# Cyber safety

**The online world is part of everyday life for many children and young people. It is a huge virtual playground where they can play, learn and socialise. It can be accessed by computers, mobile phones and other electronic devices.**

**Parents can help children get the most from the online world by being involved from the start and helping them learn how to stay safe. You don't have to be an expert. Knowing where to fi nd things out and get help is what's important.**

## Children and the online world

Parents today have seen technology grow at a rapid pace. New words such as Facebook, social media, apps and smartphones have become part of everyday language. Some parents are very familiar with new technologies and use them a lot. Some may use them a little, while other parents can think this 'new world' is not for them.

Whatever your views about online technology, it is important to realise it is very much part of children's 'real world'. It's where they can spend a lot of time and gain many educational and social benefi ts. As they get older, their online communication becomes a key part of their 'social identity'.

## What parents can do

Parents often worry they don't know enough about online technology. That's OK – you don't have to be an expert. The most important thing is to be involved and not leave children to work it out on their own – just know how to find things out and where to get help. It might be easier than you think to become a 'digital parent'.

It is important to:

> start early and talk with children about what they are doing. This builds trust. Children will accept your involvement in their online activities and be more likely to come to you later if something worries them

> help them learn about risks and practice safe technology skills

> teach them to question what they see online and to realise not everything they see is real. You might ask 'Why do you think they are doing that?or 'What would happen if they did that in real life?' This helps children learn your family values and to be critical consumers

**Don't let the online world shape children's values – they need balanced information and guidance from you.**

> have rules and limits that suit each child's age and maturity – these will change as children grow up and gain skills

> agree how you will filter and monitor internet use to make sure children are safe. Be upfront

– if you go behind their back it may encourage them to hide things from you

> make sure children have plenty of 'technology-free' time. Learning to entertain themselves without technology is a skill that needs practice. Active and creative play are important for children's healthy development. A balance of online and offline activities helps them develop a range of skills and interests.

**It is important to stay involved in your child's online life. How you do this will change as children gain skills and become more independent.**

**Ensure the time children spend online fits within the recommended time for all screen use:**

**> no screen time for children under 2 years**

**> no more than one hour per day for children under 5 years**

**> no more than two hours per day of recreational use for children 5 to 18 years.**

### Cyber smart tips

> Keep computers and devices which link to the internet in a room that is open. It will be easier to know what children are doing.

> Keep electronic devices out of bedrooms after 'lights out' as they can interfere with sleep.

> Make agreements with your children about safe internet use at home and away from home. You might include:
  - respectful online behaviour – 'netiquette' means not doing or saying anything online they wouldn't in person
  - not sharing personal and family information
  - rules about safety, e.g.
    - not making new friends online without talking to you first
    - what to do if they are bullied
    - what to do if they see something that worries them or they are asked to do something that makes them feel uncomfortable
    - not exposing younger children to inappropriate content, including games.

> Select a reliable Internet Service Provider (ISP) that can assist with cyber safety for children.

> Install and maintain reputable anti-virus, blocking, filtering or monitoring software to protect your computer and restrict access to unsuitable material. Use parental control software and set updates to happen automatically.

**The best way to keep children safe online is to supervise them and know what they are doing. No software can completely guarantee their safety.**

> Be aware of websites that can help with cyber safety, e.g.
  - ThinkUKnow, the Australian Federal Police online safety website, has lots of great safety information about the internet, social networking, mobile phones and games
  - the Australian Communications and Media Authority website has a cyber smart guide for parents, cyber smart programs for children and young people of all ages, and many other resources to help families stay safe online
  - The Australian Council on Children and the Media website has a list of good children's sites as well as guides for deciding what games and apps are suitable for children.

> Learn how to check what children are viewing:
  - know their 'on-line' names, email addresses, passwords and what sites they use
  - keep track of what's being looked at by checking 'Bookmarks', 'Favourites' or 'Internet History' on their browser
  - learn how to block unwanted contact on sites they use. The ThinkUKnow website tells you how to do this on popular sites.

> Ask your local library about what services they provide, e.g. free internet training, guides for safe internet use or good websites for children.

> Check your school's Information Technology and Anti-Bullying policies, and make sure what you do at home is in line with these. Encourage the school to provide online safety training for students and parents.

> Report bullying or inappropriate behaviour to the Cybersafety Contact Centre at the Australian Communications and Media Authority website. Report child exploitation or other crime to the ThinkUKnow website or Crime Stoppers.

> If you think your child is in danger contact your local police, or if there is an emergency call 000.

## Mobile phones and digital devices

Smartphones are popular as mobile phones and a way to link to the internet. They provide access to emails, online games, music, apps and social networking sites. They can be used to take and send photos. Other devices such as tablets, gaming devices and media players can also connect children to the online world.

