Australian Government

Australian Institute of Family Studies

Office of the A/Director
Telephone +61 3 9214 7821

8 January 2015

Ms Christine McDonald
Secretary
Standing Committee on Environment and Communications
Legislative Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

ec.sen@aph.gov.au

Dear Ms McDonald

**Inquiry into the Enhancing Online Safety for Children Bill 2014 and the
Enhancing Online Safety for Children (Consequential Amendments) Bill 2014**

Thank you for your communication on 9 December 2014 inviting the Institute to provide
a submission in relation to the above topic.

Although the Institute has not recently conducted any emperical research on the topic,
we have compiled a summary of relevant research and information relevant to
practitioners and policy makers working with children and their families.

Attached for the attention of the Committee is the Institute's fact sheet on Online Safety
(updated January 2015) - https://www3.aifs.gov.au/cfca/publications/online-safety.

If you require anything further, please do not hesitate to contact the writer.

Yours sincerely,

Dr. Daryl Higgins
Acting Director

Enc.

Online safety

CFCA Fact Sheet— January 2015

Join the conversation

Get the conversation started!

- See all comments
- Add a comment

The purpose of this paper is to provide information about online safety and relevant resources available for parents.

For additional information specifically focused on cyberbullying, see *Parental Involvement in Preventing and Responding to Cyberbullying*.

What is online safety, and why is it important?

Young people are increasingly exposed to an open and collaborative online culture, which allows them to access information, maintain friendships and relationships with family, and engage in creative content production (Collin, Rahilly, Richardson, & Third, 2011). Young people, however, are at a dynamic stage of development in which risk-taking behaviours and emerging decision-making capacities can lead to negative outcomes (Viner, 2005).

An awareness of how to ensure safe practices online is an important skill for young people. While parental involvement in safe use of technology should start from a child's first use, parents continue to be a critical influence in ensuring that teenagers practice responsible digital citizenship and engage in online activities safely.

"Online safety" is used interchangeably with terms such as "Internet safety", "cybersafety", "Internet security", "online security" and "cyber security". The risk of using computers, mobile phones and other electronic devices to access the Internet or other social media is that breaches of privacy may lead to fraud, identity theft and unauthorised access to personal information. Other risks for children include cyberbullying, stalking, or exposure to illicit materials. Criminal offenders have proven to be highly skilled at exploiting new modes of communication to gain access to children, and children can easily access adults-only materials if there are no protective mechanisms in place (Australian Communications and Media Authority, n.d.; Queensland Police, 2014)

These situations can place a young person's emotional wellbeing, and in extreme cases physical wellbeing, at risk. This is particularly so where little or no attention has been paid to monitoring use, communicating with teenagers about use, or the security of the device being used. In these types of cases, and for the purpose of this paper, online safety is a child protection issue.

While online safety is important for protecting children from dangerous and inappropriate websites and materials, this does not mean that parents should discourage their children from accessing the Internet. The challenge is to help children enjoy the benefits of going online while avoiding the risks (Raising Children Network, 2011).

Government regulatory practices in Australia

The Australian Communications and Media Authority (ACMA) works with consumers and other stakeholders in the communications industry to achieve active self-regulation and co-regulation. Together, they act to ensure compliance with license conditions, codes and standards, and the collection of both federal and state laws that apply to Internet content in Australia (ACMA, n.d.).[1]

The principle of "co-regulation" reflects parliament's intention that government, industry and the community all play a role in managing Internet safety issues in Australia. ACMA also monitors the effect of regulations to ensure they are responsive to the community's needs (ACMA, n.d.; Communications Alliance, 2014).

Media campaigns related to online safety

A number of education and awareness campaigns promoting online safety target both children and parents, yet evidence to show the effectiveness of these campaigns remains limited (Connolly, Maurushat, Vaile, & van Dijk, 2011). Similarly, while there is evidence that cyberbullying and cybersafety programs increase young people's awareness, there is limited evidence to show that they lead to behavior changes (Mishna, Cook, Saini, Wu, & McFadden, 2010).

What is known is that campaigns are most effective when they integrate information with training and skill acquisition. Websites, leaflets and other information-only resources may have a limited impact when delivered in isolation. Information provided through interactive training programs, online quizzes, video games and formal curriculum assessment are more likely to translate to more secure conduct online (Connolly et al., 2011). For this reason, parents are encouraged to facilitate their children's engagement with age-appropriate interactive learning materials related to online safety.

