SUBMISSION No. 94

Submission to the Commonwealth Joint Select Committee on Cyber-Safety Inquiry into Cyber-Safety for Children and Young People

Table of Contents

1. THE ONLINE ENVIRONMENT IN WHICH AUSTRALIAN CHILDREN CURRENTLY ENGAGE, INCLUDING KEY PHYSICAL POINTS OF ACCESS 2
2. ABUSE AND EXPLOITATION OF CHILDREN ONLINE 7
3. INAPPROPRIATE SOCIAL AND HEALTH BEHAVIOURS IN AN ONLINE ENVIRONMENT 11
4. PRIVACY ISSUES FOR CHILDREN AND YOUNG PEOPLE 14
5. AUSTRALIAN RESPONSES TO CYBER SAFETY THREATS 17
6. WAYS TO SUPPORT SCHOOLS TO CHANGE THEIR CULTURE TO REDUCE THE INCIDENCE AND HARMFUL EFFECTS OF CYBER-BULLYING 22
7. THE ROLE OF PARENTS, FAMILY AND THE COMMUNITY 28

1. THE ONLINE ENVIRONMENT IN WHICH AUSTRALIAN CHILDREN CURRENTLY ENGAGE, INCLUDING KEY PHYSICAL POINTS OF ACCESS

Children and cyberspace

Cyberspace is a world accessed by children through the internet. Children use a range of different media to access cyberspace. They not only use the family's home computer, but also multi-functional devices and technologies including mobile phones, webcams and other hand-held devices.

Cyberspace offers children a way to connect with others, share experiences and voice opinions. However, children are not a homogenous group and the nature of their engagement with cyberspace is fluid. The ways in which they engage depend on each individual child's interests and maturity.

There are risks to safety in the real world that children learn to deal with as part of growing up. The strategies young people employ to deal with general safety issues are transferable to many of the risks in cyberspace.

However, there are particular risks unique to cyberspace that young people can be vulnerable to. These risks stem from potential anonymity on the internet and can be predatory in nature.

In traditional face-to-face communication, people are able to comprehend non-verbal cues which help to identify risks to safety and make decisions. These cues are not necessarily present on the internet which hinders children's ability to manage predatory risks.

Internet Access

Students can use private computers located in their own homes, as well as computers available in libraries, shopping centres and internet cafes, and mobile phones in a range of locations. They can access a range of sites including websites they themselves create.

While the use of technology at school can be the subject of some regulation, use at home and other places outside of school can be unfiltered and unsupervised by adults. Internet providers, parents, other carers and the broader community must play a role in the safe participation of children in the online environment.

Internet Access in Schools

Internet and online communication services in schools are provided by the NSW Department of Education and Training for research and learning and communication between students and staff. Student access to internet and online communication tools at school assists them to develop information and communication skills necessary for effective and appropriate use of the internet. It also provides a context for learning about roles and responsibilities in communication, respectful relationships and personal safety.

Each time a student logs on to the NSW Department of Education and Training's Web Services portal, an acceptable usage statement appears. Before they can access the internet students must accept undertakings about responsible use of electronic communication and to report any inappropriate behaviour to teachers.

The *Online Communication Services: Acceptable Usage for School Students* defines the Department's policy for school students in the appropriate and acceptable use of internet and online communication services provided by the Department. It includes advice on access and security, privacy and confidentiality, intellectual property and copyright, and misuse and breach of acceptable usage. A copy of this policy is available at: https://www.det.nsw.edu.au/policies/general_man/general/accep_use/PD20020046.shtml?level

Impact of the Digital Education Revolution – NSW on student access

Senior students in NSW government schools have access to the *Digital Education Revolution – NSW* wireless network in schools. The laptops are wirelessly enabled and can connect outside of the school grounds in places such as the public library, in the home, internet cafes – anywhere students collaborate, study and learn.