### Cyber smart tips

Decide whether you are happy for your child to have a mobile phone or device that links to the internet. Consider your child's age and maturity and what it will mean for them to use it safely. If you go ahead:

> learn how to set parental controls. You can limit access to adult content, select times when the phone can be used, block unwanted calls and manage costs by:
  - asking staff at the phone shop to show you how
  - checking the device's website
  - visiting the ThinkUKnow or Australian Mobile Telecommunications Association websites
  - searching for videos on how to set up controls for the device on 'YouTube'

**It is important to know the functions of your child's mobile phone and digital devices so you can ensure they are using them safely.**

> make sure your child knows to:
  - only give their number or personal details to people they know and trust offline
  - keep their phone in a safe place and have a PIN or passcode to stop others from using it. Phones can be stolen and used to send negative texts or images to people on contact lists
  - screen calls or turn the phone off if they get unwanted contact
  - turn off the phone's location settings when using it to access social networking sites from home – people can find out your home address
  - not return missed calls from unknown numbers. It may be a scam where the call is directed to a premium service at a cost
  - report inappropriate behaviour through the Australian Communications and Media Authority's website, or child sex exploitation matters through the ThinkUKnow website.

## Sexting

It is important that young people do not use any electronic device to send or forward sexually explicit text or photos. This is called 'sexting'. Once an image is sent they have no control over what happens to it or who else sees it. It could be online forever.

Sending nude or sexual photos of themselves or others under 18 years of age could be classed as possessing and distributing child pornography. This can cause serious harm and have serious consequences. For more information about sexting, visit Cybersmart Parents at the Australian Communications and Media Authority's website.

**Make sure children know that what they say and post online stays there forever. It can be seen by people they may not intend. Help them think about the risks and long-term impact of their actions.**

## Social networking

Social networking sites enable you to keep in touch with friends and family, send photos and videos, download games, and even play online games with lots of other people. They make it easier to connect with more people and share more about your life than ever before.

The rules for most social networking sites state that users have to be over thirteen years of age. However, site operators don't have to ask for proof of age. If a parent provides access to a social networking site for a child under thirteen it is important they supervise the child's use as there can be many risks.

Having friends is very important to children and young people. They need to know it can be risky 'friending' people or accepting 'followers' if they don't know them – how do they know if the person is who they say they are? They might intend to cause harm. There is also a risk that personal information or photos could be misused or their identity stolen.

Keeping up with the sites young people use can be hard as new sites emerge and trends change, e.g. Facebook is less popular now that parents and even grandparents are using it.

Some young people use Facebook to keep in touch with family, and Twitter, Instagram and Snapchat to contact friends.

**Make sure young people know it is dangerous to use a mobile phone when driving a car or walking near traffic.Accidentsrelatedto mobile phones are increasing.**

### Cyber smart tips

> Set up your own social networking accounts so you know how they work.

> Know what sites your children are on and supervise them in line with their age and maturity.

> Visit the website to find out about cyber safety features on key social networking sites.

> Make sure your child or young person:
  - only accesses sites that are suitable for their age (see the Australian Communications and Media Authority's Easy Guide to Socialising Online)
  - creates an online nickname that doesn't identify them, and uses an image of something they like instead of a photo of themselves in their profile
  - lets you view their profile, and 'friends' you or accepts you as a 'follower' on sites they use
  - checks privacy settings often to ensure their profile is only seen by people they want
  - learns how to block people they don't want making contact, and how to save things in case you need to make a complaint
  - knows how to report abuse or inappropriate content to the social networking site
  - doesn't list a webcam (a camera built into the computer, or added on) in their profile if they are using one for talking with family and friends
  - gets permission from others before putting their photos online, and asks their friends to do the same for them
  - never agrees to meet a new online friend without you
  - never responds to a contact which makes them feel uneasy.

## Games and apps

Games and apps can be great educational tools that build skills and a sense of achievement, as well as being lots of fun. There has been an explosion in the use of games and apps that can be downloaded from the internet by people of any age, and many are free. Even young children can spend a lot of time playing them.

It is important for parents to know the content of games and apps that children are using. The Australian Council on Children and the Media's website has an app review service, 'Know before you load'. It can help you find the best apps and avoid some of the pitfalls. Some apps are labelled 'educational' but are not much more than repetitive activities. The best apps are those giving children a chance to experiment and try out their own ideas, e.g. creating drawings or music.

The app reviews on the Australian Council on Children and the Media's website provides a description of each app and the age recommendation, as well as whether there is:

> advertising and product information – many apps contain advertising and it can be hard for young children to tell the difference between the advertising and the game
> in-app purchasing – real purchases can be made from inside the app, causing bill-shock for parents
> content that may be inappropriate such as violence, sexualised images or coarse language
> gambling content – some apps have simulated gambling machines or elements of gambling embedded in the game.

For young people, multi-player online games are very popular. They can play their favourite game with friends as well as meet new people with similar interests anywhere in the world. It is important for young people to be cautious about sharing personal information with people they meet through online games. They can't really be sure who that person is.

