Joint Select Committee on Cyber-Safety
Inquiry into Cyber-Safety

Introduction

We welcome the opportunity to make a submission to the Joint Select Committee on Cyber-Safety. In the following sections, we address the topics identified as the initial focus of inquiry in which we have expertise. A list of recommendations is also included.

Introduction to the Murdoch Childrens Research Institute

Murdoch Childrens Research Institute (MCRI) is Australia's largest child health research organisation. As the research partner of the Royal Children's Hospital, our team has a unique bench to bedside approach, enabling us to more quickly translate research discoveries into practical treatments for child health. Our team of 1200 researchers is focussed on conditions such as mental health problems, allergies, diabetes and premature birth that are increasingly affecting Australian children, and conditions such as cancer and genetic disorders that remain unsolved. www.mcri.edu.au

Introduction to the Centre for Adolescent Health

The Centre for Adolescent Health is Australia's leader in responding to the health problems that affect young people between the ages of 10 and 24 years. We are part of the Royal Children's Hospital, closely linked to The Murdoch Childrens Research Institute and Department of Paediatrics at The University of Melbourne.

The vision of the Centre for Adolescent Health is ***'making the difference to young people's health'*** through our core business of ***'advancing adolescent health knowledge, practice and policy'***.

The Centre for Adolescent Health has integrated its work across 3 clusters;

1. **Adolescent Health Services**
   Specialist and multidisciplinary primary health and other clinical services and peer support programs that deliver high quality health care services to young people in various settings including hospital, community based settings and in detention.
2. **Learning, Innovation and Community Practice**
   Workforce development and working collaboratively with communities to build the capacity of professionals, organisations and communities to enhance the wellbeing of young people.
3. **Research**
   The focus of much of the Centre's research is into health risk behaviours and factors which protect young people from harm. Most of the Centre for Adolescent research is undertaken within the Healthy Development theme of the MCRI at the Royal Children's Hospital

Response to topics identified as the initial focus of the inquiry

1. The online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles)

Young people are using technology in all aspects of their lives and access the online environment in many ways. Many are using the online environment safely. The Australian Communications and Media Authority (AMCA, 2007) reported that Australian children spend an average of one hour and 17 minutes per day using the internet, or 9 hours per week. Each day Australian children spend an average of:

- 49 minutes on internet activities such as emailing, visiting social web sites and messaging
- 15 minutes playing online games
- 13 minutes doing homework on the computer and/or internet.

Trying to block young people's access to the online environment through particular physical points of access is unlikely to be effective – there will always be another physical point of access to use. Hence, comprehensive approaches are required to minimise cyber-safety threats. These include educating students and parents about appropriate behaviour online, and regular communication between adults and young people about their experiences with technology.

2. Abuse of children online, particularly cyber-bullying

Cyber-bullying is defined as "Any type of harassment or bullying (teasing, telling lies, making fun of someone, making rude or mean comments, spreading rumours, or making threatening or aggressive comments)" (Hertz & David-Ferdon, 2008) that occurs through information technology such as email, a chat room, instant messaging, a web site, or text messaging. Cyber bullying differs from "traditional" bullying because it confers the perpetrator anonymity, bullying can continue 24 hours a day, 7 days per week so is therefore more difficult to escape, and can occur in highly public domains. Although the research is not yet available to show it, the way in which cyber-bullying occurs and the severity or frequency may greatly impact on the impact on the victim(s). For example, some of the more public cases that have resulted in teenage suicide have followed very public cyber bullying.

There is widespread community concern about the relatively recent phenomena of cyber-bullying. There have been many stories in the media of the impact of cyber-bullying on young people. This has created a sense in the community that cyber-bullying is very common. However, research to date shows that the rates of cyber-bullying are lower than "traditional" forms of bullying. For example, in the Australian Covert Bullying Study, reported rates of cyber-bullying are 7-10% for students in Year 4 to 9 over the school term (Cross et al., 2009). Hemphill et al. (2010) have also shown that the rates of cyber bullying are lower than those of traditional bullying (cite conference paper). To date, research is limited by the use of inconsistent definitions of cyber bullying and the lack of longitudinal data on the factors that influence cyber bullying.

A common obstacle to young people reporting (cyber) bullying is that they are not confident that telling an adult will help the situation, fear that it may worsen, and also fear that their access to the internet will be restricted or removed. It is therefore crucial that adults in young people's lives and all of us know what to do when (cyber) bullying is reported to stop the bullying occurring.

The current available advice regarding the prevention of cyber bullying is to use current bullying prevention programs (see Point 8 below).

