The Australian Psychological Society Ltd

Submission to the
Joint Select Committee on Cyber-Safety

July 2010

APS contact:

Dr. Susie Burke

s.burke@psychology.org.au

This submission was prepared for the Australian Psychological Society by
Ms. Emma Sampson, Dr. Susie Burke, and Ms. Heather Gridley
with expert advice from Dr Helen McGrath and Dr Michael Carr-Gregg

ABN 23 000 543 788
The Australian Psychological Society Ltd, Level 11, 257 Collins Street, Melbourne VIC 3000
Phone +61 3 8662 3300; Fax +61 3 9663 6177; Email: contactus@psychology.org.au; Web www.psychology.org.au

Acknowledgments

This submission has been prepared by Ms. Emma Sampson, Dr. Susie Burke, and Ms. Heather Gridley.

Dr Susie Burke is Senior Psychologist, Public Interest at the Australian Psychological Society. Psychology in the Public Interest is a unit of the APS dedicated to the communication and application of psychological knowledge to enhance community wellbeing and promote social justice. The public interest team undertakes and encourages strategic research and produces position statements, submissions, tip sheets and media releases on a range of social issues.

Ms Emma Sampson has a background in community psychology and is currently employed as a research assistant, in the area of Psychology in the Public Interest at the *Australian Psychological Society*. Emma has experience working within the community sector, for a community-based organisation in the outer northern suburbs of Melbourne, and more recently in the evaluation of community based programs.

Ms Heather Gridley, FAPS, is a community psychologist and Manager, Public Interest, at the Australian Psychological Society**.**

Expert advice was generously provided by Dr Michael Carr-Gregg and Dr Helen Mc Grath.

Dr Michael Carr-Gregg is an adolescent psychologist in private practice, founding member of the National Centre Against Bullying, and Ambassador for the National Depression Initiative beyondblue. Michael was previously Associate Professor in the Department of Paediatrics at the University of Melbourne, and is a regular columnist for Girlfriend, Australian Doctor and commentator on Radio 3AW.

Dr Helen McGrath is Adjunct Professor RMIT University, School of Education and Senior Lecturer, Deakin University. She is a Counselling Psychologist in Private Practice, a Member of the National Centre Against Bullying, consultant to the Alannah and Madeline Foundation and Senior developer of the eSmart Project.

APS Submission to the Joint Select Committee on Cyber-Safety

Summary of Recommendations

- Recommendation 1

It is recommended that ongoing research into prevention and cyber-safety strategies be developed, with a particular focus on cyber risks and strategies for different age groups. This should include a rigorous evaluation of what works in terms of prevention, treatment and policy.

- Recommendation 2

It is recommended that cyber risks and cyber-safety be framed as part of child and youth development; that is, as part of the development of respectful relationships and building positive relationships skills among young people.

- Recommendation 3

Cyber-safety strategies therefore should not be seen as separate to (or more or less important) than addressing other forms of bullying and discrimination (such as racism, homophobia or sexual violence).

- Recommendation 4

It is recommended that strategies to reduce cyber-bullying involve supporting the development of young people as competent cyber-citizens, promoting cyber-literacy, the ability to critique information, and socially responsible behaviour in the use of digital technology.

- Recommendation 5

The notion of cyber-safety should include the concept of inclusiveness, so that support is provided for those who are marginalised from online technologies, to access them equitably.

- Recommendation 6

An engagement strategy to involve young people in the definition of cyber-threats and in designing, implementing and evaluating cyber-safety initiatives should be developed to ensure children and young people are part of key decision making processes.

- Recommendation 7

In the light of young people being aware of emerging technologies (keeping pace with changes), and of their potential roles in witnessing and intervening in cyber-safety threats (such as cyber-bullying) among their peers, peer education and intervention programs should be developed and adequately resourced as a key part of any cyber-safety initiative.

- Recommendation 8

Strategies for protecting children from online threats should be part of a broader parenting approach, for example, that involves taking responsibility for overseeing their children's

behaviours and learning non-aggressive alternatives for dealing with conflict, such as good conflict resolution skills.

- Recommendation 9

It is recommended that parents are educated and supported to use an internet filter (without relying solely on this strategy), to discuss and use the internet with children and encourage them to critically evaluate information accessed online, to monitor and supervise their child's internet/phone use, and to involve young people in deciding appropriate limits and agreeing on age appropriate consequences.

- Recommendation 10

It is recommended that schools are encouraged and supported to adopt a whole-school approach to cyber-safety that balances the use of online technologies for creativity and learning in a safe way.

- Recommendation 11

Cyber-bullying should be an integral part of broader student wellbeing and discrimination policies, and not seen as separate to these concerns.

- Recommendation 12

Teachers should be provided with regular training and support about how to appropriately understand and respond to cyber-risks.

- Recommendation 13

Schools should take an active role in disseminating information to parents and children, enabling parents to use the information to raise their own awareness of online risks as well as potential threats posed by their children's computer use (e.g., of social networking sites).

- Recommendation 14

It is recommended that government undertake widespread education for parents, teachers and young people around cyber risks and safety strategies, as well as adequately resource and support schools to implement cyber-safety strategies identified above.

- Recommendation 15

Industry should develop (and regularly update) appropriate Internet safety software that effectively filters inappropriate material from access by children, while still affording young people the opportunity to access information that forms part of broader creativity and learning.

- Recommendation 16

Government should provide an information or referral service which assists parents and schools to navigate best practice technology, such as internet filtering systems.

