

PARENTS AND CARERS GUIDE TO ONLINE SAFETY



THINKUKNOW AUSTRALIA

ThinkUKnow is a partnership between the Australian Federal Police (AFP), the Commonwealth Bank of Australia, Datacom and Microsoft Australia, and is delivered in collaboration with state and territory police and Neighbourhood Watch Australasia.

ThinkUKnow is Australia's first and only nationally delivered, law enforcement led, online safety program.

Self-protection through education and empowerment is the key for children to protect themselves against threatening or harmful situations online.

The program focuses on what young people do online, the challenges they may face, and how to get help if something goes wrong.

MISSION

ThinkUKnow aims to empower every Australian to be safe, respectful and resilient online.

CONTACT US

You can find more information at thinkuknow.org.au

To book a ThinkUKnow presentation, contact the booking centre on 1300 362 936 during business hours or visit the ThinkUKnow website.

facebook.com/ThinkUKnowAustralia

twitter.com/ThinkUKnow_Aus

ThinkUKnow is a free program, delivered by volunteers from:













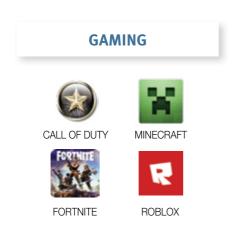
CONTENTS

See, Say, Do – Gaming	2
See, Say, Do — Social Networking and Dating	4
See, Say, Do — Instant Messaging	6
See, Say, Do — Video and Image Sharing	8
Know the Challenges	10
	10
	11
	12
	13
> Dating and Sexting	14
··· → Cyberbullying	16
	18
ThinkUKnow Presentation Evaluation	19
Family Online Safety Contract	21
Taking Action	23
Support Services	24



Children and young people play games to pass time, to be creative, problem solve, socialise and for escapism. Games can be played on numerous devices, including hand held devices, which can all have some level of online access. Many games offer 'in game' chat functions and ways to connect with other users. Think Minecraft, Call of Duty, and Candy Crush.

Many parents and carers may not be aware that some games have an 'in game' chat function.



It is important young people learn to play online games safely and respectfully.

There may be some challenges young people come across when playing online games.

Most games will have a rating much like movies and TV shows. Ask yourself if the game is age appropriate for the young person playing it. These ratings are used to protect young people from accessing inappropriate material. This material may be psychologically harmful to children and exposure may desensitise children to extreme material, such as pornography, child exploitation material, radicalised ideologies, and criminal activity. Young people may also be subject to bullying, swearing and rudeness when gaming on a platform that is not age appropriate. Anonymous 'in game' chat can provide a possible platform for online child sex offenders to target young people. Case studies have shown predators using 'in game' chat as a gateway, and subsequently directing their targets to other platforms to elicit photos and facilitate meetings.

It is important young people learn to question the value and accuracy of the content they see online. Have open and honest communication with your child about what to do if they see something that upsets them.

WHAT CAN I DO?

- ••• Check the classification, as these can be a good indication as to whether the content and functionality is suitable for children. Classifications are sometimes set by game or app developers and not independently assessed.
- Many games contain in-app purchases which can lead to a hefty bill—it is a good idea to disable in-app purchases.
- ••• Only download apps from the official stores, such as Apple's App Store or the Google Play Store.
- … Encourage your child to come to you or a trusted adult if they see something online that makes them feel uncomfortable.



SOCIAL NETWORKING AND DATING



There are lots of ways to connect online by using social networking apps. We encourage everyone to use technology positively and in a balanced way. Parents and carers have an important role to play.

Young people use social networking apps to build and maintain relationships, showcase their creativity, to look for content of interest and connect with like-minded people. This can be done through social networking websites, chatrooms or apps.

Popular choices for young people include Facebook, Twitter, Instagram and Snapchat. However, what is most popular often changes on a weekly basis!

Any device or app when used incorrectly has the potential to cause harm. There may be some challenges your children come across when using social networking apps and websites.

Maintaining privacy can be difficult, with many social media apps using a device's features to pin point its location. It is also important young people set their privacy settings to 'private' or 'friends only' to mitigate unwanted contact. Settings are frequently changing so it is worth researching if you are unsure about the settings of an app or website your child is using.

WHAT CAN I DO?

