of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws
cyberbullying
Submission 18 - Attachment 1

SOS

GUIDE TO CYBER SAFETY

THINK U KNOW .org.au

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, crime prevention program. ThinkUKnow is pro-technology.

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, what they can do 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 about how to stay safe online at **www.thinkuknow.org.au**

To book a ThinkUKnow presentation, you can book online or contact the booking centre on 1300 362 936 during business hours.

facebook.com/ThinkUKnowAustralia

twitter.com/ThinkUKnow_Aus

ThinkUKnow is a free program, delivered by volunteers from:

In collaboration with:

WHAT THEY SEE

Having open and honest communication with your child about what to do if they see something that upsets them is important.

Young people often use the internet to pass time. They may search for videos, interesting information, or use it to answer questions. Teenagers in particular might access websites to learn more about the changes happening to their bodies, as well as information on relationships and sexuality.

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

Accessing inappropriate 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.

WHAT CAN I DO?

- Have open and honest conversations with your child about what to do if they see something online which upsets them. A list of support services can be found on the last page of this guide and at thinkuknow.org.au.
- Encourage your child to come to you or a trusted adult if they see something online that makes them feel uncomfortable.
- Know the content your child is searching for online.
- Know the places your child may access the internet—at a friend's house, at school, at the library.
- Discuss appropriate safety rules about using the internet and technology. Our **Family Online Safety Contract** is a good way to start discussions.
- Talk to your child about the importance of understanding that not everything they see online is true.
- Reinforce that illegal activities conducted online can be traced by police and they may be held criminally responsible for their actions, including cyberbullying.
- Where possible, supervise internet use of very young children.
- Consider filtering software, parental controls and safe search controls.

WHAT THEY SAY

Young people use the internet to chat and socialise with their friends, and sometimes to make new friends. This can be done through social networking websites, chatrooms or apps, and includes things such as posting content to a person's Facebook page or commenting on a photo on Instagram.

Popular chat app choices for young people include Kik, WhatsApp and Whisper. However, what is most popular changes constantly!

Instant messaging or direct chat is sometimes built into apps and games. Think Snapchat, Minecraft, Call of Duty, Instagram, Facebook, and Skype.

Be aware: Not everyone online is who they say they are. Some apps don't require registration or verification so you may never know who your child is chatting to.

WHAT CAN I DO?

- Know who your child is friends with online. Ask them if they have met them/know them?
- Know which apps, social networking websites, or instant messaging functions your child is using.
- Talk to your child about what personal information is okay to share online.
- Ensure secure privacy settings are enabled on your child's social networking accounts and devices.
- Be aware of how to block and report users, pages or groups.
- Know how and where to get help on the various sites and apps your child uses.
- Discuss appropriate safety rules about chatting to people online.

Our **Family Online Safety Contract** in this guide is a good way to start discussions with your children about online safety.

WHAT THEY DO

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

Any device or app when used incorrectly has the potential to cause harm. The best way to find out what your child does online is to ask them, but here are some common activities.

SOCIAL NETWORKING

FACEBOOK
INSTAGRAM
SNAPCHAT
YOU TUBE
MUSICAL.LY
WHATSAPP
SKYPE
TWITTER
PERISCOPE

WHAT CAN I DO?

- Research or download the apps, games and websites your child uses so that you become familiar with how they work. The ThinkUKnow website has lots of tips for apps.
- Before you download games 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.

GAMING

CALL OF DUTY
MINECRAFT
CANDY CRUSH
CLASH OF CLANS

APPS

HAPPN
MESSENGER
POKEMON GO
TINDER
MUSICAL.LY
KIK

- 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 apps 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 Android marketplace.
- Make sure your child only has people they know and trust as online friends and contacts.
- Talk to your child about strategies to avoid being pressured into sharing or doing something online they are not comfortable with.
- Ensure your child is aware that they should never arrange to meet someone in person they've 'met' online without taking along a trusted adult.

KNOW THE CHALLENGES

Just like everything we do, there are some challenges we may face online.

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

privacy

your data

information sharing

relationships and personal safety

dating and sexting

cyberbullying

reputation

WHAT CAN I DO?

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

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

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 settings).

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

1. **A licence agreement**
   This allows the service to change, add, delete, publicly display, reproduce, copy, distribute, sell and use your personal information. This includes your photos, posts, private messages, comments and videos without your permission.
2. **Law enforcement disclaimer**
   This means the service can provide information to police for investigative purposes.
3. **Community guidelines**
   These are the rules around how to use the service and consequences for breaking the rules, such as shutting down an account. These guidelines also usually indicate the minimum age requirement for using that service.
4. **Privacy policy**
   This explains what private information the service 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 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 and financial details to enable them to commit fraud.