1. Introduction

The Australian Psychological Society (APS) welcomes the opportunity to make a submission to the Joint Select Committee on Cyber-safety. The online environment and associated technologies have enabled unique opportunities for learning, connection, and communication and now play a particularly central role in the lives of children and young people. While it appears that much access to the internet is positive and beneficial, there are concerns regarding the potential for harm, especially in relation to children and young people. Given that children are still in the process of developing the ability to assess risk and manage the consequences of decisions, they are particularly vulnerable to the risks of cyber threats. Inappropriate use could also have detrimental impacts on the healthy development of children including cognitive functioning, physical and mental health, sexuality, and attitudes and beliefs.

The APS is well placed to contribute to this Inquiry by identifying psychological research and best practice as it relates to cyber-safety among children and young people. The APS has developed a series of literature reviews, discussion papers and position statements which have informed this submission. These include position papers on racism and prejudice and on media representations and responsibilities, tip sheets on helping girls develop a positive self image and on talking with children about violence and injustice, and a parent guide to helping children manage conflict, aggression, and bullying.

This submission focuses on cyber-safety from a psychological perspective. It responds to the terms of reference by providing an overview of the online environment, identifying specific risks associated with cyber-safety threats, and discussing ways to encourage safe online access. Specific vulnerable groups with complex needs who are particularly affected by online technologies are also identified, and young people, parents and schools are the focus of a series of recommendations that is provided.

In addition to this submission, the APS recommends attention to the work of the Allanah and Madeline Foundation, and specifically refers the inquiry to a literature review on *Young people and technology* conducted by Dr. Helen McGrath in 2009.

2. About the Australian Psychological Society

The APS is the premier professional association for psychologists in Australia, representing over 19,000 members. Psychology is a discipline that systematically addresses the many facets of human experience and functioning at individual, family and societal levels. Psychology covers many highly specialised areas, but all psychologists share foundational training in human development and the constructs of healthy functioning.

Psychologists have been substantially involved in collaborative, multi-disciplinary work on social issues internationally and nationally for decades. They bring their psychological skills and knowledge to enhance understandings of the psychological and systemic issues that contribute to social problems, and to find better ways of addressing such problems.

The APS supports nine professional Colleges that represent specialist areas of psychology: Clinical, Community, Counselling, Educational & Developmental, Forensic, Health, Organisational and Sport Psychology, and Clinical Neuropsychology. A range of Interest Groups within the APS also reflect the Society's commitment to investigating the concerns of, and promoting equity for, vulnerable groups such as Indigenous Australians, gay and lesbian people, minority cultures, older people, children, adolescents and families. The promotion of a peaceful and just society and protecting the natural environment are the focus of other APS Interest Groups.

Psychology in the Public Interest is the section of the APS dedicated to the application and communication of psychological knowledge to enhance community wellbeing and promote equitable and just treatment of all segments of society.

3. Responding to the Terms of Reference

The APS is not in a position to respond to all of the terms of reference, but has identified and responded to the terms where psychological knowledge and best practice are most relevant.

3.1 The online environment – the good, the bad and the ugly

Terms of Reference (a) i. The online environment in which Australian children currently engage, including key physical points of access, and stakeholders controlling or able to influence that engagement.

The internet has revolutionised the way we communicate, and now plays a central role in the lives of children. Children are likely to be exposed to online technology from a very young age and increasingly have immediate and ongoing access to online environments. While there are considerable benefits to this access to technology for education, connection, communication and even safety, there are growing concerns around ensuring safe access for children and developing appropriate limits and supports around this access.

Online technologies are growing and expanding rapidly, and each form poses both potentials and risks for children and young people. These technologies include mobile phones, email, internet/websites, instant messaging, chat rooms, blogs, online forums, social networking sites, video sharing sites and virtual reality sites.

Most children and young people use online technologies on a daily basis. The Australian Communications and Media Authority (ACMA) (2009) has found that Australian children aged 8 to 9 years use the internet for an average of 1 hour, 6 minutes every two days, while young people aged 16 to 17 years average 3 hours, 30 minutes on the internet every day.

While children and young people may not necessarily use online technology more than adults, their use differs from that of adults. Younger children are more interested in individual activities online, such as playing games (ACMA, 2009), while young people aged 12-17 use the internet mainly for social interaction via use of social networks or communities such as Windows LiveSpace, YouTube, Facebook and MySpace (IPSOS, 2008). Such online technologies enable young people to stay connected to their existing (real world) peers and are important to their social wellbeing. A small proportion of young people use online social networking to build networks of new friends (ACMA, 2009).

There is a relatively limited understanding about marginalised young people's use of online technologies and there is growing concern that disparities in ICT access, quality, and skills (digital divide) will reinforce existing disparities in health and social outcomes (Vichealth, 2005). Although more recent research highlights that young people who experience marginalisation *do* access and engage with ICT, the quality of the access available to them is often limited (Blanchard, Metcalf, Degney, Herrman & Burns, 2008). For some disadvantaged groups however, the internet has enabled freedom of expression and engagement where face-to-face contact is difficult, which highlights the potential for online technologies to create new processes of social inclusion, encouraging freedom from discrimination and violence and facilitating access to economic resources (Vichealth, 2005).

Knowing how to use the internet safely is key to a positive online experience and to ensuring the benefits of the internet are realised and children are protected from harm. While most recent research has found that children and young people have a high level of awareness of cyber-safety risks and of key messages about staying safe online, it is also acknowledged that "children and young people have limited experience in assessing risk and predicting and weighing up the potential consequences of their behavioural choices" (McGrath, 2009: 2). Children and young people who are already isolated and marginalised are particularly vulnerable here.

Children and young people access the online environment in a range of ways including at physical points such as at home, school, library or cafes, and increasingly have ongoing access with the development of new technologies (e.g., internet access via mobile phones, broadband). While key stakeholders such as peers, teachers, parents, government and industry have an important role in influencing young people's use of online technologies, this role needs to go beyond monitoring and supervision as young people's access becomes increasingly *mobile* (as discussed below).