- Hensure secure privacy settings are enabled on your child's social networking accounts and devices.
- When the point of the point
- ••• Be aware of how to block and report users, pages and groups.

SOCIAL NETWORKING





SNAPCHAT



BE AWARE!

Not everyone online is who they say they are. People can be anonymous online or will have usernames which may or may not identify them. Some apps don't require registration or verification so you never know who your child is chatting to online.

Our Online Safety Family Contract on page 20 is a good way to start discussions with your children about online safety.



INSTANT MESSAGING



Instant messaging apps are characterised by the ability to send and receive messages in real-time. Many social networking apps often have a complementary messaging service, like Facebook Messenger. Messaging apps allow people to communicate in 'private' rather than on a public wall or forum. These are also popular for young people as they don't cost anything– except data—unlike phone calls and texts.

It may be difficult for young people to know who they're talking to, as some apps allow anonymous signup. This could make it hard for parents and carers to monitor who their children are talking to, and what content is being shared.

Some messaging apps allow users to have 'secret' conversations. This feature allows the message to be locked down to one device, and sometimes requires a password to retrieve the messages.

WHAT CAN I DO?

- ••• Make sure your child only has people they know and trust as online friends and contacts.
- ••• Teach your child that it is never ok to meet with someone they have only ever spoken to online. If they do, take along a trusted adult.
- Young people should let their friends know if their account has been hacked. The hacker might try and access the profiles of friends too, or send them nasty messages under your child's name.

INSTANT MESSAGING







MESSENGER

KIK

WHATSAPP



SEE SAY DO

VIDEO AND IMAGE SHARING

Video and image sharing apps allow users to create, send and receive photos, videos and even real-time live video streams. Examples of this type of app are Facebook Live, Periscope, Instagram, YouTube and Snapchat.

Live streaming apps may not have moderation of filtering on the live stream, meaning that young people may see things that are inappropriate.

It is important young people are aware of their surroundings when they are using these apps. They need to be aware that background imagery, noises and other factors may give away a lot of personal or private information.

The images and videos users share can be a representation of who they are, whether accurate or not. It is important to remind children to think before they post, as the content they share can have consequences later on.

IMAGE/VIDEO SHARING



WHAT CAN I DO?

- Before you download and install an app, check which features of your device (such as the Global Positioning System (GPS) function) the app wants permission to access. Disable any features which are unnecessary for the app to access.
- ••• Make sure location and GPS settings are turned off and broadcasts are set to 'private'.
- ••• Make sure your child is familiar with what information is acceptable to share online.
- ---- Always check what information could be given away in the background of a photo or video.
- Remind your child to think before they post.

KNOW THE CHALLENGES

There are some challenges we may face online.

Most of these will relate to privacy, personal safety, relationships or reputation.

It is your child's right to feel safe.

Young people will make mistakes in relation to technology.

Your child needs to know what action to take if something happens online. They should be aware of how to block and report on every game, site and app they use.



PRIVACY

Policies, Terms and Conditions

Whenever you sign up to a social media account or download an app, you are asked to agree to its Terms and Conditions. Unfortunately, many people don't read the fine print and may not apply the most appropriate privacy settings (which are rarely the default setting).

Most social media services have four parts to their **Terms and Conditions:**

- A licence agreement—This allows the service to change, add, delete, publicly display, reproduce, copy, distribute, sell and use your personal information including your photos, posts, private messages, comments and videos without your permission.
- Law enforcement disclaimer

 This means they can provide information to police for investigative purposes.
- Community guidelines These are the rules around how to use the service and consequences for breaking the rules, such as shutting an account down. These guidelines also usually indicate the minimum age requirement for using that service.
- Privacy policy—This explains what private information the company collects, how it is used, and what privacy settings you can use.

YOUR DATA

Teaching children basic online security skills is important, particularly as they get older and begin creating their own accounts, making purchases or doing online banking. Here are some challenges to look out for:

SPAM

Spam involves unsolicited, commercial, electronic messages being sent to an email account, mobile phone or via social media.

These messages may contain advertisements for goods or services, attempts to capture banking or credit card details, or may even contain malware.

SCAMS

Scams are most commonly received through email. Some examples of online scams include unexpected money or winnings, fake charities, dating and romance scams, or the buying and selling of illegitimate products.