The *Digital Education Revolution – NSW* wireless network provides a secure online environment. The student laptops are subject to a strict internet filtering policy and any site that is not recognised by the filter is blocked, including so-called proxy sites that enable users to by-pass the filter. Any site that is recognised is categorised according to its content, and the Department determines which categories can be accessed.

Digital Education Revolution – NSW is developing a Digital Citizenship education program proposed to be implemented in 2011. Digital Citizenship is a strategy to teach students the knowledge and skills to be good digital citizens.

Following consultation with Digital Education Revolution counterparts in other States, the Commonwealth Department of Broadband, Communications and the Digital Economy, and the Australian Communications and Media Authority, *Digital Education Revolution – NSW* has developed the Digital Citizenship domains upon which to base the Digital Citizenship education program.

Digital Education Revolution – NSW consulted with the NSW Secondary Principals Council Digital Education Revolution Taskforce on 16 February 2010 and then requested the Australian Curriculum, Assessment and Reporting Authority to include Digital Citizenship in the national curriculum.

Strategies that will accompany this initiative and form part of the digital citizenship program are the development of:

- a digital citizenship education program that includes how to use social networking sites constructively and responsibly;
- a professional learning program for teachers that includes social networking;
- an educational strategy for parents.

Internet Access in NSW Public Libraries

Libraries as key physical points of access to the online environment

Public libraries across NSW provide free internet access for the community. They form a critical element in community development, supporting lifelong learning, literacy and education.

NSW public libraries have:

- 368 locations— 99 central library services, 269 branch libraries (and 23 mobile libraries);
- 3.2 million members (47% of population);
- 14,636 opening hours per week;
- 37 million visits in 2008/09;
- 2,344 staff and hundreds of volunteers;
- 624,607 children and young people as members with many more non-members also using library spaces.[1]

The *Library Act 1939* guarantees everyone in the NSW community access to public libraries. All libraries have conditions of use relating to public internet access. Children and young people can access the internet in public libraries.

- Conditions of internet use vary between local authorities. However, it is common for parents or guardians to be required to give permission for their child to use the internet. The Library Council of NSW recommends this practice be applied in all public libraries.[2]
- The State Library provides free access to the Internet. The Library also offers wireless access to the Internet for clients with their own laptops or PDAs. The State Library recognises the privacy of the library user and

[1] NSW Public Library Statistics 2008/09

[2] Library Council of NSW (2008) Access to Information in New South Wales Public Libraries Guideline http://www.sl.nsw.gov.au/services/public%5Flibraries/policies/docs/accesstoinformation2007.pdf

> does not monitor the information or sites accessed by clients. This service is available to young people and children should they choose to apply for a readers' card.

Work in NSW public libraries is not currently classified as "child-related employment" under the existing legislation. Library staff do not provide formal supervision to children and young people in the public library environment. At all times this responsibility remains with the parents and guardians of children and young people.

The Library Council of NSW develops guidelines to provide additional support to public libraries, including the *Children's Policy Guidelines for NSW Public Libraries (2008).*[3]

In regard to using the internet the following guidelines apply:

> Public libraries promote and support public access to information. Library staff should assist clients in the use of electronic resources including the Internet, recommend websites on particular subjects, and select appropriate websites for inclusion in the library's electronic collections. Parents/guardians of young people are solely responsible for the young person's access to and use of the library's Internet facilities, including access to sites, their subject matter and content. Parents/guardians must ensure that their children's use of the Library's Internet facilities accords with the library's Internet policy.
>
> It is recommended that young people's use of the Library's internet facilities should be authorised by parents/guardians. Provision should be made for this authorisation on the library's junior membership forms. The clause should state that the parent/guardian will ensure the child abides by the library's Internet policy.[4]

Internet Access in Hospitals

There are a number of issues facing hospitals in terms of the provision of access to technology by children and young people. For example, parents may provide children in hospitals with laptops and iPhones with wireless access to an external network which would then allow access to inappropriate internet sites. In addition, some parents may request that a hospital allow their child to access their private Internet Service Provider (ISP), which would then allow access to any internet site. However, access to ISPs or general internet sites has been

