THINK U KNOW .org.au

# CYBER SAFETY AND SECURITY GUIDE FOR YOU AND YOUR FAMILY

AFP AUSTRALIAN FEDERAL POLICE

Microsoft

DATACOM

CommonwealthBank

# ABOUT THINKUKNOW AUSTRALIA

ThinkUKnow Australia is a partnership between the Australian Federal Police (AFP), Microsoft Australia, Datacom and the Commonwealth Bank which aims to raise awareness among parents, carers and teachers of how young people are using technology, the challenges they may face and how to help them navigate these challenges in a safe and ethical way.

ThinkUKnow is delivered in collaboration with policing partners New South Wales Police Force, Northern Territory Police, Queensland Police Service, South Australia Police, Tasmania Police, Western Australia Police as well as Neighbourhood Watch Australasia.

ThinkUKnow was originally developed in the United Kingdom by the Child Exploitation and Online Protection (CEOP) Centre, and has been adapted to suit the Australian audience. The Australian Federal Police holds the exclusive licence for ThinkUKnow in Australia.

## WEBSITE

The ThinkUKnow website—**www.thinkuknow.org.au**—provides additional resources including fact sheets, booklets, an e-newsletter and practical tips and resources on protecting your family online.

You can also access the online booking tool through the ThinkUKnow website to organise a presentation, or you can contact 1300 362 936 during business hours.

## CONTACT US

You can contact us at:

**www.thinkuknow.org.au**

**facebook.com/ThinkUKnowAustralia**

**twitter.com/ThinkUKnow_Aus**

# CONTENTS

# YOUNG PEOPLE AND TECHNOLOGY

# SOCIAL NETWORKING

## WHAT IS SOCIAL NETWORKING?

Social networking describes a range of websites and mobile applications that allow users to create a personal profile and connect, interact, and share with other users from around the world.

Social networking allows young people to connect with friends and family, share photos and videos, play games, and chat with other users online.

Many young people may have multiple social media accounts and this often forms an integral part of developing their social identity.

## WHAT ARE THE CHALLENGES OF SOCIAL NETWORKING?

Issues may arise when young people are accepting 'followers' (people) who they do not know in the real world as friends, or when they receive aggressive or hostile communication from friends or followers.

## SOCIAL NETWORKING APPLICATION EXAMPLES

- Facebook
- Instagram
- YouTube
- Snapchat
- Kik Messenger
- Google+
- Twitter
- Club Penguin

## TIPS FOR SAFE SOCIAL NETWORKING

1. Know who your child is friends with online.
2. Talk to your child about what personal information is okay, and what is not okay, to share online.
3. Ensure secure privacy settings are enabled on your child's social networking accounts.
4. Be aware of how to block and report users/pages/groups if an issue were to arise.
5. Know how and where to get help on the various sites and apps they use and check out our list of Useful Websites at the back of this booklet.

# ONLINE GAMING

## WHAT IS ONLINE GAMING?

Online gaming can be a great way for young people to have fun, interact and compete with people from around the world. Online gaming can take place using a device that is able to connect to the internet such as a computer, mobile phone, gaming console (e.g. Xbox or PlayStation) or portable gaming device (e.g. PS Vita and Nintendo 3DS).

Some games are free to play, while others allow users to purchase and download software or pay a subscription fee to play. Online gaming is often much more than simply playing a game. Gaming communities also provide a communication platform, allowing players to take part in instant messaging (IM), chat rooms, blogs and even voice communication using headsets and Voice over Internet Protocol (VoIP).

Among the most popular online games are massive multi-player online role-playing games (MMORPG), where a large number of users participate in an online, virtual world. Players interact using fictional characters, represented by self created avatars, of which they have complete control. There is also a market in trading cheats and gaming credits, and new versions of popular games continue to evolve to meet demand.

Gaming apps on mobile devices have also become very popular and many of these can be downloaded for free or a small fee, but may also include in-app purchases.