The following is a snapshot of campaigns that provide targeted and interactive online learning opportunities for children and parents.

BackMeUp - Australian Human Rights Commission (link is external)
> BackMeUp is an anti-bullying campaign that showcases videos created by young Australians taking a stand against cyberbullying.

Bravehearts online (link is external)
> Internet safety resources focus on online risks; information for young people; information for parents and carers; Internet safety contacts and further links and resources.

Budd:e - Stay smart online (link is external)
> Budd:e is an award-winning cyber-security education package with fun and challenging interactive games that help Australian students stay safe and secure online. The package includes self-learning modules for primary and secondary students that can be accessed at home, as well as resources for teachers and parents.

Cybersafety help button download page (link is external)
> The Help Button provides Internet users, particularly young people, with a "one stop shop" for cybersafety information and assistance. Once downloaded, the button sits on the desktop or in the toolbar. When double clicked, the button allows users to talk, report or learn about cybersafety issues such as cyberbullying, scams and fraud, and unwanted contact.

CyberSmart - ACMA (link is external)
> Cybersmart provides activities, resources and practical advice to help young kids (link is external), kids (link is external) and teens (link is external) safely enjoy the online world. The links contain audio-visual materials, tips and links plus additional resources for school teachers (link is external) and Indigenous communities (link is external) . A catalogue of useful library resources (link is external) is also provided.

Make cyberspace a better place - KIDS Helpline (link is external)

Kids Helpline campaigns to help children enjoy the freedom and fun of using the Internet and to help make cyberspace a fun and safe place.

Tagged (CyberSmart) - ACMA (link is external)

Developed by the ACMA's Cybersmart program, Tagged has received acclaim for its realistic depiction of teenagers and the problems they can face in a digital world. Since its launch in September 2011, Tagged has become a popular resource for Australian teachers and parents. More than 10,000 copies of the film and posters have been distributed nationwide and it has attracted nearly 50,000 views on YouTube.

The Allanah & Madeline Foundation – eSmart Programs (link is external)

These cybersafety resources are targeted at children in the home and at school. eSmart Schools (link is external) is an evidence-based educational program designed specifically for the management of cybersafety in schools. The Foundation is also in the process of developing eSmart Homes (link is external), a guide for parents and carers to ensuring child safety.

Some campaigns are delivered in collaboration with a wide variety of public and private agencies. As a result, there is a large degree of crossover in the material of various contributors presented across the websites. Furthermore, initiatives may target a specific issue (such as cyberbullying), or they may be delivered as part of a broader social awareness campaign (child protection). For additional resources about online safety, see "Further Resources" below.

Practical tips for parents to help children and young people use the Internet

The following tips will help parents provide support and guidance for children and young people as they increasingly engage in online activities.

Monitoring and supervision

Monitoring a young person's online activities includes checking that websites are appropriate for a child's use and keeping an eye on the screen.

If parents are willing to provide children and young people with access to mobile phones and computers, then a responsibility to understand, model appropriate behaviour, and communicate the basics of good digital citizenship should come with the access.

Advice on monitoring often focuses on keeping the computer in a shared family area, yet in the age of wireless connections and Internet-enabled smartphones, this is increasingly difficult. Similarly, young people may control their own online details, such as passwords and web browser histories. Ways in which these difficulties can be addressed include:

- Developing a plan about Internet use in partnership with family members. This can include:
    - details of appropriate online topics;
    - privacy setting checks;
    - physical locations for Internet use, and parental monitoring ("looking over the shoulder" or "line of sight" supervision);
    - limits on screen time;
    - limits on when wireless Internet connections and/or mobile devices will be available; and
    - what may be identified as "inappropriate posts" on online profiles.
- An "Internet use agreement" may be useful to develop with older children.
- Taking an active role in discussing the benefits of online activities with children and young people, and what strategies they may use to respond to cyberbullying, other negative online behaviours, or if they unintentionally access adult content. Discussions can include how these

rules may apply wherever they are online, including at home in their bedroom and when they are outside the home, for example, at a friend's place.