Malware

Malware is software you may be tricked into installing that will track what you are doing or may even freeze your device forcing 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.

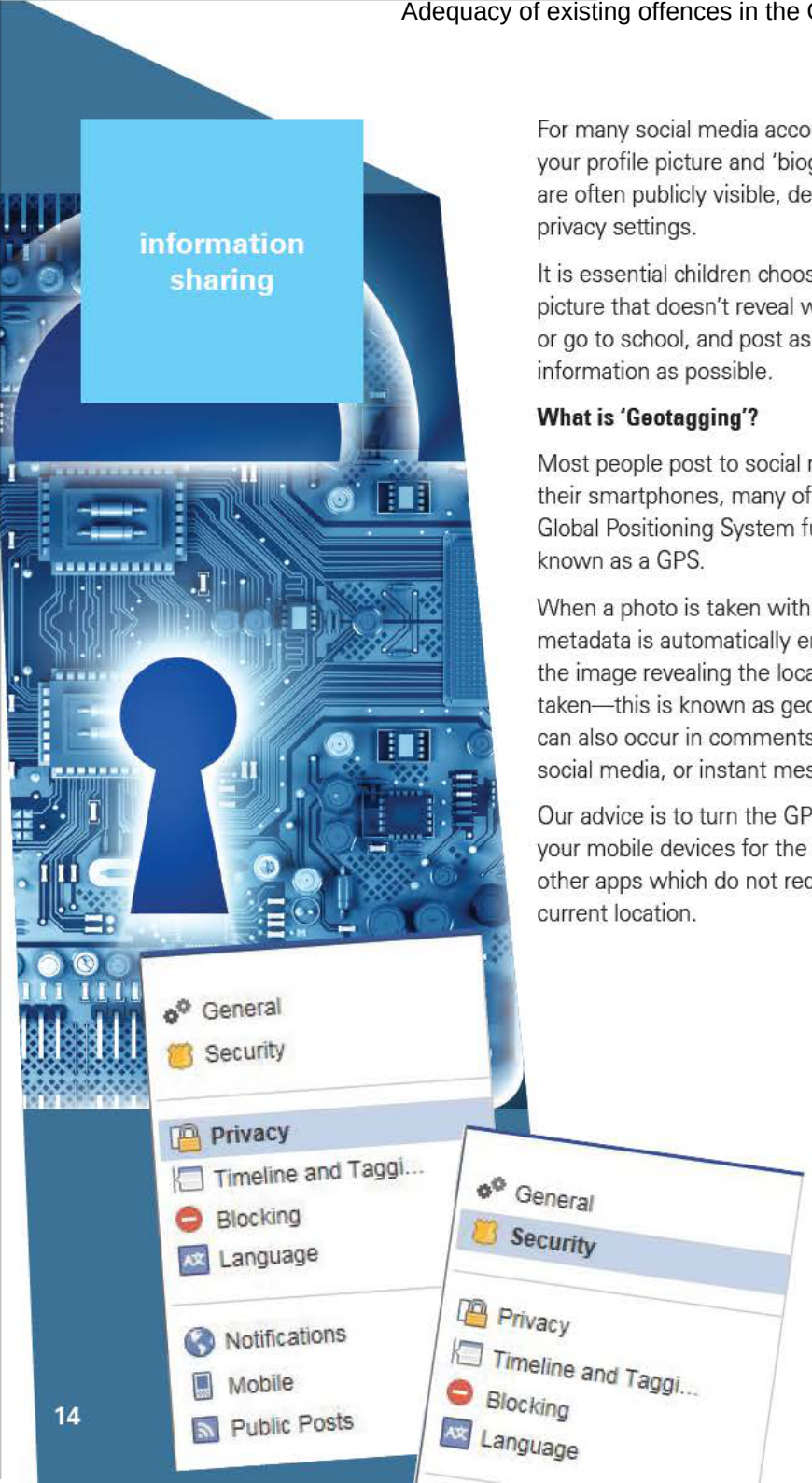
WHAT CAN I DO?

- Use a passphrase that has more than 16 characters and includes numbers, letters and symbols.
- Passwords should be changed regularly, and not used for multiple accounts.
- Use spam filtering software available from your email account provider.

Tell your children 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.

Having strong security for your accounts can help protect you from unauthorised access, extortion, identity theft or fraud.



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

It is essential children choose a profile picture that doesn't reveal where they live or go to school, and post as little personal information as possible.

What is 'Geotagging'?