## WHAT ARE THE CHALLENGES OF ONLINE GAMING?

Issues may arise when young people are communicating or sharing personal information with players they do not know or know only from the game, or if they receive aggressive or hostile communication while playing.

## EXAMPLES OF ONLINE GAMES

- World of Warcraft
- Clash of Clans
- Minecraft
- Call of Duty
- Steam

## TIPS FOR SAFE GAMING

1. Where possible use private servers to restrict gameplay to a trusted group of people.
2. Encourage your child to avoid sharing personal or private information such as their name, the school they attend or even the name of their local sports team.
3. Ensure your child chooses a username or avatar that doesn't identify personal information like their name or their age (i.e. MattEvanzz98 is not a safe username, WOWisthebest11 is safer).
4. Nothing in life is free—warn your child about accepting gifts (even virtually) from people they don't know.

# CLOUD COMPUTING

## WHAT IS CLOUD COMPUTING?

Cloud computing is where a user can store, share or access data or programs through the internet rather than saving it to a device. While it appears these files are stored in 'the cloud', the files are often physically stored on multiple servers around the world.

Similarly, when using social networking sites or webmail accounts your data is stored in the cloud.

## WHAT ARE THE CHALLENGES OF CLOUD COMPUTING?

There may be some concerns about the security and privacy of sensitive information which is stored in 'the cloud', and the ability of unauthorised people to access this information.

## EXAMPLES OF CLOUD COMPUTING

- iCloud
- Facebook
- Instagram
- Hotmail
- Gmail
- DropBox
- OneDrive

## TIPS FOR SAFE CLOUD COMPUTING

1. Ensure that you use strong passwords for your accounts.
2. Avoid sharing sensitive information over the cloud.
3. Research which cloud computing solution is most appropriate to your needs.

# MOBILE DEVICES AND APPS

## WHAT ARE MOBILE DEVICES AND APPS?

A mobile device is an electronic device which allows for voice or data communication by connecting to a network of base stations known as cell sites. Mobile devices may also support applications such as text messaging (SMS), internet access, photo and video messaging (MMS), Bluetooth, camera and gaming.

If your child has access to a smart phone, chances are they've downloaded some apps. Apps (short for 'Applications') are programs which can be used for a wide range of purposes such as social networking, lifestyle, news and education. Some apps are free, while others can cost anywhere from 99 cents to hundreds of dollars. Additionally, many apps which are free to download require payment to use certain features within the app.

## WHAT ARE THE CHALLENGES OF MOBILE DEVICES AND APPS?

Any device or app when used incorrectly has the potential to cause harm. It is important that you communicate with your child about how they are using a device or application and the legal and ethical ramifications of inappropriate use. They also need to be aware of the dangers of communicating with people they don't know via any device or app.

## EXAMPLES OF APPS

- Google Maps
- Kik Messenger
- Skype
- Candy Crush

## TIPS WHEN USING APPS

1. Research or download the apps your child uses so that you become familiar with the activities they are involved in.
2. Check the classification of apps as these can be a good indication as to whether the content and functionality is suitable for children. Be aware however that classifications are set by the app developers and not independently assessed.
3. Only download apps from the official stores, such as Apple's App Store or the Android marketplace. Illegitimate app stores or app websites may contain pirated apps or malicious software (malware).
4. Before you download and install an app, check which features of your device (such as the GPS function) the app wants permission to access. Disable any features which are unnecessary for the app to access.
5. Many apps contain in-app purchases which can lead to a hefty bill if you or your children aren't careful. To find out how to disable in-app purchases, refer to your device's user guide online.

# PRIVACY MANAGEMENT

# ONLINE PRIVACY

## WHAT ARE THE CHALLENGES?

Children and young people are growing up in a world of privacy changes. They have different notions of privacy than parents, carers and teachers and will ultimately shape our conceptions of privacy in the future.

We need to provide them with the social and digital literacy skills to manage their own privacy, and respect the privacy rights of others.

