation' or 'checking-in' functions that identify their location. These can be limited or disabled
- do not expose younger children to inappropriate content. Make sure children know to tell you or another trusted adult if they've seen inappropriate content
- know as they get older they can develop a positive online 'digital identity'. When well-managed this can showcase skills and creativity.

Children with special needs

Parents might think that not being online is the safest option for some children and young people with special needs. However, it is important to consider the benefits that online resources and connection with others could bring, and what would be involved in keeping children safe. Installing parental controls can reduce risk. See the Australian Council on Children and the Media and Common Sense Media websites for reviews of games and apps, including those for children with special needs.

Cyberbullying

Cyber bullying can involve abusive or threatening messages, making fun of someone, or posting embarrassing or damaging information, images or videos. It is a big concern because it causes harm, can escalate quickly and involve a lot of people. It can happen anytime day or night. Research shows that 55% of children and young people do not tell their parents because they are afraid they will overreact and make things worse.

If there is cyber bullying:

- show you understand what this means for your child or young person. It can have a big impact emotionally, socially, and sometimes physically. Reassure them it can be dealt with and you will support them
- do not say you will take their phone or device away. They may hide the bullying from you and removing devices can cut them off from supportive friends.
- collect evidence of the bullying before deleting or blocking – take screen shots, print pages, save videos, note web addresses
- report it to the site or service. If they do not remove it within 48 hours, the eSafety Commissioner can help you have it removed – UK Council for Child Internet Safety (UKCCIS) – GOV.UK
- report it to the school if it is by another student. Keep a written record of contact with the school
- if you know who is doing it, do not confront them or their family members. This can make things worse
- report serious threats to your local police. An online threat could be against the law.
- Make sure children and young people:
- have other responsible adults to talk to if they don't want to tell you
- seek support if they are very upset.
- know how to support a friend who is bullied. If this happens, encourage them to seek help from a trusted adult. It can be a big emotional load to carry alone.

Social media

Connecting with friends and others is very important to children and young people. They can spend a lot of time on social networking sites and apps such as Instagram, WhatsApp, Snapchat or TikTok. Most require users to be over 13 years of age. This is for legal reasons, and does not mean children this age have the maturity to cope with social media. They do not require proof of age. If you provide access for a child under 13 years it is important to supervise their use as there can be many risks.

Make sure children and young people:

- set privacy settings so their profile is only seen by people they intend, and check settings often
- know they can use a nickname and an image of something they like instead of a photo of themselves
- let you view their profile and 'friend' you or accept you as a 'follower'. Explain your reasons
- know that most messages and images they share can be accessed, saved, manipulated and distributed by others, and their personal information misused or identity stolen
- get permission from friends and others before putting photos of them online and 'tagging' them. 'Tagging' provides information about the person's activities and creates a link to their profile they may not want. They could ask their friends to do the same for them
- ensure geolocation data is turned off and metadata not embedded when sharing photos
- know the risks of 'friending' people, accepting 'followers' or 'chatting' with people they don't know in real life. They may not be who they say they are and intend harm
- know how to report abuse or inappropriate content
- know to tell you or another trusted adult if anything concerns them. Assure them they won't be punished or have devices taken away. Remind them to collect evidence before blocking or deleting offending material.

It can help to set up your own social networking accounts so you know how they work.

Online grooming

Online grooming is when someone attempts to make online contact with someone under 16 years for sexual purposes. This is a crime.

Make sure children and young people:

- only talk online with people they know and trust in real life

- tell you or another trusted adult straight away if someone makes them feel uncomfortable or sends them something sexual, even if it is someone they know
- do not list a webcam in their profile
- never accept gifts or agree to meet online friends without you.

If you think your child is in danger contact your local Police.

The most important thing is that children know what to do if something worries them, or they are asked to do something that makes them feel uncomfortable. If you think your child is in danger call the Police straightaway.

Sharing sexual images

Make sure children and young people understand the harm that sending sexual texts, images or videos ('nudes' or 'sexts') can cause to themselves and others.

Help them understand:

- they have no control over who sees it, even if they only send it to a friend
- it can have a big impact on relationships
- images can be online forever, even if using apps that only display images or videos for a short time.

Sending sexual images of themselves or others under 18 years could also be classed as possessing and distributing child pornography, even if participants consented. This can have serious legal consequences.