Protection

Parents can be encouraged to:

* Find out whether their child's school has an Internet policy and how online safety is maintained. Inquiries should focus on the strategies used to educate children and young people about online safety and cyberbullying, whether parents are involved in cyberbullying initiatives and if they are involved in developing cyberbullying policies.
* Point out to children that some websites on the Internet are for grown-ups only and are not intended for children to see. Discuss what strategies a teenager might adopt if he/she accesses this content.
* Use a family-friendly Internet service provider (ISP) that provides proven online safety protocols. Filtering tools should not be solely relied on as a solution, however - open discussion and communication with young people about monitoring and supervision is needed.
* Empower children to use the Internet safely by mutually exploring safe sites and explaining why they are safe. It's also important to educate children on why it's not safe to give out any personal details online.

Engagement and communication

Parents can be encouraged to:

* Discuss with children how they may recognise the difference between online information that is helpful or unhelpful, true or false, useful or not useful. For example, government or education websites may contain more accurate information than opinions that are posted on an unfamiliar person's blog.
* Increase their own knowledge and become more adept at engaging in online activities and exploring social networking sites that are being used by their children. Learning alongside children and young people can be an effective way to achieve this - parents can be encouraged to let their children be the "experts" and help them understand the tools they are using online.
* Focus on the positive aspects of the Internet - spend time looking together at sites that are fun, interesting or educational. Find sites together than are age- and stage-appropriate for children.
* Encourage your child to question things on the Internet. When looking at a new site, your child could ask questions such as, "Who is in charge of this site?", "Have I found information, or is it just opinion?" or "Is this site trying to influence me or sell me something?".

Report

If you have found any material online that you believe is prohibited or inappropriate, you should contact the ACMA. For further information, go to ACMA's website (link is external), where a range of resources are available for parents and caregivers.

Sources: ACMA, n.d.; O'Keeffe, Clarke-Pearson, & Council on Communications and Media, 2011; Raising Children Network, 2011; Robinson, 2012.

The significance of 13 years old

As part of their privacy policies, social networking sites such as Facebook, Twitter and YouTube specify that users must be at least 13 years old, a requirement of which parents may often be unaware.

The minimum age stipulations are based on the requirements of the US Congress as set out in the *Children's Online Privacy Protection Act.*[2] The Act specifies that website operators must gain verifiable parental consent from parents prior to collecting any personal information from a child younger than 13 years old (O'Keeffe et al., 2011). As such, many social networking sites avoid this requirement by setting a minimum age of use at 13 years old - but there is no onus on website operators to *verify* the age of users.

Further resources

Online safety information is easily accessible through any search engine, and numerous sites are devoted specifically to this issue. This section identifies several Australian websites about online safety that can be useful for parents and caregivers.

Communications Alliance - Guide for Internet users (link is external)
> This guide assists Australian Internet users to understand Australia's co-regulatory framework for online content, pursuant to the requirements of legislation. The Communications Alliance is a non-profit, private sector industry body that, among other things, develops best practice rules for the industry in Australia in conjunction with ACMA.

Cybersafety information for parents (link is external) - Queensland Government Department of Education, Training and Employment
> This website offers a range of information and resources about cybersafety for teachers and parents. Included is *Cybersafety and cyberbullying: A guide for parents and caregivers*, a resource targeted at responding to inappropriate online behaviour.

Cybersafety help and advice – Australian Government Department of Communications (link is external)
> The Department of Communications provides a hub of information about cybersafety in a simple format, with information about where and how to report risky online behaviour, and how to stay safe online. The site also provides an easy guide to socialising online (link is external).

CyberSmart Parents - ACMA (link is external)
> This resource is designed to assist parents to help their children enjoy safe and positive experiences online. It provides information on how children and young people use the Internet, contains various strategies to manage risks and describes the issues children face in the online world.

Images of Children and Young People Online (NCPC Resource Sheet)
> This Resource Sheet contains information about legal issues, privacy laws, emerging issues, classifications of online images, good practices, lodging a complaint about a website and links to additional resources.

Online Safety and Security – Australian Government Department of Communications (link is external)
> The Australian Government provides a collection of links to initiatives and resources focused on protecting Australian Internet users.

Parental Involvement in Preventing and Responding to Cyberbullying (CFCA Paper)
> This paper from the Child Family Community Australia information exchange outlines definitions and statistics related to cyberbullying. It explores the differences between cyberbullying and offline bullying, and parents' roles and involvement in preventing and responding to cyberbullying incidents. The aim is to inform practitioners and professionals of ways to help parents clarify their roles, and provide them with the tools to help their teenaged children engage in responsible online behaviour.