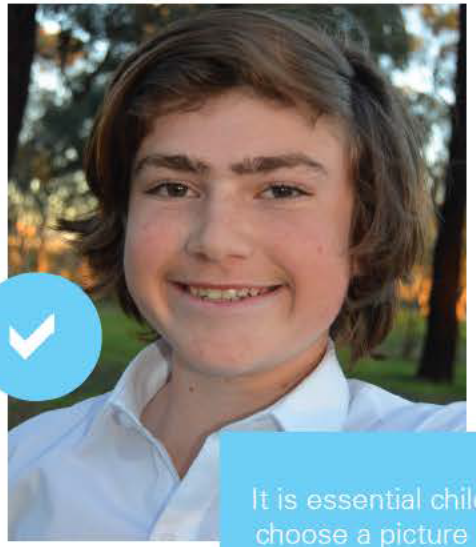
Most people post to social media from their smartphones, many of which have a Global Positioning System function, better known as a GPS.

When a photo is taken with the GPS on, metadata is automatically embedded into the image revealing the location it was taken—this is known as geotagging. This can also occur in comments posted on social media, or instant messages.

Our advice is to turn the GPS off on your mobile devices for the camera and other apps which do not require your current location.

WHAT CAN I DO?

- Encourage your child to use the most secure privacy settings for their accounts.
- Check the privacy policies and Terms and Conditions of the sites and apps your child uses.
- Discuss with your child what personal information should never be shared online.
- Turn off the location in the device 'settings' for apps that don't require a GPS.
- If your child does not meet the minimum age requirement and you are comfortable with them using the account or app, record and save their login details to check their activity.
- We also discourage young people from sharing their location on social media, such as through 'checking in'.



It is essential children choose a picture that doesn't reveal where they go to school or live, and post as little personal information as possible.

relationships and personal safety

Online grooming

Online grooming is when an adult makes 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 of what young people 'do' and 'say' online, and they use various techniques to 'lure' young people in order to make communicating with them easier.

Do you know who your children are talking to?

WHAT CAN I DO?

- Have a discussion with your child about who they might be communicating with online. Do they really/actually know them?
- Ensure your child's contacts are people they have met, trust, and are safe to communicate with on a regular basis.
- Young people should never send photos or share personal information to unknown people, including their location.
- Nothing in life is free—warn your child about accepting gifts from people they don't know; they might want something else in return.
- 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 it's important to remind them that they have the right to feel safe, and not to fear taking actions to preserve that safety.
- 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 your 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 online sexual abuse, act on it.
- Anyone can report abuse or illegal activity online at afp.gov.au or by clicking on the 'Report Abuse' button at thinkuknow.org.au.
- 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.

dating and sexting

Sexting or sending 'nudes' refers to the sharing of explicit texts, images or videos.

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.

Sending sexually explicit images or text messages may have legal and ethical implications. It is important that you encourage your child to think about the material they send, post or receive.

There is also a trend toward apps that share 'erasable' media, where young people send material believing that it 'disappears' after a short time. However, entire deletion cannot be guaranteed and content can easily be copied or forwarded without permission.

Vault, safe, or decoy apps—also known as 'ghosting' apps—might look like legitimate apps, but can be used to store and hide images.

WHAT CAN I DO?

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

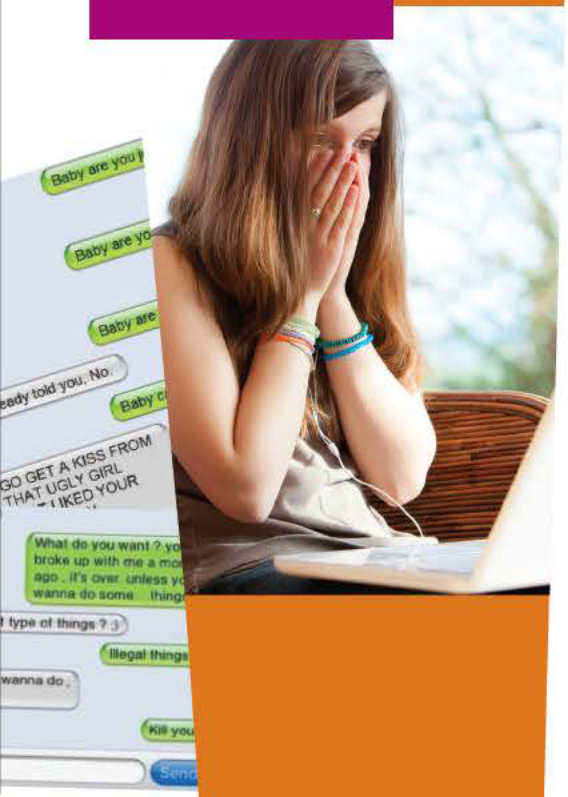
If your child has been creating, sending or receiving 'sexts':

- 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. However, under Commonwealth law, an image of someone under the age of 18 in which they are naked, in a sexualised pose, or engaged in a sexual act may constitute child pornography offences.
- 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.

dating and sexting



Sextortion

'Sextortion' is a relatively new crime type. It occurs when someone threatens to distribute your private and 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 information or images they have obtained unless victims comply with their demands.