Sometimes intimate images or videos are shared without consent to shame or humiliate someone. This 'image-based abuse', or threatening to do it, is an offence. You can report it to the eSafety Commissioner or ReportCyber. They can help to have it removed and sometimes take action against the person involved. It is also an offence to film or share images of someone being humiliated or degraded, such as in a school yard fight. If any of these things happen to your child or young person, reassure them it can be dealt with. They will need extra love and support from you.

Pornography

Children and young people can come across pornography by accident or by searching for it. Parental controls on devices can minimise the risk.

If your child has come across it, stay calm, talk about what happened, and be aware of how they may feel. Answer their questions honestly but briefly and problem-solve together.

Young people need to understand that pornography is not real life. Talk about respectful relationships and discourage them from viewing it. See the eSafety Commissioner website for more on how to respond.

Games and apps

Games and apps can be lots of fun and great educational tools that build skills and a sense of achievement. Many can be downloaded free.

The best ones are those where children can try out their own ideas, like creating drawings or music. Some are labelled 'educational' but are not much more than repetitive activities.

Free games often have a lot of advertising, and it can be hard for young children to tell the difference between advertising and the game.

Many have 'in-app purchasing' which can cause bill shock for parents. Prevent this by installing parental controls and not saving credit card details on devices you share.

Games are designed with 'hooks' that challenge children and young people just enough and the positive feelings from small wins can keep them playing a long time. It can help to monitor the amount of time they play. Time spent playing games can mean less time doing slower, more demanding tasks such as reading or playing board games.

Gambling risk

Games and apps can simulate gambling or have gambling strategies embedded. There are no warnings because gambling content does not require classification in the same way as violence or sexual material. Exposure to simulated gambling at a young age can groom children for gambling and make it more likely they will gamble when older. They can think that gambling is based on skill rather than chance, and believe the more they play the better they will get, just as they do in other games. This is reinforced when games make it easier to win than in real-life gambling.

Parents can:

- help children recognise gambling and understand how it works
- avoid gambling in front of children and not engage in gambling as a family

Violence in games

Games with graphic violent or sexual content have been linked to emotional problems, particularly in younger children who are not able to fully understand what is real and what is not.

Violent games put children at risk of:

- thinking it's OK to be aggressive
- being insensitive to others and desensitised to violence
- becoming scared of their world
- increased angry feelings, thoughts and behaviour. Players can identify with a violent character and

- think their behaviour is OK. When violent behaviour is rewarded it is more likely to be repeated and to increase.

You could:

- check the game's classification and reviews
- not allow 'first person shooter' games where the player is the aggressor
- not allow games where characters are mutilated or killed or where there is sexual violence
- play games with children and note their reactions. Do they become aggressive, frightened or upset? Ask what they like about the game and their favourite character. Help them question whether the behaviour would be OK in real life
- install parental controls to restrict the duration and timing of play, and access to games with specific age ratings. Talk with children about your reasons for doing this.

Lead by example and don't play violent games in front of children. You may need to be firm when limiting violent games as some children like these the most.

Multi-player online games

Young people often enjoy multi-player online games. They can play with friends and meet new people anywhere in the world.

You could:

- remind young people not to share private information
- monitor when they play. Some happen in different time zones which can mean young people are playing when they should be sleeping. Using rapid-fire games before school can also hyper-arouse the brain and make it harder to pay attention at school.

Problematic game use

It can be hard to know whether a child or young person's gaming is becoming a problem. Some signs include:

- it is affecting their school, social life, health or wellbeing
- they are becoming isolated and preoccupied with gaming
- they are anxious when not playing and losing interest in friends and other activities.

It can help to:

- look at what else is happening in their life to see why games have become so important
- keep communication open, eg asking what they like about the games

It can be hard for children and young people to limit or stop playing games without help.

You can get further advice and information from:

- School, Mrs Lesley Bickers – Computing & Online Safety Lead

- https://parentingsmart.place2be.org.uk/article/supporting-healthy-gaming-habits

- https://parentingsmart.place2be.org.uk/article/safe-social-media-for-primary-aged-children

- https://www.justonenorfolk.nhs.uk/staying-safe/staying-safe-online

- https://www.gov.uk/government/groups/uk-council-for-childinternet-safety-ukccis

- https://www.suffolk.gov.uk/community-and-safety/staying-safe-online/e-safer-suffolk/

- National Bullying Helpline – 0845 2255 787

- NSPCC (Cyber-Bullying) – 0808 800 5000

- https://www.internetmatters.org/advice/6-10/

- Child Exploitation and Online Protection command - https://www.ceop.police.uk/Safety-Centre/