[3] Library Council of NSW (2008) Children's Policy Guidelines for NSW Public Libraries http://www.sl.nsw.gov.au/services/public%5Flibraries/library_mgt/lib_management_docs/childrens_%20policy_%20guidelines.pdf

[4] Library Council of NSW (2008) Children's Policy Guidelines for NSW Public Libraries http://www.sl.nsw.gov.au/services/public%5Flibraries/library_mgt/lib_management_docs/childrens_%20policy_%20guidelines.pdf p. 8

refused in the past due to past misuse of downloading inappropriate material and sending inappropriate messages to other children in hospital.

NSW Health advises:

- Access to social network sites such as Facebook are blocked at hospitals that care for children and young people (Children's Hospital Westmead, Sydney Children's Hospital);
- Monitored access for children and young people is granted to Livewire.org.au, an online community service for siblings and parents that is strictly controlled and wholly owned by a subsidiary of the Starlight Children's Foundation;
- Access is granted to the Department of Education and Training network to allow continued education while in hospital.

2. ABUSE AND EXPLOITATION OF CHILDREN ONLINE

Cyber-bullying

Cyber-bullying is a relatively new phenomenon which involves the inappropriate use of information and communication technologies. Forms of digital communication used to bully may include e-mail, instant messaging, social networking sites, chat rooms, web sites, blogs, and text messages. Activities can include "flaming" (repeated negative messages), impersonation, denigration, cyber-stalking, and "happy slapping" (filming a set up fight and posting it for others to watch).

There has been widespread debate about whether cyber-bullying should be distinguished from other forms of bullying behaviour or whether it is just bullying behaviour using technology. Cyber-bullying can be considered bullying behaviour using technology as it involves repeated behaviour, which is intended to hurt or humiliate and where there is a power imbalance between the parties. Researchers such as Marilyn Campbell of the Queensland University of Technology note that several characteristics distinguish cyber-bullying from other forms of bullying:

- people who are bullied have no place to hide, and can be targeted anytime and anyplace;
- cyber-bullying can involve a very wide audience;
- people who bully are relatively protected by the anonymity of electronic forms of contact, which can safeguard them from consequences or retaliation;
- people who bully do not usually see the response of the victim, changing the satisfactions or inhibitions normally generated by bullying.

Many incidents of cyber-bullying occur outside of education contexts, although a significant proportion is reportedly done by school peers.[5] In fact, cyber-bullying is reported to be a growing problem for school-aged children. The number of children who report being cyber-bullied is estimated to be approximately a third of those victimised through traditional forms.[6] A survey of 120 grade eight students in Brisbane found that 14% had been bullied, most often by text messages. [7]

Research into cyber-bullying is still in its infancy, but some studies suggest it may be more harmful for children and young people than traditional bullying.

[5] Willard, N.E. (2006), Cyber bullying and cyber threats. Eugene, Oregon: Center for Safe and Responsible Internet Use, is a comprehensive source with a North American slant.

[6] Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2007, in press). Cyber bullying, its forms and impact in secondary school pupils. Journal of Child Psychology and Psychiatry.

[7] Campbell 2005, cited in Bauman, S. (2007), Cyberbullying: a virtual menace. Paper downloaded from www.ncab.org.au. Retrieved 19 January 2009.

This is because harmful messages online can potentially be received by millions of people and because written insults such as text messages can be read repeatedly by the victim whereas verbal insults may be more easily forgotten.[8] Research shows that young people who are cyber-bullied most commonly report feelings of frustration, anger, sadness and distress. [9]

In one 2007 study participants were asked to rate the harm caused by differing cyber-bullying media in comparison to the effects of traditional bullying. Although most forms of cyber-bullying were rated as having a similar impact, picture video clips were perceived to cause much greater harm than traditional bullying[10].

A common theme of research on bullying is that children and young people who are bullied often show a reluctance to seek help. There appears to be a similar trend with cyber-bullying.