# POLICIES, TERMS AND CONDITIONS

## WHAT ARE PRIVACY POLICIES AND TERMS AND CONDITIONS?

Whenever you sign up to a social media account or download an app, you are asked to agree to the Terms and Conditions of using that service. Unfortunately, most people tend to scroll to the bottom of the Terms and Conditions and select "I Agree", without reading what they've agreed to.

While it is difficult to enforce the thorough reading of these Terms and Conditions, it is important that children and young people (and the adults responsible for their care) are aware of what they agree to when using these programs and apps. Most Terms and Conditions contain the following:

1. **A licence agreement**—means you license that company to use your content, including photos, messages and browsing activities, for a variety of purposes for their commercial interest.
2. **A law enforcement disclaimer**—means information may be shared with police in a criminal investigation.
3. **Community guidelines**—rules on how to treat others and the site or app itself. These guidelines will also indicate the minimum age to use the site or app which is most commonly 13 years of age. While there are services out there for younger children, such as Club Penguin, the majority of social media services are restricted to users 13 years and above.
4. **A privacy policy**—explains how to manage how your private information is shared, what information the company collects, and what privacy settings you can enable. Adjusting the privacy settings available on the sites you use can give you greater control over who has access to your information.

# GEOTAGGING

## WHAT IS GEOTAGGING?

Geotagging refers to the embedding of location data, such as Global Positioning System (GPS) coordinates, in posts and images taken on smartphones and high-end digital cameras. When these images are shared online, the location data is also shared and can be accessed by other users to find the location of where the image was taken.

An image taken at home and then shared online could reveal the young person's home address, even if you have not tagged your location on the social networking site you are using. There have even been instances where a person has posted on their social media account that they are away on holidays, allowing clever criminals to search through the GPS coordinates embedded in other posts and break into their house while they are on a vacation.

Location information can also be revealed by photos (for example, a photo of a young person in their school uniform can provide their school name and location during the week), location-sharing apps and 'checking in' on social network services. This functionality allows users to share their exact location in real time which can be great for connecting with friends, but could be misused if it ends up in the wrong hands.

## HOW CAN I AVOID POSTS/IMAGES BEING GEOTAGGED?

Geotagging can be disabled through the settings or camera options on your mobile device. This information can be found in your device manual, on the manufacturer's website, or on the ThinkUKnow website—**www.thinkuknow.org.au/site/geotagging**

# E-SECURITY

## SPAM

Spam refers to unsolicited, commercial, electronic messages sent to a person's email account, mobile phone or via social media. These messages may feature advertisements for goods or services, attempts to capture banking or credit card details, or may even contain malware.

## SCAMS

Scams are not unique to the Internet, they have occurred for centuries. The Internet, however, allows for scams to have a much greater coverage. These scams may intend to defraud you of money or attempt to steal your personal details (identity theft).

## MALWARE

Malicious software, or malware, is an unfortunate fact of life when using the internet. Malware includes viruses, worms, Trojans, spyware and adware. These not only have disruptive impacts on how your computer operates, but can also be used to steal your personal information or even allow your computer to be remotely controlled and used for illegal purposes.

Malware can be spread in a variety of different ways including through email (either through attachments or links), clicking on pop-ups or even by visiting infected websites. It might also be spread by using an infected portable storage device in your computer or laptop.

## E-SECURITY TIPS

1. Delete emails from people you do not know without opening or responding to them.
2. Use spam filtering software available from your email account provider.
3. Do not give out your email address or mobile phone number unless you know how that information will be used.
4. Read the Terms and Conditions carefully before agreeing to any offer.
5. Check your credit card and bank account statements and report any suspicious transactions to your bank or financial institution.
6. Never click on a link in an email or web page, type the address into the browser yourself.
7. Install and maintain anti-virus and anti-spyware software on all your devices.
8. Be aware that sometimes spam emails may look like they have come from someone you know—if it looks or sounds unusual, delete it.

**And remember, if it looks too good to be true, it probably is!**

# RELATIONSHIP MANAGEMENT

# CYBERBULLYING

## WHAT IS IT?

Cyberbullying is the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group, which is intended to harm (Bill Belsey, www.cyberbullying.org).