3.2 Cyber-safety threats

Terms of Reference (a) ii. the nature, prevalence, implications of, and level of risk associated with, cyber-safety threats, such as:

- *abuse of children online (cyber-bullying, cyber-stalking and sexual grooming);*
- *exposure to illegal and inappropriate content;*
- *inappropriate social and health behaviours in an online environment;*
- *identity theft; and*
- *breaches of privacy*

While there are clearly risks posed by the online environment, especially for children and young people, these risks have often been over-exaggerated, with the media portraying 'worst case scenarios'. Similarly, often it is 'technology' that has been blamed for 'behaviour that is rooted in wider social problems and in the psychological issues that characterise adolescence' (Shariff & Gouin, cited in Cross et al, 2009: 39).

The risks to children and young people can be grouped in the following ways;

- content risks (harm from the actual content of the material that children can access or be exposed to),
- confidentiality risks (such as invasion of privacy)

- contact risks (harm that arises from other people making inappropriate or hurtful contact via the internet or following on from internet contact).

The following is a discussion of the nature, prevalence and implication of these three risks. There are also concerns about the opportunity costs that children experience when internet technology dominates their lives at the expense of other types of activity and interest, but these concerns are beyond the scope of the current inquiry.

3.2.1 Content risks

Most experts agree that despite their ability to effectively use online technologies, children still need protection from content that exploits their immaturity and could harm their development (Biggins & Handsley, 2000). Content that is inappropriate for children includes material that is highly sexualized, pornographic, violent, consumption-promoting, or perpetuating of negative stereotypes.

Viewing highly sexualized images of women, or violent material for example, has many risks for children's psychological development and mental health, by potentially skewing their views of normality and right and wrong at a time when both girls' and boys' brains are still developing (which continues into their 20s). Below is a discussion of the content considered to constitute a risk for children and young people to access.

Pornography

Access to pornographic material on the internet is a serious concern for children. Mental health professionals have expressed growing concern about the impact of exposure to pornography on the child's developing sense of sexual identity (Benedek & Brown, 1999; Wartella, 2000; Zillman, 2000), and there is increasing concern about the link between exposure of children to pornography and sexual abuse of children. Exposure to pornography can impact on children's sexual identity by promoting unrealistic self-objectification. This is addressed further below, drawing on a comprehensive report by the American Psychological Association (APA, 2007).

Sexualisation of children

The sexualisation of children is another harm that comes via online technology (but of course is not limited to online media). Sexualization occurs when (among other things), a person's only ascribed value comes from his or her sexual appeal and behaviour, to the exclusion of other characteristics, a person is sexually objectified, and rather than being seen as a person with the capacity for independent action and decision making, is made into

a thing for others' sexual use; and/or sexuality is inappropriately and prematurely imposed upon a person such as a child. (APA, 2007).

All forms of media provide examples of sexualized images of girls and women. Research shows that women more often than men are portrayed in a sexual manner (e.g., dressed in revealing clothing, with bodily postures or facial expressions that imply sexual readiness) and are objectified (e.g., used as a decorative object, or as body parts rather than a whole person). These images are ubiquitous in all forms of online media.

Sexualization has been shown to have negative effects in a variety of domains, including cognitive functioning, physical and mental health, sexuality, and attitudes and beliefs. For example, cognitively, self-objectification has been repeatedly shown to detract from the ability to concentrate and focus one's attention, thus leading to impaired performance on mental activities such as mathematical computations or logical reasoning, research links sexualization with three of the most common mental health problems of girls and women: eating disorders, low self-esteem, and depression or depressed mood, self-objectification has been linked directly with diminished sexual health among adolescent girls (e.g., as measured by decreased condom use and diminished sexual assertiveness) and girls and young women who more frequently consume or engage with mainstream media content offer stronger endorsement of sexual stereotypes that depict women as sexual objects (APA, 2007).

Violence

There is a vast literature on the harm that is done to young people through their exposure to violent media, confirming that content does matter. The online environment provides ample opportunities for young people to access violent content, such as video games and websites, and can act as a vehicle for enacting and encouraging violence. For example the Cronulla riots were organised online via the internet and via SMS, and racist comments that perpetrate negative stereotypes have been recorded on social networking sites such as Facebook.

The evidence strongly suggests that exposure to violent video games is a causal risk factor for increased aggressive behaviour, aggressive cognition, and aggressive affect, and for decreased empathy and prosocial behaviour.

Consumerism, advertising and online gambling

Children and young people are also at risk of being contacted by unscrupulous salespeople who try to sell them expensive and possibly disadvantageous mobile or internet plans, via emails offering them speak deals, free memberships or gambling opportunities (McGrath, 2009), as well as by advertisements that may mislead them into purchasing or agreeing to certain activities (eg; buying products online). Children can be particularly vulnerable to marketing offers they 'sign up' to that result in a torrent of spam, or ongoing charges for downloads they can't control.

Advertising has the potential for a range of effects on children, including increasing their product awareness, their positive attitudes towards a product, their inclination or actual buying behaviour, and their tendency to request purchases from parents, as well as arousing cues for children, cravings, thought preoccupations, and increasing the perceived value of certain products as rewards in families. It is manipulative of children who are too young to discern its intent. Young children are particularly vulnerable to being deceived and exploited by advertising because they lack the cognitive skills to defend themselves against persuasive advertisements.