The most common type of scam through email is known as 'phishing'. Phishing scams attempt to trick people into providing personal information, particularly financial details, to enable them to commit fraud.

MALWARE

Malware is software which you are tricked into installing that will track what you are doing. Ransomware is a type of malware which freezes your device and forces you to pay a 'ransom' to have it unlocked.

These programs may be sent to you through websites or pop-ups which you can click on, or through email or social media messages. Having strong security for your accounts can help protect you from unauthorised access, extortion, identity theft or fraud.

WHAT CAN I DO?

- ••• Use a passphrase that has more than 12 letters and includes at least four words. Swap some of the letters for numbers or characters.
- Passphrases should be changed regularly, and not used for multiple accounts.
- Use spam filtering software available from your email account provider.

TEACH YOUR CHILD TO:

- ----- Be careful not to click on links in suspicious emails.
- Not to open emails from unknown senders.
- Avoid giving out their email address or mobile phone number unless they know how that information will be used.

For more information, see the ThinkUKnow SOS Guide to Cyber Security

KNOW THE CHALLENGES INFORMATION SHARING

For many social media accounts, your profile picture and 'biography' are often publicly visible, despite your privacy settings.

PRIVACY SETTINGS

If your child has a social media account, make sure that their privacy settings are secure. This means 'Friends only' on Facebook, and 'Private' for both Instagram and Twitter.

For more information on how to change settings visit thinkuknow.org.au

WHAT IS 'GEOTAGGING'?

Most people post to social media from their smartphones, which have a Global Positioning System, better known as a GPS. Our advice is to turn off the GPS on your mobile devices for the camera and other apps which do not require your current location. When a photo is taken with the GPS on, metadata is automatically embedded into it, revealing the location and time it was taken—this is known as geotagging. This can also occur in comments posted on social media, or instant messages.

WHAT CAN I DO?

- Know what your child has agreed to in the Terms and Conditions and make accounts private.
- Look at the privacy policies of the sites and applications your child uses.
- If your child does not meet the minimum age requirement and you are comfortable with them using the account or app, consider having their login details to monitor their activity.
- ••• We also discourage children and young people from 'checking in' at locations on social media.



KNOW THE CHALLENGES

RELATIONSHIPS AND PERSONAL SAFETY

ONLINE GROOMING

Online grooming is when an adult makes online contact with someone under the age of 16 with the intention of establishing a sexual relationship.

The offence occurs in the communication phase so no physical contact need ever occur for police to step in and investigate.

We encourage children to avoid talking online to people they don't know, but if they are communicating with a stranger they need to avoid sharing personal information and know how to report suspicious behaviour.

Online groomers are aware what young people 'do' and 'say' online, and they use various techniques to lure young people in order to make communicating with them easier.



WHAT CAN I DO?

- Young people should never send photos or share personal information, including their location, to unknown people.
- ••• Young people may receive unwanted sexual advances from other young people that can cause some distress. For some young people, they may be more concerned with hurting the other person's feelings than protecting themselves in these situations so it is important to remind them that they have the right to feel safe in all situations, and not to fear taking actions to preserve that safety.
- Nothing in life is free—warn your child about accepting gifts from people they don't know; they might want something in return.
- Be aware of how to block and report on the games, apps and site your child is using so that you can take quick action if someone makes them uncomfortable online.

If you suspect a child is being groomed online

- Trust your instincts. If you are concerned about the possibility your child, or know of a child, who is at risk from sexual abuse, act on it.
- It is important to collect evidence to provide to police. Take screenshots of conversations, usernames and copy URL's before blocking or deleting the other user.
- To report an emergency or concern which requires a high priority response, such as a child who is in immediate danger or risk, call Triple Zero (000) or your local police station.
- Anyone can report abuse or illegal activity online at <u>afp.gov.au</u> or by clicking on the 'Report Abuse' button at <u>thinkuknow.org.au</u>

KNOW THE CHALLENGES

DATING AND SEXTING

Sexting or 'sending nudes' is the creating, sharing, sending or posting of sexually explicit messages or images via the internet, mobile phones or other electronic devices.

Young people may engage in this activity to show intimacy with their partner, in the hope to attract a partner or to express themselves to others.

We focus our youth education on the importance of not sharing images or videos they might have received from someone in confidence. If a young person is sent a sexual image, they need to respect that it is not their image. They don't own it and have no authority to share, show or send it to someone else. It can also be an offence to store this material.