3. Inappropriate social and health behaviours in an online environment (e.g., technology addiction, online promotion of eating disorders, drug usage, underage drinking, smoking and gambling)

As in any environment that young people enter, there is a risk that they will engage in risk-taking behaviours. There is still much debate about the existence of "internet addiction" and currently no official psychological or psychiatric diagnostic category for internet addiction (McGrath, 2009). Nevertheless, the phenonmen of compulsive use of the internet has attracted considerable interest particularly in China and Korea. There have been some high profile cases of 3-15 days of continuous play of massively multiplayer online role-playing games (MMORPGs) leading to cardiolumonary-related deaths. Yee (2006a& 2006b) surveyed 30,000 MMORPG players and found that up to 50% of these players reported themselves to be addicted, and that most of these individuals were under 30 years. In addition, 70% of the MMORPG players interviewed had played continuously for over 10 hours. Anecdotal evidence from Dr Reid's work with young people on cybersafety in schools suggests that young people often describe the internet as addictive, and many report giving up sleep or other important tasks to be on the internet. Whilst further research is important to understand the rate and nature of compulsive or extensive internet use, equally as important is the development of an array of responses and strategies to the problem to be implemented by parents, educators, clinicians.

Another area of concern regarding young people's internet use is unwanted exposure to pornography. Extensive population based research in the US has found that 1 in 4 children under the age of 12 years have inadvertently been exposed to pornography on the internet(Mitchell, Wolak, & Finkelhor, 2007). This exposure most often comes in the form of pop-up windows illegally entered into children's gaming sites. Such exposure necessarily has enormous consequences for the development of young people's concept of normal and health sexuality and expectations of their own physical development (i.e. the penises and breasts displayed in typical pornography are often considerably larger than the norm and often medically altered). In addition, this exposure also contributes to the sexualisation of children which is unacceptable. As children's exposure to pornography may be difficult to avert given the insidious nature of its insertion into sites where children frequent, addressing this exposure in sexual education in schools is critical. Further, ensuring that parents are participants in children's online activities is critical given most sexual education occurs at home, and giving parents ways of educating and managing these scenarios is important.

From a government perspective, rather than introducing a filter, continuous random checks of websites children frequent may be more useful in identifying threats. Further, as the internet is global rather than national, working internationally to create internationally binding laws around child pornography and infiltration of websites frequently visited by children is critical.

4. Identity theft

Young people may be unaware of the possible consequences of revealing personal information and placing photos online. In educating young people about appropriate

use of the online environment, it is also important for them to be made aware of the risks of providing personal information. It is also important for parents to have this information available to them.

5. Breaches of privacy

Anectodal evidence from Dr Reid's work with children suggests that one form of cyberbullying is to "guess" a friend's password to their different social networking accounts. Children and adults often use the one password for many accounts, and in particular, pets are often the password – for the unsuspecting, guessing is easy. Once inside a person's social networking account an array of inappropriate behaviours occur – such as posting bullying things about others, posting embarrassing photos or stories. It needs to be incumbent upon those who provide social networking and other password protected internet services to require a secure password – i.e. a combination of letters, numbers, capital letters, and no real words.

6. Australian and international responses to these cyber-safety threats

There is a growing consensus that using only filtering software and related techniques to reduce cyber-safety threats is not effective. A range of responses is required. These include educating students and parents about appropriate behaviour online, and regular communication between adults and young people about their experiences with technology.

7. Opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with these cyber-safety issues

Given the accessibility of the online environment world-wide, it is crucial that all stakeholders (Australian and international) work together to address cyber-safety issues. The nature of threats to cyber-safety demands that stakeholders from a range of disciplines are involved in finding solutions, including parents, educators, law enforcement, information and communication technology, and young people themselves. Australia needs to work at an international level and band with other governments to demand better solutions from those who provide internet services. Without an international consensus those who provide internet services are able to ignore national laws and regulations.

8. Ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying

Given that threats to cyber-safety and particularly cyber-bullying can occur anywhere, any time of day, schools are an important context in which to provide young people with interpersonal and technological skills. **However, schools are not the only important context to address cyber-bullying. Parents, families, carers and the broader community all play vital roles (see below).** The extent to which schools play a role in reducing cyber-bullying remains a hot topic for debate. However, where there is a spill-over of issues at school into cyber-space there may be an argument for schools taking action. Regardless, schools can play an important role in teaching students valuable social, interpersonal and conflict resolution skills to aim to prevent all forms of bullying including cyber-bullying.

Given that cyber-bullying is a fairly new issue, there is limited research available on the key factors that lead to cyber-bullying. There are a range of evidence-based bullying prevention programs available to schools (e.g., Friendly Schools, Friendly Families, Olweus Bullying Prevention Program). Current advice from research leaders in the bullying field is to continue to use these programs to adopt a universal approach to prevention. These include important principles such as:

- Taking a whole-school approach
- Planning for and creating a caring, respectful, inclusive and supportive school culture
- Use evidence-based programs
- Use a risk management approach that includes setting up secure reporting systems for students to report bullying to teachers
- Focus on skill development for students (including bystander skills), teachers, and leadership teams.
- Regularly, monitor, evaluate and review practices and policies

(McGrath, 2005 *Making Australian schools safer*).

In relation to school policies, educators need to review their current bullying prevention policies and identify whether they need to be modified to explicitly refer to cyber bullying. This can include having a plan for what to do if an incident occurs. Encouraging schools and regions to work collaboratively on developing school policies is important.