Raising Children Network - Safety tips for parents of toddlers to teens (ages 4-15) (link is external)

The Raising Children Network website displays tabs for each phase of a child's development, from newborns to early teenagers. Internet safety tips and a comprehensive range of resources are provided to cater for each specific age group, with the exception of newborns and toddlers.

schoolatoz - NSW Department of Education & Communities (link is external)

Practical help for parents about cybersafety and keeping kids safe online are provided in the schoolatoz website. It includes ten cybersafety tips every parent should know (link is external), and information from experts about cybersafety. Useful information is also provided for parents of children who are bullied.

Schools and Cybersafety - Victorian Department of Education and Early Childhood Development (link is external)

Providing advice for schools on cybersafety and the responsible use of digital technologies. The website covers a range of topics including bullying, cybersafety strategies and practical steps and actions relating to online incidents.

Stay Smart Online (link is external)

This is a one-stop shop providing information for Australian Internet users on the simple steps they can take to protect their personal and financial information online. The site has informative videos, quizzes and a free Alert Service that provides information on the latest threats and vulnerabilities.

ThinkUKnow - Internet Safety Program (link is external)

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers. Created by the UK Child Exploitation and Online Protection (CEOP) Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia. Users will need to subscribe to the site to gain access to its tools and resources.

Who's chatting to your kids? - Queensland Police Resource (link is external)

A brochure published by the Queensland Police Service's Task Force Argos. This brochure provides information to parents on Internet safety for children and young people. It discusses social networking, mobile phones, webcams and online gaming, and provides information about the types of things to look out for that may indicate that children could be at risk.

Some of the more popular social networking sites provide information specifically tailored to help parents understand their child's use of the site. For example:

- Facebook: *Help your teens stay safe* (link is external)
- YouTube: *Parent resources* (link is external)

References

- Australian Communications and Media Authority. (no date). *Internet content complaints (link is external)*. Retrieved from <www.acma.gov.au/Citizen/Take-action/Complaints/Internet-content-complaints>.
- Collin, P., Rahilly, K., Richardson, I., & Third, A. (2011). *The benefits of social networking services: A literature review*. Melbourne: Cooperative Research Centre for Young People, Technology and Wellbeing.
- Connolly, C., Maurushat, A., Vaile, D., & van Dijk, P. (2011). *An overview of international cyber-security awareness raising and educational initiatives*. Research report commissioned by the Australian Communications and Media Authority. Melbourne: Commonwealth of Australia/ACMA.
- Communications Alliance. (2014). *Guides for Internet Users*. Retrieved from <http://www.commsalliance.com.au/Activities/ispi/guide_for_consumers>
- Mishna, F.,Cook, C., Saini, M., Wu, M., & MacFadden, R. (2010). Interventions to prevent and reduce cyber abuse of youth: A systematic review. *Research in Social Work Practice*. doi: 10.1177/1049731509351988.

- Mishna, F., Saini, M., & Solomon, S. (2009). Ongoing and online: Children and youth's perception of cyberbullying. *Children and Youth Services Review, 31*, 1222-1228.
- O'Keeffe, Clarke-Pearson, & Council on Communications and Media. (2011). Clinical report: The impact of social media on children, adolescents and families. *Pediatrics, 127*(4), 800-804.
- Queensland Police. *Who's chatting to your kids?* (link is external) (2014) Retrieved from <www.police.qld.gov.au/programs/cscp/personalSafety/children/childProtection/>
- Raising Children Network. (2011). *Internet safety for children (link is external)*. Retrieved from <raisingchildren.net.au/articles/internet_safety.html>
- Robinson, E. (2012). *Parental involvement in preventing and responding to cyberbullying* (CFCA Paper No. 4). Retrieved from <www.aifs.gov.au/cfca/pubs/papers/a141868/index.html>.
- Viner, R. (Ed.). (2005). *The ABC of adolescence*. Malden, Mass.: BMJ Books/Blackwell Publishing.

1 For access to codes relating to Internet use, see "Initiatives and codes" (link is external) on the Communications Alliance website

2 Further information: *How to comply with Children's Online Privacy Protection Act* (link is external).

Acknowledgements

Publication details

Publication meta

We'd appreciate if you share with us how useful you found this paper and how you might use the information (such as forwarding it to a colleague, using it to inform training/policy/practice, or including information in a newsletter/bulletin).