In Australia as elsewhere, the past 10 years has seen a burgeoning of more sophisticated ways to gamble, including access to 24-hour gambling through the internet, mobile phone technology and interactive television platforms. Internet access poses unique problems for national regulation and regulation of access via minors. Internet and wireless-based gambling is increasing, and greatly increases accessibility (Australian Gaming Council, 2008). There is evidence that younger people are significantly more likely to participate in most forms of gambling (except lotteries and bingo) than older people. Under-aged gambling is particularly common: around 60% of young people (13-17 years) report gambling at least once per year (Lambos, Delfabbro, & Pulgies, 2007). Internet gambling in the form of gambling on interactive gambling sites (e.g., online casinos) is not legal in Australia under the 2001 Interactive Gambling Act 2001, but use of the internet as a vehicle to place bets on approved forms of gambling, such as sporting events and wagering, is allowed (Australian Gaming Council, 2008/09).

3.2.2 Confidentiality risks

Another contact risk is that to privacy and confidentiality. Many ways of interacting with the online environment expose people to a wider public than is possible offline. Young people often post personal and identifying details without thinking of the consequences. For example, ACMA (2009) found that seventy-eight per cent of young people claimed to have

personal information, such as a photograph of themselves, on their social networking profile pages. If children are chatting to people online whom they know (or think they know) and trust while in the safety of their own home, they will often let down their guard or try new things. Children and young people can also post or send material that can then be very easily and widely circulated, beyond their control. Private images and information can be sent to other people, which can be potentially embarrassing or harmful to the person or their families. Once this material has been circulated and made available on the internet, it can be very difficult, if not impossible, to remove. For example, young people may use their phone to take sexual photos of themselves (with no enticement from another to do so) and transmit it to others via mobile phone or internet, unaware of the risk they are putting themselves in by undertaking such activities (McGrath, 2009).

Part of adolescence is individuality and self-expression, and the online environment offers young people an opportunity to express their individuality by posting personal information and images. ACMA (2009) found that 'the option of protecting their privacy online often falls by the wayside in favour of wanting to stand out to others online' (p.8).

3.2.3 Contact risks

The third form of risk from the online environment comes from contact with others, either from people known to the user, or from strangers. At worst, users can be a target for predators and paedophiles who make contact with children and young people via the internet. Children and young people may also be contacted by people they do not know through social networking sites. For example, ACMA (2009) found that sixty-one per cent of young people surveyed reported accepting 'friend requests' from people they do not know offline.

While the threat to children and young people of sexual predators is real and serious, the incidence of this type of contact as a proportion of sex crimes committed against young people is low (McGrath, 2009), and messages aimed at children around awareness of this type of contact/threat have widely been effective in alerting them to this particular danger (ACMA, 2009). It appears that "many teenagers frequently interact safely online with people they don't know as part of the development of their identity" (McGrath, 2009: 34).

Cyber-bullying is one contact risk that has been consistently identified as a risky behaviour with serious consequences for children and young people, as discussed in more depth below.

Cyber-bullying

Cyber-bullying can be seen as a mutation of the bullying that has long pre-dated the internet, albeit with some different features (McGrath, 2009). Willard (2006) defines cyber-bullying as "being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies" (cited in McGrath, 2009: 24). It may involve repeated threats, attacks, humiliations or insults, or there may be attacks using different media/methods. "Cyber-bullying can be carried out in many different and sophisticated ways that remove the schoolyard parameters from traditional bullying and expand the problem to the borderless cyberworld" (McGrath, 2009: 21).

Cyber-bullying can take place via all methods of online communication, and can take a variety of forms including (but not limited to) harassment and threatening messages, denigration (sending nasty SMS, including homophobic, sexist or racist comments), masquerading, impersonation, outing and trickery (sharing private personal information, messages, pictures with others), social exclusion (intentionally excluding others from an online group and sexting (sharing explicit material by mobile phone).

Cyber-bullying differs from traditional bullying in a number of ways, including giving the illusion of anonymity, occuring 24/7 and thus being harder to escape; it often involves no authority (adults are are less aware of cyber-bullying as it is nearly always carried out secretly) and can amplify the impact of 'regular' bullying. McGrath (2009) has summarised the similarities between offline and online bullying, which include being destructive human relationships involving power and social control, most offline bullying actions have a cyber-bullying counterpart and victimised young people experience the same feelings of powerlessness and humiliation from being bullied on and offline.

There is a lack of research into the prevalence of cyber-bullying as it is a relatively new phenomenon, has various definitions, has applied to different age groups and has not always been recognised as different in some ways to offline bullying (McGrath, 2009). As a result, data suggests that anywhere between 4% and 42% of all young people are likely to have experienced cyber-bullying (McGrath, 2009), with research pointing to the experience of cyber-bullying increasing with age. For example, ACMA (2009) found that cyber-bullying was experienced by just one per cent of 8 to 9 year olds, but 19% of 16 to 17 year olds surveyed. Similarly, Cross et al (2009) found that between 7-10% of students were cyberbullied each term, and with a spike in bullying when children move from primary to secondary school.

There are risk factors within the individual, within their family, within the school, within the community and within the peer group. For example, there is an increase in the likelihood of young people being bullied offline if they have experienced cyber-bullying, and an increase in bullying related to increased access to online technologies, such as mobile phone or wireless internet (McGrath, 2009). While there are mixed findings regarding student disclosure of bullying to their parents, research does highlight the increased incidence of bullying in those schools that are taking less action to stop it (Cross et al, 2009).

Risk factors associated with students who cyber-bully are summarised by Cross et al, 2009 and include include having access to mobile phone, having no internet use rules at home, having a history of bullying others face to face, having been cyber- and face-to-face bullied themselves, being more lonely and less connected to school, and attending a less supportive school (Cross et al, 2009).

Bullying has many negative impacts on the victim, including: impaired social and emotional adjustment; poor academic achievement, anxiety, depression and suicidality; poorer physical health; higher absenteeism; and increased loneliness and low self esteem (Cross, 2009). Emerging evidence suggests that bullying (potentially cyber-bullying) is implicated in the suicide of young people (Gough, 2007).