It can be committed using the internet, digital, gaming and/or mobile technologies. 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.

The prevalence rates of cyberbullying in Australia vary with research suggesting between 10-25% of children having experienced cyberbullying. The rate of cyberbullying is still far less than the rate of traditional bullying but its effects can be much more harmful.

**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.

## WHY DOES IT HAPPEN?

The perceived anonymity of the internet and the inability to see the immediate reaction of someone can lead children and young people to behave in a way which they wouldn't necessarily do in a face-to-face situation.

## WHAT ARE THE CHALLENGES?

Cyberbullying can occur 24 hours a day, 7 days a week as children and young people are almost always accessible via their mobile phone or the internet. It is often categorised as covert bullying as it goes unseen or unnoticed by adults.

While every child is different there are a few warning signs that could indicate your child is being bullied:

- changing patterns in how they use the computer or their mobile phone
- increase in text messages, often at all times of the day or night
- trouble sleeping or having nightmares
- becoming withdrawn or depressed
- feeling unwell
- becoming anti-social/not wanting to go out with their usual friends.

## DEALING WITH CYBERBULLYING

**If your child is being bullied …**

- Talk with your child about conflict they may have experienced.
- Keep evidence of bullying behaviour such as instant messenger conversations or online posts.
- Discuss options with your child and their school.
- Report content to the site on which it occurred.
- It is important to avoid removing access to technology as this may prevent your child from talking to you if future issues arise.

**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 FOR ADDRESSING CYBERBULLYING

1. Building parental connectedness can help build resilience in children and help them to overcome conflict.
2. Encourage your child to support their friends who are being cyberbullied and assist them in telling a trusted adult.
3. Provide opportunities for your child to develop their own strategies for combating cyberbullying.
4. Create an environment in which your child is comfortable coming to you with any issues they face online without fear of having their devices confiscated.
5. Talk with your child about appropriate forms of conflict resolution so that they do not resort to cyberbullying.
6. 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.
7. Encourage your child to reduce their exposure to people they don't know who may upset them, by changing their privacy settings.
8. Find out the policies of your school, sports organisation and any of the sites and applications your child uses in relation to cyberbullying.

# ONLINE GROOMING

## WHAT IS IT?

Online grooming occurs when an adult makes online contact with someone under the age of 16 with the intention of engaging in sexual activity (child sex abuse). The offence is committed in the communication phase so no physical contact need ever occur for police to step in, investigate and arrest offenders.

Some offenders pretend to be another young person and develop a friendship with the child, however, a large proportion are upfront with the fact that they are an adult but make the child feel as though an adult-child relationship of this nature is acceptable or normal. Online sex offenders are often very skilled at manipulating children and young people and may 'groom' multiple children simultaneously.

Some offenders will use the anonymity and disinhibition provided by the internet to quickly raise requests for sex with a child or young person. Other offenders may use a gradual approach where a friendship is established, sexual concepts are introduced, the child is exposed to adult pornography and child exploitation material, and finally asked to create their own or meet up for sex.

## WHY DOES IT HAPPEN?

People may be involved in online grooming for financial or sexual purposes. Sadly, the global trade in child abuse material is worth billions of dollars each year.

## WHAT ARE THE CHALLENGES?

Many instances of online grooming are not visible to parents, carers or teachers, and may go unreported. It is important that children and young people are aware of the potential challenge of online grooming and what they should do if someone online makes them feel uncomfortable. Parents, carers and teachers may also wish to keep an eye out for the following potential warning signs of online grooming:

- **Aggressive and secretive behaviour when questioned about their online activities**—this may seem typical of teenagers but when it is outside the child's normal behavioural pattern, it may be an indication that they are being manipulated by an offender online.
- **Unexplained gifts or cash**—both tangible and/or virtual gifts, perhaps given as a gesture of friendship or as payment for some behaviour on the child's part.
- **Change in the use of sexual language**—as part of the grooming process, an offender may introduce sexual concepts into the conversation, show the child adult pornography then child exploitation material, and even ask the child to produce their own child exploitation material. This can have an effect on the language used by the child, as new sexual concepts are introduced.