In November 2009, the NSW Legislative Council General Purpose Standing Committee (No.2) released a report entitled, *Inquiry into Bullying of Children and Young People*. The report is available online at www.parliament.nsw.gov.au. A number of the recommendations concern the issue of cyber-bullying, namely recommendations 6, 11, 13, 19, 20, 21, and 24.

The NSW Government has responded to those recommendations and is implementing a range of strategies to deal with bullying of children and young people at school. The NSW Government's response to the inquiry's recommendations is also available online at www.parliament.nsw.gov.au The report recognises that bullying is a whole of community issue and commits the Government to work hard to ensure greater coordination and cooperation across all levels of government, school systems, schools, the community and researchers in efforts to address bullying.

Each school within NSW is required to have an anti-bullying policy, and bullying matters are initially dealt with internally by schools. A bullying incident becomes the responsibility of the NSW Police Force if it involves a criminal offence. The NSW Police Force's School Liaison Police and Youth Liaison Officers address cyber bullying issues in high schools and primary schools.

Principals have the power to impose strong sanctions to counter cyber-bullying. The *Student Discipline in Government Schools* Policy makes plain "*the school discipline policy may apply outside of school hours and off school premises where there*

[8] Campbell 2005, cited in Bauman, S. (2007), Cyberbullying: a virtual menace. Paper downloaded from www.ncab.org.au. Retrieved 19 January 2009.

[9] Hinduja, S. & Patchin, J. W. (2007, in press) Cyber bullying: An exploratory analysis of factors related to offending and victimization. Deviant Behaviour.

[10] Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. & Tippett, N. (2007, in press). Cyber bullying, its forms and impact in secondary school pupils. Journal of Child Psychology and Psychiatry.

is a clear and close connection between the school and the conduct of students" and the *Suspension and Expulsion of School Students - Procedures* specifically recognise that behaviour that may warrant suspension includes "hostile behaviour directed towards students, members of staff or other persons including verbal abuse and abuse transmitted electronically such as by email or SMS text message".

The NSW Digital Citizenship education program (see Topic 1) includes cyber-bullying as a cross domain theme in all Years K-10. This theme runs across each domain as relevant and promotes the expectation that all students should be active in preventing cyber-bullying and understand that even one-off hostile cyber actions can have a negative widespread impact due to the rapid dissemination and relative permanency of the message sent. Students should understand the characteristics and forms of cyber-bullying and hostile cyber behaviour and the steps they can take if experiencing or observing these behaviours.

Youth Suicide and cyber bullying

Evidence has shown that both traditional bullying and cyber bullying can lead to depression, decreased self-worth, hopelessness, and loneliness - all of which are precursors to suicide and suicidal behaviour.

Youth suicide continues to be a significant public health concern in NSW despite the suicide rate for young people 15-24 years falling from 15.2 per 100,000 people in 1996/97 to 5.9 per 100,000 in 2008, the lowest in Australia. As these figures are not subdivided according to cause, the impact of cyber bullying on these figures is unclear.

Sexting

'Sexting' is the act of sending intimate images to another person via mobile phone networks. Under Commonwealth legislation there are only criminal implications for the sender and receiver if the image constitutes child pornography. However, distributing images that do not constitute child pornography may nonetheless be a form of abuse or cyber-bullying, if a child is coerced into posing or if the images are distributed without consent.

Peer to Peer chat rooms

Peer to Peer chat rooms can be conducive to cyber bullying and other inappropriate behaviour. School-related incidents, for example, can continue online out of school hours.

NSW Police advise that Peer to Peer chat rooms are also used by sexual predators to groom and procure children. In these cases, the offender uses a false profile to engage in inappropriate conversation with the victim, tempting the victim to send explicit images of themselves, and encouraging the victim to meet with the offender to engage in sexual activity. The NSW Police Force has an investigation unit dedicated to dealing with these crimes.

Peer to Peer chat rooms have enabled Child Exploitation Material (CEM) to be exchanged between paedophiles.