Those who bully others are also negatively impacted by their bullying behaviour. The effects of bullying others include: anxiety, depression and suicidality; greater risk of delinquent behaviour; increased alcohol and substance use (Cross, 2009).

Marginalised young people and cyber-bullying

Young people are not a homogenous group, and some researchers and practitioners have highlighted the particular vulnerability faced by young people who already face life difficulties and/or are marginalised. For example, Willard (2007) points to young people who are ‘at risk’ in other areas of their life, such as facing ongoing challenges related to personal mental health, sexuality, school and/or peers, as being more vulnerable to being victims of cyber-bullying.

Children and young people with disabilities and who are lesbian, gay, or trans-gender, or who are perceived to be so may be at particularly high risk of being bullied by their peers (APA, 2004). Hillier, Turner and Mitchell (2005, cited in Youth Affairs Council of Victoria, 2009: 20) have pointed out differences in homophobic bullying to other forms of bullying,

such as homophobic bullying being more difficult to challenge than other forms of bullying, due to teacher fear of a backlash from parents or community if they challenge homophobia, or may be afraid of being labelled as homosexuals themselves, the difficulty for same-sex-attracted young people to access support if they are experiencing bullying due to the need to disclose their sexual preference and the alienation that same-sex-attracted young people experience is often more extreme (for example after disclosing their sexuality they may be alienated at home or lose the support of their parents).

Similarly, young people with a disability have also been identified as particularly vulnerable. The Youth Affairs Council of Victoria (2009: 26) cites research by Taleporos (2009) highlighting that:

- statistics from the UK indicate that approximately 80% of students with an intellectual disability are bullied.
- bullying accounts for 20-30% of the cases that come to Youth Disability Advocacy Service for individual advocacy work, and
- cyber-bullying of people with a disability often happens under the guise of humour, making it harder to detect.

3.3 Cyber-safety: Ensuring safe online access

Terms of Reference (a) iii Australian and international responses to current cyber-safety threats (education, filtering, regulation, enforcement) their effectiveness and costs to stakeholders including business.

Terms of Reference (a) iv Opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cyber-safety issues

Terms of Reference (a) v Examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised

Terms of Reference (a) vi Ways to support schools to change their culture to reduce the incidence and harmful effects of cyber-bullying

Terms of Reference (a) vii Analysing information on achieving and continuing world's best practice safeguards

Cyber-safety strategies aim to give children, their parents/carers and teachers safe and responsible ways of using and accessing the internet, ICT and mobile phones, ensuring online risks are managed and online experiences are safe and positive (ACMA, 2007). Strategies need to include all aspects of the online environment, including the online industry (regulation, enforcement, filtering), schools (policies, education, management), families, and

young people. The broader context within which the internet is used (e.g., family context, broader society) also needs to be considered as part of any cyber-safety strategy.

Many of the strategies to address cyber threats however, centre around the support, education and limits provided to children, and are not specific to the internet, as they apply to how children are supported, protected and assisted to thrive in all aspects of their lives. They apply to the internet as one mechanism that children use to communicate, relate, get information and socialise.

3.3.1 Industry and technology

Technology needs to be part of the solution, although care must be taken not to rely solely on technological solutions such as internet filters, as technologies emerge more rapidly than these filters can keep up with. For example, there is no filtering facility for mobile phones to prevent unacceptable material from being delivered – now or in the foreseeable future. There is a role for the government in collaboration with the community to develop the criteria needed for appropriate filtering technologies that minimize risk to children while maintaining freedom of speech/use and not creating an illusion of safety. These technologies should be developed by industry and be freely accessible to schools and parents, and be easy to implement. Mobile phone manufacturers and ISPs need to be engaged to be part of the solution, by making controls available and taking down offensive information promptly.

More specifically in terms of company websites that are aimed at children, ACMA (2009) found that visibly displayed safety information is taken notice of more than an optional link, with effective safety messages displaying safety rules at the start of website access, advice and restrictions about using personal details (such as their name), providing warnings never to share passwords, and requiring parental permission upon signing up to a website if the child is under 13.

3.3.2 Legal solutions

While beyond the scope of this submission, the APS acknowledges the considerations raised by McGrath (2009) regarding legal issues around cyber-safety, which include:

- The balance between freedom of speech, the right to privacy and cyber-safety
- The potential for criminal charges and/or civil claims against users
- Discrimination and racial vilification
- Legislation controlling the behaviour of ISPs; and

- The responsibility and rights of schools in responding to a cyber attack or cyber-bullying that occurs outside school hours and off the school premises.

In addition, while legal implications should not be the sole driver of cyber-safety measures targeted to children and young people, important components of cyber-safety include informing them about their 'digital footprint', including the likelihood that their activities are often very traceable, and facilitating them to take responsibility for the consequences of their actions, including that they may be held liable for inappropriate activity.

3.3.3 Schools

Schools have a very important role to play in ensuring responsible and safe use of technology. The challenge for schools is embracing new technologies as positive tools for teaching, learning and building relationships whilst at the same time identifying and addressing the safety risks attached to their use (McGrath, 2009).

It is essential that schools provide students with the assistance and education to enable them to use online technologies for responsible and creative learning. Ensuring schools have an *acceptable use* internet (cyber-safety) policy that every single member of the school community needs to sign off on is important, and there need to be clearly articulated rules and regulations with consequences for breaches of those rules. Working in collaboration with parents and students to develop such a policy, making cyber-safety an integral part of student wellbeing practices in schools, and including cyber-safety as part of the curriculum will better ensure the policy's relevance.

