eSafety Parent Communication and Engagement Strategy

Objective:	To develop a 10 week eSafety Parent Communication and Engagement Strategy
Target audience:	Parent group
Responsibility:	Assign who's responsible for developing and delivering which message and make sure to get their full commitment.
Key messages:	You need to know or learn what motivates your parent group.
	1. 6.
	2. 7.
	3. 8.
	4. 9.
	5. 10.
Timing and frequency:	Find out the best time and frequency needed to get your messages across and achieve your goals. Sort out which message should occur when considering other key dates and deadlines.
Sensitivities:	Have there been any critical incidents to be aware of that might relate to any of the key messages?
Channels:	Choose the right combination of vehicles to carry your messages to your target audiences eg: school app, school website, social media channels, parent/teacher meeting.
Evaluation:	Indicate how the results and effectiveness of the communication plan will be measured.

Commissioner's blogs

- * Is your child at risk of self-harm or suicide?
- * Don't be in the dark about 'dark social'
- * 'Revenge Porn' by another name
- * Don't go breaking my heart...online
- * Back to school: parents encouraged to #talkb4sharing
- * Tackling online pornography on many fronts
- * The perils of image-based abuse
- * Playing safe? The nuts and bolts of connected toys
- * Social engineering: a very human problem

- * Fighting for a respectful (online) society
- * Instagram and Facebook Live: Redefining living in the moment
- * Combatting cyberbullying on multiple fronts
- * Are we allowing strangers into our lounge rooms through our children's technology?
- * Protecting children in the darkest places
- * Is there such a thing as "safe sexting"?
- * Can parenting be outsourced in the sharing economy?
- * You give me yours and I'll give you mine

iParent themes

Online risks	Cyberbullying, Inappropriate, offensive and illegal content, Online pornography, Sexting, Trolling and Unwanted contact.
Staying safe	Digital legacy, Is 'sharanting a good idea?, Online basics, Balancing time online, digital reputation, e-security, online gaming, photos, video and social media, protecting personal information, privacy, social networking, connected toys.
<u>Multimedia reviews</u>	Movies and games, TV.
Online safeguards	Filtering software, parental controls, search safely.
<u>Get help</u>	Immediate help, support for kids, support for parents, reporting.

Cyberbullying support tool for parents

Sometimes cyberbullying feels like a minefield. As a parent it can be hard to know if a situation qualifies as serious cyberbullying. Work your way through our <u>support tool</u> for guidance on how we can help you.

Research insights

Young and social online

The video illustrates young people's use of social media and their attitudes towards it. It also includes data on the top 5 social media services used, privacy settings and personal information shared on social media by young Australians. Young people's likes and dislikes about social media are also covered.

Connected kids and teens

The video explores the digital practices of teens and kids. They use a range of devices to go online. There are key differences between the online habits of teens and kids.

Teens, kids and digital dangers

The video presents the findings on kids' and teens' negative experiences online, particularly cyberbullying. It sets out the prevalence of specific cyberbullying behaviours, the adverse effects of negative online experiences and any action taken after the incident. It also explores the types of cyberbullying incidents witnessed by kids and teens.

Chatterbox video series

Chatterbox aims to empower parents to approach eSafety issues with confidence and increase understanding of the main online safety issues children experience.

Selfies and Someone-Elsies	The episode explores some of the risky behaviours young people can engage in while online and offers tips on how to manage some of the most common parenting challenges in the online world.
Tots, Teens and In-Betweens	Has the digital world changed childhood forever or will kids always be kids regardless of changing environments? Chatterbox ponders where technology fits with the trials and tribulations of growing up.
Trolling, Tagging and Bagging	The episode explores the potential for harm if social media is misused and the need for young people to be aware of the rules and etiquette principles that apply to digital interactions.
The Internet's Underbelly	The digital world has made pornography accessible, anonymous and affordable, but for young people it can be damaging and disturbing. This episode focuses on accessing age-inappropriate content and unwanted contact.
Screentime and Downtime	Kids now consume many hours of screen time a day and it can become excessive or compulsive and interfere with their physical, mental and social health. This episode explores the idea of a healthy balance of offline and online time.
<u>Digital Rights</u> <u>versus Digital</u> <u>Wrongs</u>	Young people are still developing their self-regulation skills. In this episode we explore the tools and knowledge needed to deal with ethical situations online.
Parental Control Tools	The episode examines parental control tools, their benefits, their limits and how they can help you manage your child's online time.
<u>Blurred Lines</u>	Who has responsibility for a child's eSafety education? This episode looks at the blurred lines between parenting, teaching and protecting and communicating with your children in the digital age.
Cyberbullying	Figuring out what to do if your child has experienced cyberbullying can be daunting. This episode simplifies the information down to the four essential things.