## TIPS TO KEEP CHILDREN SAFE FROM ONLINE GROOMING

1. Make sure your child's online contacts/friends are people they know and trust.
2. Acknowledge that your child may talk to people they don't know online and let them know to keep their conversations general and avoid sharing personal information.
3. Nothing in life is free— warn your child about accepting gifts from people they don't know.
4. Discuss with your child who they can speak to about sensitive issues or things they may be too embarrassed to tell you about. This might be an aunty or uncle, older cousin or trusted family friend.
5. Talk about the difficult issues – it is important to speak with your child about sex and sexuality (or advise them where to access the correct information) otherwise they may seek advice from untrustworthy people online.
6. Help your child develop strategies for saying no to sexual solicitations from people online.
7. Make sure your child knows how to block and report people on the sites and applications they use.

# INAPPROPRIATE CONTENT

## WHAT IS IT?

The internet is a vast source of information and knowledge, however some content online may be inappropriate or harmful for children and young people. Without adequate supervision or guidance, children could unintentionally or deliberately access inappropriate, illegal or explicit content online. This inappropriate content may in fact be illegal, or simply inappropriate for the age and developmental level of the child.

Some examples of inappropriate content include gossip/rumour pages, meme pages, sites promoting criminal activity or extremist views, filmed fights and sexting. Some of this content may be proactively sought by a child or young person, for example, pornography or pro-suicide websites. Other content may be accidentally encountered either by typing in an incorrect URL, pop-up advertisements or clicking on links in emails.

## WHAT ARE THE CHALLENGES?

Accessing inappropriate material may be psychologically harmful to children and exposure may desensitise children to extreme material, such as pornography, child exploitation materials, radicalised ideologies and criminal activities.

## WHAT CAN I DO?

There are various strategies you can employ to reduce exposure to inappropriate content and any harm caused by exposure.

For children under the age of 10, we strongly advise supervising their use of the internet and exploring technology with them. You can set up bookmarks for the sites they are allowed to use, or create a folder on your tablet or smartphone with the apps or games they are allowed to play. You may also wish to use filtering software, parental controls and safe searching controls.

Children in their tween years may be savvier about the internet and want more freedom to explore it in private. Safe searching and parental controls may still be useful, but it is important to discuss safe surfing and develop a procedure for what they should do if something upsets them online.

Teenagers may be even more difficult to supervise and can often bypass parental controls and filters. It is crucial that they know how to search safely, and where they can go to report prohibited content or seek support for inappropriate content they have come across.

Regardless of age, having open and honest communication with your child about what to do if they come across something which upsets them online should form a critical part of any strategy.

## TIPS TO AVOID INAPPROPRIATE CONTENT

1. Monitor and supervise your child online where possible (particularly for pre-teen children).
2. Know where your children may have access to the internet—at a friend's house, at school, the library—as a parent or carer you will not always be able to control what they can access so talk to your child about what is appropriate for them to be viewing.
3. Discuss appropriate safety guidelines about using the internet and technology. One great idea is to collaborate to make a family internet usage contract.
4. Talk to your children about the importance of understanding that not everything they read on the internet is true. Encourage them to find out who wrote it, what their intentions may be and if they can back up the information from another source.
5. Make sure your child knows which health and wellbeing sites are trustworthy so that they receive advice from appropriate sources.
6. Reinforce with your child that illegal activities conducted online can be traced by police and they may be held criminally responsible for their actions if they are over the age of 10.
7. Help your child to develop digital literacy skills important for assessing the reliability of sources online.
8. Provide your child with a list of mental health and wellbeing support services which they can access online, such as **www.headspace.org.au** and **www.reachout.com.au**.
9. Talk with your child about why pornography is not an accurate depiction of healthy adult sexual relationships and why it shouldn't be seen as a form of education.
10. Encourage your child to come to you or a trusted adult if they see something online that makes them feel uncomfortable.