Most schools currently have bullying policies and many have specific cyber-bullying policies. Unfortunately, these are often not backed up with clear procedures that are consistently followed by teachers, or widely known and understood by teachers, students and their parents/carers. Regardless, policies alone are not sufficient to address the behaviours and should be accompanied by:

- Monitoring students' online activity and take action against threatening or unsafe online behaviour
- Increasing the skill and confidence of teachers to deal with cyber-safety issues
- Using filters and blocks wihtout depending upon them
- Learning the language and interacting with young people on their turf
- Developing and advertising acceptable-use policies
- Focusing on peak times (e.g., school transition)

- Involving parents, including education about use of internet and internet filtering technology
- consistent use of appropriate techniques for managing peer relationships, such as restorative justice, method of shared concern, and support group approach, with more limited application of punitive approaches (Carr-Gregg, 2010).

Addressing cyber-bullying should be considered part of the school's broader approach to developing respectful relationships between students and addressing bullying and discrimination more generally. Cyber-bullying is a reflection of attitudes and behaviours students manifest in the 'real world', and often accompanies other forms of bullying. Teaching positive relationship strategies, empathy skills, the importance of bystander intervention and conflict resolution skills (anger management, problem solving, decision making) in schools is part of a whole school approach to effectively addressing cyber-safety. Cyber-safety strategies therefore should not be seen as separate to (or more/less important) than addressing other forms of bullying and discrimination (such as racism, homophobia or sexual violence).

Teacher education and awareness is key to this whole-school approach. Cross et al (2009) for example found that teachers were less confident in addressing cyber-bullying compared to other forms of bullying, and that "young people reported losing faith in reporting bullying behaviour because some teachers and other adults are not taking action or not recognising covert bullying as bullying when they see it or when it is reported, especially via cyber means". Staff training, positive classroom management, resources and support for development of appropriate strategies, principal commitment, and reconciliation/restorative techniques are all important as part of teacher engagement in cyber-safety. The teaching of values, rights and responsibilities, as well as a commitment from the school leadership team to creating a respectful and caring school culture that is modelled by teachers in their interactions with each other and students, are essential here (Carr-Gregg, 2010).

Some commentators have cautioned against the approach adopted by many schools of preventing access to many online environments (such as social networking sites) in response to worst-case scenarios that exploit parental fears (Sharples et al, 2009). This approach in some situations has prevented teachers from exploring the benefits of the internet for creativity and social learning, and does not encourage young people to take responsibility for making safe decisions about their engagement with online technologies.

Cross et al (2009) conclude that the most promising interventions appear to be those that take a whole-school approach which includes the development of programs aimed at:

- enhancing a positive school climate and ethos which promotes pro-social behaviours
- providing pre-service and in-service training of all school staff to assist them to recognise and respond appropriately to signs of covert bullying
- creating physical environments that limit the invisibility of covert bullying
- increasing the awareness among young people of how group mechanisms work and strengthening their skills in conflict resolution; and
- developing anonymous, peer-led support structures for students to access when they feel uncomfortable.

3.3.4 Young people

Bullying among children almost never happens in isolation, and while cyber-bullying may occur more privately, often other students know about it and thus have the option of intervening (Cross et al, 2009). Spears (2009) for example highlighted "the peer pressure to pass on an image or message that young people experience and the need for young people to develop skills and techniques to respond to bullying on the net or by phone as bystanders or witnesses" (p. 13).

Children and young people therefore need to be part of cyber-safety solutions. Involving young people in discussions about cyber-safety is an important part of their development (e.g., awareness of consequences of actions, taking responsibility for choices, learning to treat others with respect). Also, as research has found that young people aged 12-17 years are most likely to discuss internet issues with their friends (ACMA, 2009), the education and involvement of young people in ensuring a safe online environment is essential.

It is important (and part of how students are educated) for example, that they are involved in and (partially) responsible for the moderation and monitoring of online activities (Sharples et al, 2009). Similarly, involving children in defining bullying, constructing bullying and harassment policies and being part of the delivery of anti-bullying strategies leads to increased ownership and effectiveness of such policies.

Peer education and interventions are important in reducing the impacts of cyber-bullying. The majority of peer interventions have been found to be effective, with the bullying stopping within a short period of time of peer intervention and reconciliation occurring when bystanders intervened (Cross, 2009). Students who are 'defended' are better adjusted, and

report less peer-reported victimisation one year later (Sainio, Veenstra, Huitsing, & Salmivalli, 2009, cited in Cross, 2009).

3.3.5 Parents and families

Some researchers have identified a generation gap between young people and their parents in relation to online technology. While increasingly many parents are using the internet themselves and are actively supervising their children's online activities, there are specific factors that present challenges to their effective oversight of their children's online activities (McGrath, 2009).

There is mixed research around parental awareness of their children's online activities and confidence to provide appropriate support and oversight. For example, ACMA (2009) found that parents feel well informed about their child's internet behaviour, that the majority report conversations about internet safety, including about the use of social networking sites, and that most households have rules regarding the internet and use a number of general internet safety messages. The same research however noted that "parents admitted they did not feel suitably informed about the internet and the associated risks" (p.61).

To some extent, parental concerns regarding their children's use of online technologies does not differ from other areas of parenting or issues faced by families (e.g., resistance to setting limits). On the other hand however, the rapidly changing nature of the technology, such as increased access to the internet in private/away from parental view (e.g., via mobile phone or broadband) and changing content and use (e.g., social networking sites) suggest many parents may be unfamiliar with aspects of online technology, and therefore less confident about their ability to supervise and set appropriate limits for their children. This is magnified in disadvantaged groups, where internet access is not available in the home and parents are less likely to have used and be familiar with features of the internet.