Infographics



Kids Online



7 Ways



<u>Parenting Online</u>



Social Media



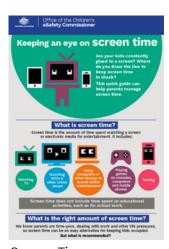
Health Check



Age Limits



How to Report



Screen Time



Checklist

Newsletter articles

- 1. Cyberbullying supporting your child online
- 2. Supporting your child's safe online social networking
- 3. Protecting your child's digital reputation
- 4. Advice to help manage children's time online
- 5. Supporting your child's safe mobile phone use
- 6. Managing unwanted online contact
- 7. Supporting your child's safe use of online games and in-app purchases
- 8. Managing sexting
- 9. Being a helpful bystander against cyberbullying
- 10. Protecting your child against online identity theft
- 11. Trolling online what it is and how to support your child
- 12. Avoiding online spam, scams and phishing
- 13. Safe use of location-based services

1. Cyberbullying – supporting your child online

Childhood bullying used to be face-to-face physical and verbal behaviour in the playground, classroom and on the way to and from school. Now online technology and constant connectivity has allowed bullying to harm children through often anonymous contact or actions. Cyberbullying can happen at any time and leave a child feeling unsafe and alone.

Cyberbullying commonly occurs through:

- * Comments posted in an open online environment such as Facebook.
- * Direct text, email or instant messages online or on a mobile phone.
- * Private features on social networking services such as Snapchat and Facebook Messenger.

Children can manage cyberbullying with your support by taking the following action:

- * **Blocking the person** cyberbullying and changing privacy settings. Retaliating or responding to the perpetrator only gives them the attention and power they want.
- * **Reporting the bullying.** Most websites have online <u>safety centres</u> and reporting facilities. Online abuse is in violation of the Terms Of Use of most social networking sites. The Office of the eSafety Commission can take <u>complaints</u> and provide assistance in relation to serious cyberbullying material that is directed at a particular child with the intention to seriously embarrass, harass, threaten or humiliate.
- * Collecting the evidence. Keeping mobile phone messages and printing emails or IM conversations.
- * Talking to someone they trust like parents or a teacher.
- * **Visiting iParent** for a list of sources of professional <u>support</u> including the Kids Helpline on 1800 55 1800, eheadspace on 1800 650 890 or <u>parentline</u>.
- * Taking the cyberbullying quiz. There is also a quiz for parents.
- * Watch the "Chatterbox" video and listen to the podcast about cyberbullying.

2. Supporting your child's safe online social networking

Social networking is an extension of offline friendships and we should treat people respectfully in the same way we do in real life. Chatting to friends using IM, chat or social networking is a great way to stay in touch and make new friends. However, your child should always keep in mind that there are some risks meeting people online—especially if they don't know them in real life.

Discuss the following aspects with your child to help them safely enjoy social networking.

- * Limit your friend list. Do you know your online friends in the real world? If not, consider changing your settings to limit interaction with them or remove them.
- * Protect personal information. Restrict information that people can use to access your finances, and to identify where you live, work or go out.
- * **Check on your images.** Does everything about your life really need to be online? How might this affect you and your reputation in the future? Take a look at the eSafety website for some <u>tips</u> for taking photos and videos and sharing them online.
- * Stay respectful. Are your posts respectful to friends and others? This is real life; being online is no excuse for bad behaviour.
- * Think twice before meeting offline. If you want to meet someone offline it is essential to take an adult with you, meet in the daytime and in a public place. Don't share personal information too early.

It is important to note that there may be age restrictions that apply to your child joining a social network. Many popular social networks are restricted to users above 13 years of age. Check out the <u>infographic</u> "Is there an age limit for kids on social media?"

If your child or someone they know wants to talk about challenging online friendships, call the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890.

3. Protecting your child's digital reputation

Children, especially during their teenage years, learn the importance of their reputation as a part of growing up.

Offline, a child's reputation can be established through behaviour in the classroom and the playground, their treatment of friends, and academic, artistic or sporting achievements. Your child's online reputation is defined by both the content they post about themselves and what others post about your child.

Tagged photos, blog posts and social networking interactions will all shape how your child is perceived online and offline. A poor digital reputation can affect friendships, relationships and future job prospects.