Internet Service Providers can implement filters to blacklist certain web addresses. An effective concept currently being trialled is the Global File Registry (GFR), which utilises details of previously seized CEM. When a user attempts to transmit one of these images via a Peer to Peer network, the image is immediately substituted with a warning of the criminal consequences involved.

Peer to Peer sites could take steps to remove and prevent the transmission of CEM when it is reported to them, and have a 'reporting button' to enable immediate reporting of inappropriate content.

Sexual abuse and cyber-bullying

Although the internet has the potential to expose children to sexual grooming, provide access by "sexual predators" and disseminate child pornography, evidence indicates that children remain at the most risk of sexual abuse from someone that has a close relationship and physical access to the child such as a parent, family member, friend, teacher, and so on.

It is of note, however, that issues of sexual abuse and cyber-bullying overlap, particularly in cases of the sexual assault of young people by other young people. NSW Health Sexual Assault Service staff have reported seeing young people (teenagers in particular) who have experienced sexual assault and where the sexual assault itself, and/or degrading images of the victim during the sexual assault, are recorded via still or video images on a mobile phone and then uploaded to an internet site and/or distributed to peers of the victim via media such as text messages, emails, facebook, etc. Where this occurs, the impact of the sexual assault on the victim commonly involves shame, embarrassment, and fear. Victims report being exposed to ridicule and taunts from peers in connection to the sexual assault.

3. INAPPROPRIATE SOCIAL AND HEALTH BEHAVIOURS IN AN ONLINE ENVIRONMENT

Online availability of alcohol and drugs

Australia has had a coordinated national policy for addressing drug abuse issues since the inception of the National Campaign Against Drug Abuse (NCADA) in 1985.

The current National Drug Strategy is in its final year of implementation. Public consultation on development of the next phase of the Strategy took place in early 2010. The consultation paper included the question: "What are the particular opportunities and challenges that technology development is likely to pose for the community and the alcohol and drug sector over the next five years?"

The results of the consultation have not yet been finalised but, when they are available, could inform this inquiry, in particular where related to monitoring online advertising content and accessibility to alcohol and other drugs via the internet.

Data regarding the purchase of alcohol and other drugs via the internet is not available. While the Australian Secondary Students' Alcohol and Drug Survey asks secondary students where they sourced the last cigarette they smoked and their last alcoholic drink, and includes the internet in a list of alternatives, to date it has not been reported as a common source of either alcohol or tobacco.

Alcohol

The NSW Government considered the issue of underage access to alcohol via the internet in 2001.

In response to concerns at that time, in 2001 legislative reforms were made so that NSW-based liquor licencees who sell liquor over the internet are required to:

- prominently display their liquor licence number on their website and in any advertisement or information published in writing or electronically in connection with internet sales (to assist with enforcement);
- display a notice stating that "IT IS AN OFFENCE TO SELL OR SUPPLY TO OR TO OBTAIN LIQUOR ON BEHALF OF A PERSON UNDER THE AGE OF 18 YEARS";
- require prospective purchasers to supply their date of birth;
- give written instructions to the person delivering the liquor requiring delivery to the adult who placed the order, or to another adult at the premises who undertakes to accept it on behalf of the adult who placed

The amendments also confirmed that delivery to a minor of liquor purchased over the internet constitutes an offence of supplying liquor to a minor by the person delivering the liquor and by the licencee who sold the liquor.

Further, a new offence was introduced if a minor takes delivery of any liquor sold over the internet. The maximum penalty for the minor was increased to $2,200, from 1 July 2008.

A new offence was also introduced that a person must not order or request a minor to take delivery of liquor sold via the internet. The maximum penalty for the person was increased to $3,300 from 1 July 2008.

These provisions were carried forward to the new *Liquor Act 2007*, which commenced on 1 July 2008. The notice to be displayed on a website regarding sale or supply of liquor to minors was updated at that time to state "IT IS AGAINST THE LAW TO SELL OR SUPPLY ALCOHOL TO, OR TO OBTAIN ALCOHOL ON BEHALF OF, A PERSON UNDER THE AGE OF 18 YEARS".