## Gambling risk

Australia has a big gambling culture but most parents would never encourage their children to gamble. However, simulated gambling can be embedded in children's games without parents realising. There are no warnings on games because gambling content does not require age restriction classification in the same way as violence or sexual material.

Simulated gambling is particularly risky for children as exposure at a young age can make it more likely they will gamble when older. Children can think that gambling is based on skill rather than chance. They can 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:

> check the Australian Council on Children and the Media site for the gambling content of games
> help children to recognise gambling and understand how it works
> avoid gambling in front of children, and don't engage in gambling activities as a family.

## Violence

Games with graphic violent or sexual content have been linked to emotional problems, particularly in younger children. Children exposed to violent media are at risk of:

> thinking it's OK to be aggressive
> being insensitive to others being hurt
> becoming scared of their world.

Many studies show that violent games increase angry feelings and aggressive 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. Parents can:

> have agreements with children about appropriate games, for example:
  – only playing games suitable for their age. Check the Australian Classification website for more information
  – no 'first person shooter' games where the player is in the role of the aggressor
  – no games where characters are mutilated or killed
  – no games with sexual violence.

You could hire the game first to make sure you are happy with the content – movies and games classified for children can still contain a lot of violence.

> play games with your children and note their reactions. Do they become aggressive, frightened or upset? Ask them what they like about the game and their favourite character. Help them question whether the behaviour would be OK in real life
> limit the amount of time children spend playing games. Limits need to fit within the recommendations for all screen use for their age (see page 2). It is also important to monitor when they play. Some multiplayer online games happen in different time zones which can mean young people are playing when they should be sleeping
> install the gaming device's parent control software if the device links to the internet. These controls will also restrict access to in-game purchases. Visit ThinkUKnow for a guide to gaming consoles.

**Lead by example and don't play violent games in front of children. Children are quick to spot double standards. You may need to be firmwhenlimiting violent games as some children like these the most.**

## Problem game use

When children and young people spend a lot of time playing games they spend less time doing slower, more demanding tasks like reading or playing board games. They also spend less time being active.

Frequent gaming can affect school and social life. A young person can become isolated and preoccupied with gaming. They may become anxious when not playing, or lose interest in friends and other activities. It is important to look at what else is happening in your young person's life to see why gaming has become so important.

**It can be hard for young people to limit or stop gaming without help. They may want to talk with a counsellor face-to-face, or contact Kids Helpline.**

## Cyber bullying

Cyber bullying is when technology is used to harm others. It usually happens more than once and can be in the form of abusive emails or texts, making fun of someone online, or posting embarrassing or damaging information or photos. Cyber bullying is a big concern because it can escalate quickly and involve a lot more people than face-to-face bullying.

### Cyber smart tips

> Contact the site administrator to have bullying content removed.

> Report bullying to the school if it's coming from another student. Schools have policies to protect students and can help stop it.

> Talk to your young person about getting support if they are very upset. The Cybersmart Online Helpline is a good place to start.

> Report serious threats to your local police. A threat made online could be against the law.

Make sure children and young people know:

> to ignore bullying messages and how to block unwanted contact on email, social networking sites, chat rooms, games and other programs

> to keep a record of bullying messages so you can report it

> how to support a friend if they are being bullied, and to tell a responsible adult

> not to bully others.

**Don't threaten to take a child's phone away or stop them going online if they are bullied. This can cut them off from their supportive friends. They could hide the bullying from you, or feel like they are the one being punished.**

## Children with special needs

Children and young people with special needs and disabilities can be held back from using online technology due to fears of cyber bullying or internet safety.

Parents may feel they don't know enough to guide their children and keep them safe. They might think not being online is the safest option. However, it is important to consider the benefits children with special needs can gain from being connected. It can help to find out what would be involved in keeping them safe.

**If children and young people with a disability are online, make sure they are taught safe and responsible use. They may need some extra support.**

[1] *Australia's Physical Activity and Sedentary Behaviour Guidelines, Australian Government*

### Want more information?

**Cybersafety Contact Centre**
Australian Communications and Media Authority Phone 1800 880 176.
Go to www.acma.gov.au hotline to make a complaint, and to www.cybersmart.gov.au for safety information and Cyber Smart Kids.

**Australian Council on Children and the Media** Phone 1800 700 357, 24/7 Helpline
Information about children and media, and app review service 'Know before you load'.
www.youngmedia.org.au

**Australian Federal Police**
To report concerns, and internet safety programs for parents, teachers and children. Entering a key word in the search bar will link you to a wealth of information.
www.thinkuknow.org.au

**Australian Classification**
Classification ratings for movies and games.
www.classifcation.gov.au

**Australian Mobile Phone Telecommunications Association**
Practical tips for mobile use
www.mobiletips.org.au

**The Alannah and Madeline Foundation**
Cyber safety programs
www.amf.org.au/cybersafety

YWCA NSW
Find your possible