WHAT CAN I DO?

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

If you have been threatened:

- Block emails and accounts and cease all contact.
- Save the details, emails, comments or other evidence you have of that person's attempt to extort you.
- Often the only leverage others have is your embarrassment—you may need to think about how you manage this.
- If you find images of yourself on a site—you can try to get them removed by contacting the site administrator.
- In certain circumstances Google may also remove images from their search results.
- Paying scammers or extortionists is never encouraged—once you have paid or complied with their demands, there is nothing preventing them from targeting you again.
- Report the incident to your local police, ACORN or the Office of the eSafety Commissioner.
- If you need to talk consider contacting counselling or support services, such as Lifeline or Kids Helpline.

cyberbullying

Cyberbullying is the use of information and communication technologies to support **deliberate**, **repeated** and **hostile** behaviour.

This kind of bullying can cause great distress and impact on a child's self-esteem and confidence. Young people may feel there is no safe place to hide from it.

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.

If your child is being cyberbullied:

- Talk with your child about conflict they may have experienced.
- Help build resilience to deal with nasty one-off comments.
- 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.
- If the content is not removed within 48 hours, report it to the Office of the eSafety Commissioner esafety.gov.au/reportcyberbullying
- 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 cyberbullying others:

- Explain to your child why bullying is unacceptable.
- Find out why the cyberbullying 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 where 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 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 online they don't know.
8. Find out the policies of your child's school, sports organisation and any of the sites and applications your child uses in relation to cyberbullying.

Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying
Submission 18 - Attachment 1

reputation

Our digital shadow can reveal a lot about who we are—this includes our social media 'likes' and 'shares', as well as our contacts and associations online.

Young people should be encouraged to stop and think before posting or sharing something online.

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.

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 reduce private and personal information being shared.

What does your digital shadow say about you?

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.
- Make sure your child's profile is set to 'private' when using social media and apps.
- 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.

TAKING ACTION

Grooming

thinkuknow.org.au

Online child exploitation

THINK U KNOW .org.au

afp.gov.au

AFP AUSTRALIAN FEDERAL POLICE

Cybercrime

acorn.gov.au (adults)

Attacks on computer systems, email spam and phishing, identity theft, online scams or fraud

ACORN Australian Cybercrime Online Reporting Network

Child pornography

eSafety.gov.au

Online child sexual abuse material

Australian Government | Office of the **eSafety Commissioner**

Cyberbullying and harassment

eSafety.gov.au (youth)

Australian Government | Office of the **eSafety Commissioner**

acorn.gov.au (adults)

ACORN Australian Cybercrime Online Reporting Network

Naked selfies and sexting

Report it to your child's school/ organisation and/or local police

USEFUL WEBSITES AND CONTACTS

INFORMATION

ThinkUKnow
thinkuknow.org.au

COUNSELLING & SUPPORT

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

FAMILY ONLINE SAFETY CONTRACT

Look on the opposite page for our Family Online Safety Contract.

Take a few minutes to sit down with your child and discuss what you expect from them online.

Use this time to come to an agreement on how you'd like them to use the internet and what you will do as a family if something goes wrong.

Also explain that there is a section for parents to sign and consider as well. This is a two way agreement. Parents, will you agree to not embarrass your children with photographs and comments on social media?

Here's some examples to include.

For kids

- I will never meet someone in person that I have only spoken to online, and I will tell my parents if someone asks to meet me.
- I will not respond to emails, instant messages or friend requests from people I don't know.
- I will put my devices to bed at night to help me get a restful sleep.

For parents

- 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.

Need help filling it out? For a version with included suggestions, visit thinkuknow.org.au

THINK U KNOW .org.au

the Carly Ryan foundation

FAMILY ONLINE SAFETY CONTRACT

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

CHILD

I _____, will:

PARENT/ CARER

I _____,will:

Signed: _____ (Child)

Signed: _____ (Parent/carer)

ThinkUKnow TOP TIPS

- Start the cyber 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 respectful relationships.
- Create a Family Online Safety Contract. We've included one in this SOS Guide, or you can also visit thinkuknow.org.au.
- Know what your kids are doing online, who they are friends with, and who they may be talking to.

www.thinkuknow.org.au

THINK U KNOW .org.au

TUK 16 1119