Young people are highly skilled in using technology. Educators and parents can talk with young people to generate ideas about how technology could be used to prevent cyber bullying.

9. The role of parents, families, carers and the community

Threats to cyber-safety are present in all aspects of a young person's life. Hence, all contexts in which a young person lives play important roles in maximising cyber-safety; parents, families, carers and the community.

Parents play a particularly important role. Students may not want to tell parents about (cyber) bullying for a number of reasons; they think they are telling tales by reporting (cyber) bullying, they think that they should be able to deal with their own problems (a sense of failure), and they think if they tell an adult the (cyber) bullying will get worse. An additional reason for young people not telling parents about cyber bullying is that they fear access to the online environment will be taken away from them. Additional reasons

- It is important for parents to talk with their children about who they interact with and where they go on the internet (monitoring of young people's activities whether it is a physical place or cyber space).
- Parents can develop rules with their children regarding safe and acceptable behaviour online and what children can do if they are a victim or bystander.
- Once parents have talked with their children about where they go on the internet, parents can explore these sites to find out more about them.
- Parents can talk with other parents about how they talk with the children about the online environment, the rules they use, and how they keep in touch with their child's use of the online environment.
- Parents can encourage their local school or cluster of schools to educate parents about cyber bullying and the online environment.

- Because technology is constantly changing, it is important that parents continue to talk with their children and other parents to keep up with the rapid developments.

Final thoughts

Two highly relevant quotes from the United State Centers for Disease Control brief for parents.

> Educators, teens, and caregivers are far ahead of researchers in identifying trends in electronic aggression and bringing attention to potential causes and solutions (Hertz & David-Ferdon, 2008, p. 17).

And finally …

> We send our children out into the world every day to explore and learn, and we hope that they will approach a trusted adult if they encounter a challenge; now, we need to apply this message to the virtual world (Hertz & David-Ferdon, 2008, p. 17).

Recommendations

1. To support quality research to better understand the threats to cyber-safety for children and young people including studies of the prevalence of these threats and research on the factors that over time influence the development of cyber bullying and related behaviours, and the impact of cyber-bullying on mental health and other outcomes.

2. As research into online and connected behaviours and threats becomes outdated very quickly due to the pace of developments in technology it is critical that the government not delay in developing and research a a range of potential ways to prevent and adequately respond to cyber-bullying and threats to cyber-safety.

3. To encourage community-wide responses to maximising cyber-safety that includes schools, parents, families, carers, and community members working together.

4. To provide children and young people with interpersonal skills and an understanding of etiquette in online environments to minimise threats to cyber-safety.

5. To ensure that young people know about the risks associated with revealing personal information and photos in the online environment.

6. Bullying prevention programs and policies be developed in schools that target all forms of bullying (e.g., physical, verbal, cyber, etc.).

7. Ensure that any revisions to the National Safe Schools Framework require schools to include in their anti-bullying policies specific reference to cyber-bullying.

8. Encourage schools to engage with parents and community members to share information, educate others, and develop co-ordinated plans for reducing threats to cyber-safety.

9. To encourage young people, parents, and other community members to talk about the threats on the online environment and how to overcome these.

10. To explore ways of using the online environment and technology to promote positive development and to overcome the threats to cyber-safety.

References

Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L., & Thomas, L. 2009. *Australian Covert Bullying Prevalence Study (ACBPS)*. Child Health Promotion Research Centre, Edith Cowan University, Perth.

Hemphill, S.A., Kotevski, A., Smith, R., Tollit, M., Herrenkohl, T.I., Toumbourou, J.T., & Catalano, R.F. (2010). *Longitudinal predictors of cyberbullying perpetration and victimisation in Victorian secondary school students*. Workshop presented at the National Centre Against Bullying 2010 conference entitled "Navigating the maze: Cybersafety and wellbeing solutions for schools. Melbourne, Australia.

Hertz, MF, & David-Ferdon, C. (2008). Electronic media and youth violence: A CDC issue brief for educators and caregivers. Atlanta (GA): Centers for Disease Control.

McGrath, H. (2005) Making Australian schools safer: A Summary Report of the Outcomes from the National Safe Schools Framework Best Practice Grants Programme (2004-2005). Canberra: Australian Government Department of Education, Science and Training.

McGrath, H. (2009). *Young people and technology: A review of the current literature* (2nd edition). Melbourne, Australia: The Alannah and Madeline Foundation

Mitchell, K.J., Wolak, J., Finkelhor, D. (2007). Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the internet. *Journal of Adolescent Health, 40(2),* pp 116-126.

Yee, N. (2006a) *The Demographics, Motivations and Derived Experiences of Users of Massively Multi-User OnlineGraphical Environments*. Presence: Teleoperators and Virtual Environments 2006:3 vol 15 s. 309-329.
Yee, N. (2006b) *Motivations for Play in Online Games*. Cyberpsychology and Behavior 2006:6 s. 772-775.