Children can protect their digital reputation by:

- * Thinking before they post. Does everything about their life really need to be online? How might this affect them in the future?
- * Setting their profile to private and checking privacy settings regularly to make sure default options haven't changed. This will allow them to <u>control</u> who sees what they post online. Visit the eSafety <u>website</u> for more information on how to protect your child's privacy online. The eSafety website has a section on <u>games</u>, <u>apps</u> and <u>social networking</u> with step-by-step instructions to control your settings for each social networking platform.
- * **Keeping an eye on photos tagged by friends.** Even if your child's profile is private, the content friends post might be available for the world to see. Some social media sites allow users to approve tags before they are attached to their profile.

If you or your child wants to learn more about <u>digital reputation</u> issues, you can visit the eSafety website.

4. Advice to help manage children's time online

A child's life is full of opportunities for them to spend time out of school with community groups, sporting clubs and their friends. Spending time online is also a regular activity for many children who enjoy communicating with friends, sharing information and playing games.

Whilst there are no guidelines for the 'right' amount of time someone should spend online or gaming, if your child is being negatively impacted by excessive use it may be time to discuss how they can take action to maintain a healthy balance. Australia's National Physical Activity and Sedentary Behaviour <u>Guidelines</u> tell us what health professionals recommend is appropriate for entertainment. You can read more about this on the eSafety website and download the <u>infographic</u> "8 tips to keep on top of your child's screen time".

Some tips to guide you in helping your child maintain a healthy balance between online and offline activities for the benefit of their health and wellbeing can be found on the eSafety <u>website</u>.

- * Look for indicators that your child may be spending too much time online, such as a declined interest in other activities, talking constantly about an online game or activity, a decline in grades, or irritability.
- * **Discuss** how other aspects of their life are being affected. Excessive use can impact on someone's health and wellbeing, family, relationships, work or education.
- * Consider establishing rules about when your child can play games or use the internet and how long they can play for. You might make a mutual agreement to set a balance of online and offline activities. You may need to establish consequences for rule breaches. Depending on the age of the child you may also set passwords that they do not know.
- * Locate the computer or device in a shared or visible place in the home so you know how much time your child is being spent online and what they are doing online. Set limits at night and remove technology devices from bedrooms.
- * **Seek** support if you have concerns. Visit <u>Parentline</u> in your state to access help through counselling, information and referral. Take a look at the "Chatterbox" video and podcast about <u>screentime and downtime</u>.

5. Supporting your child's safe mobile phone use

Mobile devices are great for keeping in touch and now with smartphones your child can connect online whenever and wherever they are.

You can support your child's use of their mobile phone by making them aware of the following:

- * **Nothing is really ever free.** Be wary of advertisements for free downloads; you may be automatically subscribed to a service which can become very expensive. When buying a phone, check details of the plan or contract and don't accept offers that sound too good to be true.
- * **Protect your privacy.** Only give out your mobile number to people you know and trust. Don't give out other people's number without their permission.
- * Think before you send or forward mobile content such as photos, texts and videos. Where might they end up?
- * Activate security features so that if your phone is lost or stolen, you can protect your personal information.
- * If your phone is lost or stolen, notify your network carrier and the police immediately. It is smart to record your unique International Mobile Equipment Identity (IMEI) number just in case it is lost or stolen in the future.
- * Treat your phone like your wallet. Don't store bank PINs or other <u>passwords</u> in your phone. Use a pin code to lock your phone if possible.

Watch the "Chatterbox" video and listen to the podcast about <u>parental controls</u>. You can also get further information about <u>parental controls</u> for computers, tablets and smartphones on the eSafety website.

6. Managing unwanted online contact

The internet has opened an unprecedented opportunity for people to communicate and receive information anywhere and at any time.

Through email and social networking, we can engage with people who are both well known, existing friends and new friends that we may never meet face to face or speak with offline.

It is important for your child to understand that as in the offline world, some people online have ill intentions. Unwanted contact is any type of online communication that your child finds unpleasant or confronting. The contact can come from unknown online friends or someone they actually know in the offline world.

Consider these steps to help your child manage unwanted contact:

- * Encourage your child to raise concerns with you or another trusted adult.
- * **Block the person** contacting your child and change the privacy settings. Don't respond to the person or give them any attention.
- * **Keep the evidence.** This can be useful in tracking the person posting unsuitable material. A guide to <u>collecting evidence</u>, along with some helpful videos on how to collect <u>screenshots</u>, is available on the eSafety website.
- * Contact the ISP, phone provider or site administrator. There are actions they can take to help.

Visit the eSafety website for ways to deal with <u>unwanted contact</u> and watch the Chatterbox video <u>The Internet's Underbelly</u> or call the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890 to chat with an experienced counsellor.

For some more useful tips, download the parent's guide to online safety.

Visit the iParent website for <u>more information</u> on ways to minimise risk <u>online</u>, without fear of online predators.