Studies have also found that children are more likely to talk to their parents than to teachers about being bullied, yet many parents of children who are bullied do not always know how best to talk to their children about the issue, and hence require appropriate information and support to deal with the incidence of bullying (Cross et al, 2009). Students have also reported qualitatively they would not tell an adult if they were being or had been cyberbullied for fear of having their computer or mobile phone removed.

Effective parental strategies are technological (e.g., internet security software), involve good communication (explaining why certain material is not appropriate), are not based on fear or

punishment (e.g., removal of internet access as a form of punishment is associated with young people not disclosing future cyber-bullying/threats), involve active engagement in social networking sites (e.g., parents should have their children as 'friends' on social networking sites) and involve setting limits around the use of online technology (e.g., using the internet in sight of parents, charging the phone in lounge area). As Cross et al. (2009) contends *…parents who provide children with good supervision and who set boundaries, while at the same time granting their children a level of psychological autonomy, enhance the development of protective social skills among their children, and strengthen their capacity to find creative rather than reactive solutions when resolving conflicts (p35).*

Many studies have therefore proposed that school-based anti-bullying interventions should have a significant parent and family component to ensure that family members play an active and supportive role in school programs, and promote protective factors against bullying in their children (Cross et al, 2009).

3.3.6 Bridging the digital divide

The increasing number of children and young people engaging in a range of social and creative online activities at home is producing a growing divide between such web-confident children and those who are restricted to using the internet at school (Sharples et al, 2009). This divide is further compounded by the restrictions implemented by many schools which limit the types of internet sites available to students, with the result that students using online technologies less are less likely to know how to respond if they are targeted. There are growing concerns that disparities in ICT access, quality and skills will reinforce existing disparities in health and social outcomes (Blanchard, Metcalf, Degney, Hermann & Burns, 2008). For these reasons, civic engagement programs and health promotion initiatives more broadly must develop effective strategies to address these challenges and build young people's capacity to use and manage ICT (Blanchard et al, 2008). Social inclusion in terms of internet access and participation should be seen as an essential part of addressing cyber-safety.

Further responses to bridging the digital divide could include schools, libraries and other organisations with connections to children providing the resources and supports for disadvantaged parents. For example, organisations could offer free 'Introduction to the Internet' courses, designed specifically for parents who have not yet experienced the internet and are thus severely disadvantaged in their ability to supervise their children's online experiences (Biggins & Handsley, 2000). Similarly providing information, advice and access

to internet filtering technology, particularly for those in disadvantaged communities (e.g., refugees, migrants, single parents), is essential to protecting the most vulnerable children.

4. Recommendations

The following is a series of recommendations based on Australian and international psychological research and best practice. The recommendations are grouped around key sites for change and action.

4.1 Defining and understanding cyber risks, threats and safety

Recommendation 1

Due to the rapidly changing nature of technologies, it is recommended that ongoing research, prevention and cyber-safety strategies be developed, with a particular focus on cyber risks and strategies for different age groups. This should include a rigorous evaluation of what works in terms of prevention, treatment and policy.

Recommendation 2

It is recommended that cyber risks and cyber-safety be framed as part of child and youth development; that is, as part of the development of respectful relationships and building positive relationships skills among young people.

Recommendation 3

Cyber-safety strategies therefore should not be seen as separate to (or more/less important) than addressing other forms of bullying and discrimination (such as racism, homophobia or sexual violence). Cyber risks should be accurately communicated and avoid over-emphasising the risk.

Recommendation 4

It is recommended that strategies to reduce cyber-bullying, involve supporting the development of young people as competent cyber-citizens, promoting cyber literacy and socially responsible behaviour in the use of digital technology (Youth Affairs Council of Victoria, 2009). Importantly this should include the encouragement of critical skills among young people that invites them to question attitudes, values, beliefs and assumptions behind information, and to consider information that uncovers social inequalities and injustices (Spears, 2009).

Recommendation 5

The notion of cyber-safety should include the concept of inclusiveness (addressing digital divides), so that support is provided for those who are marginalised from online technologies to access them equitably. On the other hand, alternative opportunities for entertainment, communication and education should be provided so that online technologies are not the only option for children and young people.

4.2 Young people

Recommendation 6

An engagement strategy to involve young people in the definition of cyber threats (especially cyber-bullying) and in designing, implementing and evaluating cyber-safety initiatives should be developed to ensure children and young people are part of key decision making processes. Governments, industry and schools should be supported to adopt this strategy.

Recommendation 7

In the light of young people being aware of emerging technologies (keeping pace with changes), and of their potential roles in witnessing and intervening in cyber-safety threats (such as cyber-bullying) among their peers, peer education and intervention programs should be developed and adequately resourced as a key part of any cyber-safety initiative.

4.3 For parents and families

Recommendation 8

Strategies for protecting children from online threats (such as breaches in confidentiality or cyber-bullying) should be part of a broader parenting approach that involves taking responsibility for overseeing their children's behaviours and setting appropriate limits. As part of such an approach, parents would assist their children to find engaging alternatives to online activities, learn how to manage their feelings, behave in appropriate ways and learn non-aggressive alternatives for dealing with conflict, such as good conflict resolution skills.

Recommendation 9

It is recommended that parents are educated and supported to use an internet filter (without relying solely on this strategy), to discuss and use the internet with children and encourage them to evaluate critically information accessed online, to monitor and supervise their child's internet/phone use, and to involve young people in deciding appropriate limits and agreeing on age appropriate consequences.

4.4 Schools, teachers and the education system

Recommendation 10

It is recommended that schools are encouraged and supported to adopt a whole-school approach to cyber-safety that balances the use of online technologies for creativity and learning in a safe way. Such a policy should be developed in collaboration with students, parents and teachers, have the commitment of the principal (leadership of the school) and be agreed upon by every single member of the school community[1].