# SEXTING

## WHAT IS IT?

'Sexting' is the sharing of sexually explicit images or messages. Sometimes, children and young people may create and share content which is inappropriate or even illegal online or over mobile devices. This content may damage the relationships and reputation of your child or others, lead to offline confrontation or even result in criminal charges.

## WHY DOES IT HAPPEN?

Young people may engage in this activity to show intimacy with their partner, in the hope to obtain a partner or to express themselves to others. Most studies show that only a minority of young people are involved in sexting and it is often linked to physical sexual activity.

## WHAT ARE THE CHALLENGES?

Sending sexually explicit images or text messages can have significant ramifications both legally and ethically. It is important that you encourage your child to think about the permanency of the images and messages they send, post or receive.

### DID YOU KNOW?

Legally, if the person represented in the image or text is under the age of 18, it can be considered 'child pornography' under Commonwealth and State or Territory legislation. These offences can carry significant penalties and can even result in a young person being listed on a sex offender's registry.

Ethically, it is important for young people to be aware that as soon as they send or post something online, they no longer have control over where that image or message will end up, or who will see it.

## TIPS TO AVOID SEXTING

1. Encourage your child to think before they post.
2. Discuss ethical sexual relationships with your child.
3. Take a social norms approach—highlight that only a minority of young people engage in sexting and that your child should not feel pressured to do the same as an attempt to 'fit in'.
4. Help young people develop effective strategies for saying 'no' to avoid creating inappropriate content.
5. Discourage the use of pornography as an educational resource.
6. Help your child understand that if they receive an image of someone, it's not their photo or their body, and therefore not their choice to share it.


REPUTATION
MANAGEMENT

# REPUTATION

Social media can be a useful tool for keeping in contact with friends and family. It can enable young people to create their own space, express their personality and market themselves to the world. This can help them to formulate their sense of identity. However, young people have to be aware of what information is shared and with whom.

The images and information posted on social networking sites can define or damage your online reputation. Employers may use social networking sites to 'research' job candidates. This may not affect young people now, but the content they post on the internet today could damage their future job prospects.

Taking simple precautions to secure social networking profiles and what is posted can ensure any private and personal information shared is protected.

## TIPS FOR PROTECTING YOUR (ONLINE) REPUTATION

1. Encourage your child to **think before they post**—take two seconds to pause and reflect on what they are posting and how it could affect them and others, now and in the future.
2. **Suggest your child regularly searches themselves online, and do the same yourself.** You can use normal search engines such as Google and Bing, or meta search engines such as **www.pipl.com** and **www.dogpile.com** which search multiple databases at once. Also search for usernames, email addresses and gaming handles.
3. Encourage your child to **discuss with their friends** what material they are sharing about them and others.
4. **Make sure your child's profile is set to private.** This allows some control over who can see the images and status updates they may post.

**Don't forget—what goes online stays online!**

# TAKING ACTION

# WHERE CAN I REPORT CYBERCRIME?

## ONLINE CHILD SEXUAL EXPLOITATION

**If you think a child is in immediate danger, call Triple Zero (000).**

If you believe that someone has behaved inappropriately or in a sexual manner towards a young person, report this to the Australian Federal Police via **https://forms.afp.gov.au/online_forms/ocset_form** or contact your local police.

## CYBERCRIME—ACORN

You can report common types of cybercrime such as hacking, scams, fraud, identity theft, attacks on computer systems and illegal or prohibited content to the Australian Cybercrime Online Reporting Network (ACORN) by visiting **www.acorn.gov.au** and following the on-screen prompts.

## CYBERBULLYING

Cyberbullying should be reported to the site on which it occurs using the report/block functions. Further advice on reporting cyberbullying can be found on ACORN (see above) or by talking to your child's school.

## CHILD ABUSE

Child abuse should be reported to your local police.

You can also report crime anonymously by calling Crime Stoppers on **1800 333 000** or submitting a report online.