There is also a trend toward apps for sharing 'erasable' media, where young people send images believing that they 'disappear' after a short time (Snapchat is a popular example of this). However, entire deletion cannot be guaranteed.

WHAT CAN I DO?

- We strongly encourage you to talk to your child about respectful relationships and direct them to trusted sources of information about sex and relationships.
- If you are uncomfortable talking to your child about these issues, direct them to sexual health services or support groups in your community.
- ••• Talk about some tactics your child could use if they feel pressured to send an image.

If your child has been creating, sending or receiving 'sexts':

Use your judgement and discretion to manage the issue, however be aware of the following:

- …. There may be emotional and psychological consequences of sexting for your child, particularly if something goes wrong.
- ••• Consider seeking advice from a health professional or your child's school. Schools have mandatory reporting obligations to police and should have an e-smart policy.
- If you believe the incident is malicious or may be a result of grooming, contact your local police immediately.

What to expect if the police become involved...

- Each state and territory police jurisdiction may deal with sexting cases differently. Under Commonwealth law, sharing nude images of people under the age of 18 (including of themselves), may constitute a criminal offence.
- ••• Laws were designed to deal with adults who offend against children, but some instances of 'sexting' may also meet the requirements of these offences.
- Police investigations will generally focus on the incidents of sexting where the image has been spread to external parties for malicious or exploitative reasons.

Image-Based Abuse

Image-based abuse can occur when someone threatens to distribute your private or sensitive material.

Individuals may be targeted through social networking sites, dating webcam or adult sites.

Police have seen instances where perpetrators have threatened to show family or friends the information or images they have obtained unless victims comply with their demands.

If you become aware this is happening

- ••• Save the details, emails, comments or other evidence you have of that person's attempt to extort you.
- -----> Block emails and accounts and cease all contact.
- ••• Often the only leverage others have is your embarrassment – consider this when you are thinking about how you will manage the situation.
- If you find images of yourself on a site you can try to get them removed by contacting the site administrator.
- In certain circumstances search engines such as Google may also remove images from their search results.
- Paying scammers or extortionists is not encouraged—once you have paid or complied with their demands, there is nothing preventing them from targeting you again.
- …. The Office of the eSafety Commissioner has established a portal with resources to assist in reporting image-based abuse: esafety.gov.au/image-based-abuse

WHAT CAN I DO?

- Make sure your software, security and systems are up-to-date.
- Cover your webcam when not in use.
- Don't open attachments unless they're from someone you know.
- Be aware that anything you share online can be saved, recorded, copied and forwarded. This includes video and voice calls.
- Be suspicious of any new or unusual 'friend' requests.

Kids Helpline is a great service for young people to discuss matters openly with an adult.



KNOW THE CHALLENGES

CYBERBULLYING

Cyberbullying can take many forms, including; repeated menacing messages; hurtful messages, images or videos; excluding others online; nasty online gossip or chat; humiliating others online; or imitating others online.

This kind of bullying can cause great distress and impact on a child's self-esteem and confidence. Young people don't feel safe because they can be bullied in their own homes and 24-hours-a-day.

Cyberbullying activities may include:

- ••• posting defamatory messages on social networking sites
- ··· spreading rumours online
- excluding a young person from an online group
- ••• sending unwanted messages, either by text, instant messaging or email.

Dealing with Cyberbullying

IF YOUR CHILD IS BEING BULLIED...

- Keep evidence of bullying behaviour such as instant messenger conversations or online posts.
- ----- Talk with your child about conflict they may have experienced.
- Find out the policies of your school, sports organisation and any of the sites and applications your child uses in relation to cyberbullying.
- It is important to avoid removing access to technology as this may prevent your child from talking to you if future issues arise.
- ---- Report content to the site on which it occurred.
- If the content is not removed within 48 hours, report it to the Office of the eSafety Commissioner <u>esafety.gov.au/reportcyberbullying.</u>

IF YOUR CHILD IS BULLYING OTHERS...

- ... Explain to your child why bullying is unacceptable.
- Find out why the bullying is occurring often a child who is bullying others may be experiencing other behavioural issues.
- ... Encourage your child to understand the offline consequences of their actions.
- … Encourage your child to think about how they would feel if they were in the other person's position.