Recommendation 11

Cyber-bullying should be an integral part of broader student wellbeing and/or discrimination policies, and not seen as separate to these concerns. Issues such as homophobia, racism, discrimination against young people with a disability and the sexualisation of girls should be addressed as part of these policies.

Recommendation 12

Teachers should be provided with regular training and support about how to appropriately understand and respond to cyber risks. This includes the capacity to build in cyber-safety as part of the broader curriculum, encouraging pro-social behaviours as part of general classroom management techniques and more specifically being able to respond to inappropriate internet use.

Recommendation 13

Schools should take an active role in disseminating information to parents and children, enabling parents to use the information to raise their own awareness of online risks as well as potential threats posed by their children's use (e.g., of social networking sites).

4.5 Government and industry

Recommendation 14

It is recommended that government undertake widespread education for parents, teachers and young people around cyber risks and safety strategies, as well as adequately resource and support schools to implement cyber-safety strategies identified above. This initiative should be recognised as part of broader educational efforts to ensure healthy development and positive relationships among children, eliminating discrimination and instilling the ability among young people to critically review information and decisions made in relation to online activities.

[1] The Alannah and Madeline Foundation's eSmart School initiative shows promise as a whole-school approach to cyber-safety.

Recommendation 15

Industry should develop (and regularly update) appropriate Internet safety software that effectively filters inappropriate material from access by children, while still affording young people the opportunity to access information that forms part of broader creativity and learning.

Recommendation 16

Government should provide an information and/or referral service which assists parents and schools to navigate best practice technology, such as internet filtering systems.

5. References

ACMA (2009a). Click and Connect - Young Australians' Use of Online Social Media: 01: Qualitative Research Report. Australian Government

ACMA (2009b). Click and Connect - Young Australians' Use of Online Social Media: 02: Quantitative Research Report. Australian Government

ACMA (2007). Media and Communications in Australian Families 2007: Report of the Media and Society Research project.

American Psychological Association Task Force on the Sexualization of Girls. (2007). *Report of the APA Task Force on the Sexualization of Girls.*Washington, DC: America Retrived 5/7/2010 from www.apa.org/pi/wpo/sexualization.html.

American Psychological Association (2004). *Resolution on Bullying Among Children and Youth (July 2004).* DC: America.

Australian Gaming Council (2008). *Internet and wireless gambling: A current profile*. Melbourne: AGC.

Australian Gaming Council (2008/09). *A database on Australia's gambling industries*. Melbourne: AGC.

Benedek, E., & Brown, C. (1999). No excuses: Televised pornography harms children. *Harvard Review of Psychiatry, 7(4),* 236–240.

Beran & Lupart (2009). The Relationship Between School Achievement and Peer Harassment in Canadian Adolescents: The Importance of Mediating Factors. *School Psychology International; 30:* 75-91.

Biggins, B & Handsley, E. (2000). Censorship in public libraries. Paper presented to ALIA Conference, Canberra, 23 October 2000. viewed 5 July 2006, <http://conferences.alia.org.au/alia2000/proceedings/biggins.handsley.html>.

Blanchard, Metcalf, Degney, Herrman & Burns (2008). Rethinking the Digital Divide: Findings from a study of marginalised young people's ICT use. *Youth Studies Australia, v.27 (4),* pp.35-42.

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.

Cross (2009). *The way we treat each other: Trends and promising recommendations from Australian youth.* Accessed 31/05/10 at http://cyber-bullyingforum.org/?p=363

Gough, D, (2007). Every Fortnight: A Life Lost Just Begun: Special Report: Teen Suicide, *The Age, February 4th, 2007.*

Hillier, L., Turner, A., & Mitchell, A. (2005) *Writing themselves in again: 6 years on. The second national report on the sexuality, health and well-being of same sex attracted young people in Australia.* Australian Centre in Sex, Health & Society, La Trobe University. .Melbourne.

Ipsos Reid. (2008). *Interactive Teens: The Impact of the Internet on Canada's Next Generation. Accessed 31/05/10* www.is-afe.org/imgs/pdf.

Lambos, C., Delfabbro, P.H., & Pulgies, S. (2007). *Adolescent gambling in South Australia*. Report prepared for the Independent Gambling Authority of South Australia. Adelaide.

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

Sanson, A., Augoustinos, M., Gridley, H., Kyrios, M., Reser, J., & Turner, C. (1998). Racism and Prejudice: An Australian Psychological Society Position Paper. *Australian Psychologist 33:* 161-182.

Sharples, M., Graber, R., Harrison, C. & Logan, K. (2009). E-safety and Web 2.0 for children aged 11–16. *Journal of Computer Assisted Learning, 2:,* 70–84.

Willard, N. (2006). *Cyber-bullying and cyberthreats: Effectively managing internet use risks in schools.* Retrieved 31/05/10 at http://www.cyberbully.org/cyberbully/docs/cbctpresentation.pdf

Williams, R.J., West, B.L., & Simpson, R.I. (2007). *Prevention of problem gambling: A comprehensive review of the evidence*. Report prepared for the Ontario Problem Gambling Research Centre, Guelph, Ontario, Canada.

Wolke, Woods, Bloomfield, & Karstadt, (2001).

Wyn, J., Cuervo, H., Woodman, D. & Stokes, H. (2005). Young people, wellbeing and communication technologies. Youth Research Centre, The University of Melbourne. Melbourne, Victoria.

Youth Affairs Council of Victoria (2009). *Sticks and stones and mobile phones: Bullying in the new Millennium. Outcomes from a Forum on Bulling and Young People in Victoria.* Melbourne, Victoria.