7. Supporting your child's safe use of online games and in-app purchases

If your child plays online games and uses apps it is important to use the games safely and understand how the costs can add up. Apps and online games provide great social interaction and entertainment but additional costs can be incurred even after you have already paid for the game.

For example, while playing the online game or using the app, your child may be given the option to pay again for extra content such as bonus game levels or points.

To help control the costs of online games and apps:

- * Turn off 'in-app' purchases in the settings of your phone and other devices so your child has to ask to buy additional levels/characters/lands.
- * Keep passwords to yourself so others can't purchase apps and add-ons without you knowing.
- * Talk to your child about costs. Explain that games, apps and the extra features in them all cost real money. Watch your child play a game or app and explain which parts cost extra.
- * Set a reasonable weekly or monthly spend for apps or games and help your child track their spending so they can make good choices. For older kids talk about data costs as well.
- * Check what your child is doing. Are the games and apps appropriate? Online games have ratings and some apps and games have inappropriate ads with links to adult websites, contain offensive material or replicate gambling games. Check out the multimedia reviews on the iParent section of the eSafety website. The eSafety website also has tips on how to protect your children from inappropriate content, including pornography, self-harm sites and violent videos and games.

Watch <u>#GameOn</u>, a video that follows the online experiences of a group of lower secondary students who find themselves in situations that catch them off-guard and teach them the consequences of making poor decisions.

8. Managing sexting

Sexting is the sending of provocative or sexual photos, images, messages or videos using a mobile phone, via email or posting online. Young people often consider sexting as a way of connecting in a relationship.

Support your child's safe online experience by considering the following:

- * Think about the legal ramifications. If anyone in the photo (naked or semi-naked) is under 18 they may be committing a crime. Viewing it or sending it to others may also be a crime.
- * Report it. If the image/video is online, you may then contact the webmaster and ask them to remove it.
- * Seek help. Ask the school to help track who might have the image and where it might be posted. Ask them to provide support to your child and others involved as the negative impacts of sexting can affect grades and behaviour.
- * Be reasonable about consequences. Sexting is not uncommon behaviour and your child is not alone in being negatively impacted. Rather than adding to the distress, implement clear consequences for your child instead. For example, by limiting phone and internet use.
- * Friends are critical. Help them stay connected to friends online and offline for support. Other trusted adults can also check your child's wellbeing and help them manage peer reactions.

Some other <u>strategies</u> can be found on the eSafety website. If your child is distressed about something that's happened to them online, seek professional help. Call the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890.

Watch this <u>video</u> about Jarrod's experience of seeing someone badly affected by the sending of naked images.

9. Being a helpful bystander against cyberbullying

Bullying used to be something you could see or hear: face-to-face physical and verbal behaviour in the playground, classroom and on the way to and from school. Now, online technology and constant connectivity means children can be bullied through often anonymous contact or actions, anytime, anywhere, and often out of sight of adult eyes.

Cyberbullying commonly occurs through:

- * comments posted in an open online environment, for example on social media sites, and
- * direct text, email or instant messages online or on a mobile phone.
- * private features on a social networking services such as Snapchat and Facebook Messenger.

Friends and family can play an important role in helping reduce the spread and impact of cyberbullying because perpetrators may back down when they see that their target has support. Here are some simple steps you can encourage your child to take if they see or know that a friend is being cyberbullied.

- * Don't forward messages or pictures. Though they may not have started it, they will become a part of the cyberbullying cycle.
- * Stand up and speak out against cyberbullying. If your child is confident, encourage them to tell the perpetrator that their comments or actions are hurtful and that they should stop. Watch this "Chatterbox" video (Episode 9) about cyberbullying.
- * Talk to someone they trust like parents or a teacher.
- * **Support your child's friend** by reporting the cyberbullying. Most websites have <u>online safety centres</u> and reporting facilities, and online abuse is in violation of the Terms Of Use of most social networking sites.

The Office of the eSafety Commission can take <u>complaints</u> and provide assistance in relation to serious cyberbullying material that is directed at a particular child with the intention to seriously embarrass, harass, threaten or humiliate.

If your child or someone you care about has been affected by cyberbullying, visit <u>esafety.gov.au</u> or contact the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890.

10. Protecting your child against online identity theft

As your child grows up they develop responsibility to access services such as a library membership, bank accounts and a mobile phone. This includes managing the use of PINS and passwords to ensure that personal information is safe and only revealed to appropriate people and organisations.

Identity theft is when your child's personal information is used without their knowledge or permission. Personal information can be accessed from their online accounts and with sufficient information, criminals can transfer money directly from bank accounts or impersonate your child online on social networking sites.