Tips

- Building parental connectedness can help build resilience in children and help them to overcome conflict.
- Encourage your child to support their friends who are being cyberbullied and assist them in telling a trusted adult.
- Provide opportunities for your child to develop their own strategies for combating cyberbullying.
- Talk with your child about appropriate forms of conflict resolution so that they do not resort to cyberbullying.
- Make sure your child knows who they can talk to about any issues they are facing online if they are not comfortable confiding in a parent.
- Encourage your child to reduce their exposure to people they don't know who may upset them, by changing their privacy settings.

Promoting resilience in young people is not a single event, but a continuous process that requires adults to be supportive and empathetic of children when things don't go their way. It also requires you, as a parent/carer, to understand resilience, so you have faith in yourself and your child's ability to cope.

WHAT CAN I DO?

- ----- Have a positive attitude when they navigate challenges.
- Look for teachable moments and encourage them to help find solutions.
- Highlight the importance of time away from the screen, eating properly, exercising and rest.
- Teach empathy and understanding of others.

If you feel like the situation is beyond the advice you have been given, get help. Seek professional support services or people. A list of support services is located on page 23.



KNOW THE CHALLENGES

REPUTATION

You never know where something posted online might end up. If something is posted then later deleted, it can still have been shared in several ways—it can be copied, forwarded, posted, saved or cached.

Some content shared online, including sexualised photos, breaking the law (e.g. vandalism) or behaving in an inappropriate or offensive way, could affect future opportunities.

Many employers, universities, and sporting groups will search for applicants or potential members online before giving them a job or contract.

Taking simple precautions to secure social networking profiles and controlling what is posted, through tagging permissions on Facebook, for example, can ensure any private and personal information shared is protected.

What a young person does and says online may form their 'unofficial CV' and they need to be aware what they do online today could impact their future.

WHAT CAN I DO?

- Encourage your child to think before they post.
- ••• Suggest your child regularly searches themselves online (and do the same for yourself).
- … Encourage your child to discuss with their friends what material they are sharing about them and others.
- Ask your child to enable tagging permissions on Facebook so that they have to approve any content they are 'tagged' in before it is shared.

What does your digital shadow say about you?

THINKUKNOW PRESENTATION EVALUATION

To complete this form online, go to www.aka.ms/tuk

SCHOOL/ORGANISATION NAME/ID _____

PRESENTATION DATE

I am a (please mark the appropriate box):

0	Parent (Carer			Feacher	С) Other
			VERY POOR	POOR	AVERAGE	GOOD	VERY GOOD
1.	How would you rate you awareness of online safe and security issues prior the presentation?	ty	0	0	0	0	0

		STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE
2.	The presentation helped me better understand how young people are using the internet and mobile technologies	\bigcirc	0	0	\bigcirc	0
3.	The presentation helped me better understand the safety issues around young peoples' use of the internet and mobile technologies	0	0	0	0	0
4.	The presentation has motivated me to take additional steps to improve the safety and security of children online.	0	0	0	0	0

COMMENTS (OPTIONAL):

Presenters (Were they easy to understand? Did they present clearly? Were they engaging?)

Content (Was the information relevant? Was it easy to understand? Were the videos thought provoking?)

Other comments (Suggestions, improvements etc.)

THANK YOU FOR YOUR FEEDBACK, IT WILL BE USED TO EVALUATE THE PROGRAM.



(Child)

the Ryan

Family Online Safety Contract

This contract helps us stay safe when it comes to what we SEE, SAY and DO online.