# USEFUL WEBSITES AND CONTACTS

## INFORMATION

ThinkUKnow
**www.thinkuknow.org.au**

ACORN
**www.acorn.gov.au**

iDcare – identity security service
**www.idcare.org**

## COUNSELLING AND SUPPORT SERVICES

Lifeline
13 11 14
**www.lifeline.org.au**

Kids Helpline
1800 55 1800
**www.kidshelp.com.au**

Reach Out
**au.reachout.com**

Bullying. No Way!
**www.bullyingnoway.gov.au**

Headspace
**www.headspace.org.au**

# SPEAKING TO YOUR CHILD ABOUT CYBER SAFETY

Encourage your child to communicate openly with you about the 'online' world, the challenges they may face, what they can do and who to talk to if they experience issues.

While many parents feel as though they are unequipped to discuss cyber safety, it's important to remember that many of the behaviours and issues we experience online are no different to those in the 'real' world – it's only the medium that has changed.

Education and communication are the most powerful tools parents, carers and teachers can use to address issues that children and young people may face online.

## BELOW ARE SOME GREAT WAYS TO START THE CYBER SAFETY DISCUSSION!

**Let them teach you!**
Your child was born into a world with technology and many can easily navigate it as if it were second nature. By allowing your child to teach you, you can see how well they explore cyberspace and identify if they need help with cyber security measures like privacy settings.

**Be in the know**
Take an interest in how your child uses technology. Are they using it to play games, talk to friends or create a blog? The more actively involved you are in how your child uses technology the more likely they are to talk to you if something goes wrong.

**Watch a movie**
There are plenty of movies that introduce challenges that children and young people may face online. Movies can be a great way to raise a topic with your child and can promote healthy discussion around what they could do if they were in that position. Check out some of the videos online at **www.thinkuknow.org.au**.

**Put it in writing!**
Speak with your child about your family values and how this extends to behaviour online. It can be a great idea to create a family internet usage contract together so that everyone in the family knows what is expected of them while they're online. A template is available at **www.thinkuknow.org.au**.

# CYBER SAFETY CHECKLIST

- ☐ **Stay up to date**—keep up to date with how your child uses their mobile devices and new apps.
- ☐ **Open lines of communication**—it is important to regularly discuss cyber safety and talk about issues your child may experience. By establishing these open and honest lines of communication your child is more likely to come to you if they experience a problem online.
- ☐ **Supervise your child**—monitor and supervise your pre-teen child when they are using the internet and mobile devices to ensure their safety.
- ☐ **Parental controls**—it may be necessary to use parental controls on mobile devices to establish limits on how and when children can access certain sites or games. It is important to note that parental controls should only be used in conjunction with open lines of communication with your child.
- ☐ **Protect your devices**—use anti-virus software and keep your operating system up to date.

## SHARE THESE CYBER SAFETY TIPS WITH YOUR CHILD:

1. **Don't share too much information online**—avoid sharing personal information such as your name, email, home address and school online—even when playing online games.
2. **Have STRONG passwords or passphrases**—make sure you have strong passwords which have at least eight characters including letters, numbers and special characters. It is also important to have different passwords for different accounts!
3. **Know who your friends are**—it is important to make sure that your online friends are people you know in real life, you trust and are people you actually want to talk to.
4. **Stay private**—make sure social networking profiles or online game profiles are set to 'private' or 'friends only'.
5. **Don't click that link**—avoid clicking on links in emails, they could be spam or scams.
6. **Don't be a keyboard warrior!** If you wouldn't say it to someone's face, don't say it online.
7. **Think before you post**—once it is on the internet it is there forever. Think about who might see it or where it might end up years into the future.

# NOTES


NEW SOUTH WALES
POLICE FORCE


NORTHERN TERRITORY
POLICE


QUEENSLAND
POLICE


POLICE


TASMANIA
POLICE


WA
POLICE


NEIGHBOURHOOD WATCH
AUSTRALASIA INC.
INCORPORATED
2006