Your child can reduce the chance of identity theft by:

- * Using secure websites for shopping and online banking. Look for the padlock symbol, a URL that begins with 'https' and correct spelling and logos.
- * Monitoring their content. If their profile has been hacked, shut it down immediately. Some sites also allow you to set up notifications when your account is logged in from an unregistered device.
- * Changing their passwords regularly. Passwords should never be shared, should be changed frequently and be a mix of letters, numbers and symbols.
- * **Not getting phished.** Ensure your child doesn't respond to calls or emails from 'banks' asking for pin numbers and passwords. If they are concerned it is not the real bank, hang up and call back their publicly listed number. If an email from a bank/credit card asks you to click on a link chances are, it's a scam.
- * **Reporting it.** If your child thinks that they have had their personal details stolen or used without their knowledge, they should talk to their bank or other related institution.

If you, your child or someone you know wants to know more about identity theft, visit <u>esafety.gov.au</u> or contact the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890.

11. Trolling online – what it is and how to support your child

<u>Trolling</u> is when a user intentionally causes distress, anger and argument in an online public forum for the purpose of disturbing other users.

Individuals who partake in trolling seek an emotional response from others, whether with malicious or humorous intent. Responding to trolling comments can result in the activity escalating.

Your children may experience trolling on social networking sites, online gaming, chat rooms or blogs. Watch the "Chatterbox" episode about trolling, tagging and bagging.

Children can protect themselves by taking the following action:

- * Ignoring the troll—responding to nasty, immature and offensive comments only gives trolls the attention they want.
- * Blocking the troll—taking away their power. If they pop up under a different name block or mute them again.
- * **Reporting trolls**—reporting to site administrators. If they pop up under a different name, report them to site administrators again. If you feel your safety is being threatened, contact the police for further advice. You may consider not using the site until the issue is resolved or the troll has become bored.
- * Talking with friends and family—if a troll has upset your child, it helps to talk about it with friends and family. You or your child can visit <u>esafety.gov.au</u> or call to the Kids Helpline on 1800 55 1800 or eheadspace on 1800 650 890.
- * Protecting friends from trolls—if trolls are upsetting your child's friend tell them to Ignore, Block, Report. Tell their family and other friends and encourage them to seek support.

Learn more about <u>trolls and online hate</u> on the eSafety website.

12. Avoiding online spam, scams and phishing

If it seems too good to be true, it probably is!

The online world provides you and your child with incredible access to communications and information. However, there are also a number of things that you must be aware of to avoid being taken advantage of.

- * <u>Scams</u> are ways of obtaining information or money through false means.
- * **Spam** is an unsolicited commercial electronic message.
- * **Phishing** is the use of email or SMS to encourage individuals to reveal financial details like credit card numbers, account names and passwords or other personal information. Phishing messages can look like genuine messages from a real bank, telecommunications provider, online retailer or credit card company.

Discuss these actions with your child to avoid this illegal activity.

- * Avoid giving out <u>personal information</u> like your email address or mobile phone number publicly. Check the terms and conditions of anything you sign up for. You may be consenting to receive commercial messages.
- * Do not accept friend requests or respond to text messages from people you don't know.
- * **Remember** that <u>banking institutions</u> will never contact customers by email seeking specific account details. Call your bank directly if you have any concerns about a contact claiming to be your bank.
- * Ensure that you only disclose financial information on websites that you trust and that have secure payment facilities. Look for a URL that begins with 'https' and padlock symbols once you get to the payment page to check it is likely to be secure.

If your child has been affected by spam, scams or phishing, they can report scams here, as well as visiting the esafety website.

13. Safe use of location-based services

Portable communication and entertainment technology has evolved with many devices now connected to the internet and using new features to deliver customised content and functionality.

Some smartphones, cameras, tablets and other small devices have a built-in feature called a geolocator that can pinpoint your exact location. This data is often published online through social networking sites, or used by location-based services such as maps, public transport apps, retail services and so on. It can also be embedded in images you take with your smartphone camera.

You can support your child's safe use of location-based services by:

- * Making sure that their location is only visible to friends they know in the real world. Check that the social networking site doesn't also show their details to those nearby who they might not know.
- * Checking their privacy settings so that if they do share location information, it's only going to the people they want to see it. If they are in doubt, they shouldn't check in.
- * Customising their location-based services so that only particular applications can access location information.
- * <u>Switching off</u> location-based services and <u>GPS</u> when they are not using them. Most devices and applications allow you to switch location information on and off as needed.
- * Encouraging them to contact the police if they feel like they are in physical danger or are unsafe.

If you, your child or someone you know wants to know more about location-based services, visit <u>esafety.gov.au.</u>