T	, will:
	(Child)
ł	Tell my parents or carer if I see something that makes me feel upset, uncomfortable or scares me.
5	Be aware that people online are not always who they say they are, and do not always tell the truth.
1	Let my parents supervise where I go online as I understand they do this to help keep me safe.
ŝ	Tell my parents or carer if someone sends me rude or naked pictures, or links that I did not ask for.
Ì	Not give out personal information about myself, my family, my friends, or others online, including full names, addresses, phone numbers or schools. Not share my passwords or usernames with anyone but a parent or carer and I
ł	understand they will only use it if they are worried about me or my safety. Treat others the way I want to be treated online and with the same respect as I would offline.
2	Never use the internet or a mobile device to cyberbully someone.
	Make sure all of my accounts are always set to private.
ł	Not talk to anyone online, or add anyone on my social networks, if I don't know them offline.
	Never agree to meet someone in person that I have only met online, and I will tell my parents if someone asks to meet me.
•	Accept my parents or carer as a 'Friend' on social media providing they ask for my permission before posting or commenting on my content, and they speak to me first if they see something they don't agree with on my profiles.
ľ,	Not respond to emails, instant messages, messages or friend requests from people I don't know.
ľ	Never send someone a photo of myself online without checking with my parents or carer first.
ľ	Learn how to block and report people online and tell my parents or carer immediately if doing this.
	Ask for permission before downloading any apps, games or software, so my parents or carer can check these are appropriate for my age and won't harm the device.
ł	Teach my parents or carer about the internet, apps, games and websites I enjoy. Agree to the online time limits set by my parents or carer and put my devices to bed at night to help me get a restful sleep.
s	igned: Signed:

(Parent/carer)

21



foundation

Family Online Safety Contract

(Parent, carer)

am providing and paying for your internet service and device. Along with this privilege comes the responsibility to protect our family and our private information.

This contract is a requirement of having this service provided to you.

If you see or hear anything online that makes you feel unsafe or worried for yourself or someone else, please know that you can come to me at any time with this concern, and we will work together to find a solution. NOTHING IS EVER SO BAD YOU CAN'T TELL A TRUSTED ADULT.

If I am unable to help you, we will contact the appropriate authorities for advice.

This contract has been created to protect you. It is my responsibility as your parent/ carer to keep you safe, so that you have a positive experience online.



CHILD ABUSE MATERIAL OR

Where can I report?

GROOMING **INAPPROPRIATE CONTENT** thinkuknow.org.au eSafety.gov.au Online child Office of the exploitation eSafety Commissioner **IMAGE-BASED ABUSE** afp.gov.au eSafety.gov.au Office of the eSafety Commissioner AUSTRALIAN FEDERAL POLICE CYBERBULLYING AND HARASSMENT **CYBERCRIME** eSafety.gov.au (Under 18) acorn.gov.au (adults) Attacks on computer systems, email spam and Office of the phishing, identity theft, online scams or fraud eSafety Commissioner Australian Cybercrime Online acorn.gov.au (adults) Reporting Network ACORN NAKED SELFIES AND SEXTING Australian Cybercrir Reporting Network Report it to your child's school/organisation and/or local police

23

SUPPORT

SERVICES



(1800 272 831) bravehearts.org.au

A national support service that can be accessed by anyone wanting information or support relating to child sexual assault.



(1800 99 10 99) childwise.org.au

A not-for-profit child abuse prevention organisation, providing access to trained counsellors.



headspace.org.au

An early intervention mental health service for 12–25 year olds.



(1800 55 1800) kidshelpline.com.au

A free, confidential telephone and online counselling service for young people between 5–25 years.



(13 11 14) Lifeline.org.au

A 24-hour crisis support and suicide prevention service.



Office of the eSafety Commissioner

eSafety.gov.au

Provides resources for students, teachers and parents/ carers on a range of online safety matters. The Office can also help with the removal of explicit and serious cyberbullying material that has been shared online



(1800 184 527) qlife.org.au

A national service that provides anonymous and free LGBTI peer support and referral for people wanting to talk about sexuality, identity, gender, bodies, feelings or relationships.



reachout.com.au

An online mental health organisation for young people and their parents.



thinkuknow.org.au

ThinkUKnow is a partnership between the Australian Federal Police, Commonwealth Bank of Australia, Datacom and Microsoft and delivered in partnership with all State and Territory police and Neighbourhood Watch Australasia. Using real police case studies and examples, ThinkUKnow provides face-to-face education and resources for parents, carers, teachers and students.

ThinkUKnow TOP TIPS

- ••• Start the online safety conversation with your child and let them teach you about what they do online.
- ••• Stay in the know—take an interest in how your child uses technology. Why not have a go and trial the apps for yourself?
- •••• Speak with your child about positive online behaviour. Be an example of the behaviour you expect.
- Whow what your kids are doing online, who they are 'friends' with, and who they may be talking to.
- … Create a Family Online Safety Contract. We've included one in this SOS Guide, or you can also visit <u>thinkuknow.org.au</u>