The NSW liquor laws cannot be used to regulate internet activities by liquor sellers who are not located in this State.

Tobacco

Any advertising of tobacco product is prohibited by Commonwealth legislation. The minimum age at which tobacco can be sold is 18 years, and it is an offence to sell to a minor, or to purchase on behalf of a minor.

Purchasing pharmaceuticals and illicit drugs online

Children may be able to purchase illicit drugs over the internet without understanding the legal implications of making such a purchase.

Of particular concern is the potential for children to purchase analogue drugs online from countries where these drugs are legal. There have been reports of the online purchase of the new analogue drug '4-MMC' (mephedrone).

Also, children may also be able to pose as adults to purchase pharmaceuticals online. Many online pharmacies based outside Australia either do not require a prescription or have an in-house pharmacist who writes a prescription based on symptoms entered online by the patient. The latter two systems are open to abuse as minimal checking is possible in relation to genuine patient requirements.

Online promotion of inappropriate social and health behaviours

Little research has focused on the impact of new technologies on young people's substance using behaviours. However, as with other education promotion opportunities, the growth in online media has provided a new means to promote alcohol, drugs, tobacco and other substances to young people.

The Ministerial Council on Drug Strategy is continuing to consider measures to restrict the retail sales and advertising of tobacco products over the internet, including possible legislation to clarify that the tobacco advertising prohibition extends to the internet.

4. PRIVACY ISSUES FOR CHILDREN AND YOUNG PEOPLE

The privacy of children and young people using the internet may be at risk in several ways.

Children are subject to the same privacy concerns as adults in relation to internet use generally. For example, data is often collected about the users of a particular computer, including the terms entered into search engines, and the websites visited.

However, children's privacy is subject to some specific risks. Children and young people are more vulnerable in the sense that they are less likely to have the nous or capacity to be alerted to potential privacy breaches, to read and understand the fine print of contracts with internet service providers and web page administrators, or to know what action may be available to them if their privacy is breached.

Further, children are often dependent on their parents or other adults for access to technology. There is a question about how much privacy children are entitled to, if any, as opposed to their parents and other adults who provide access to technology. However, two examples demonstrate why privacy issues may still arise.

First, where children are using a computer registered to their parents or another adult, information collected about children will form part of the 'user profile' for the computer at that particular Internet Protocol (IP) address. This raises privacy concerns not only in terms of the collection of such information but also in terms of the "merger" of a child's information with that of adult computer users. Adult computer users may be able to access the information collected about that particular IP address, including the information of other child users of that computer. This may be appropriate in many cases where the relevant user is the parent of the child. However, privacy concerns may arise particularly if the adult to whom the IP address is registered is not the child's parent.

Secondly, spyware (which allows its installer to 'spy' on activity on a computer by, for example, logging the keys that are typed) may impact on children differently to adults. Spyware at an internet café could be used to identify, locate and profile children using that computer. Spyware could also be placed by parents on their own computers to monitor their children's use of the internet including emails. There may be some instances where the use of spyware by parents or other adults is appropriate or necessary but there may be cases where its use is inappropriately intrusive or poses a risk to children's safety.

At present, regulation does not target spyware itself but does target the more serious and culpable uses of spyware such as internet banking fraud, browser hijacking, harvesting and collection of personal financial information, damage to computer settings, identity theft and impairment of security.[11] However, it is unlikely that regulation could effectively target the inappropriate use of spyware by parents in their own homes.

Another area of concern is the use of social networking sites such as Facebook, Bebo, Twitter and MySpace. Concerns include:

- Children may make unwise decisions about what information to post about themselves. They may be less cautious than an adult would be in this regard - studies show that risk taking behaviour increases in adolescence.[12] For example, the UK's *Loaded* magazine recently published pictures of a girl which were circulating on the internet after the now adult woman had published them on her Bebo personal profile when she was 15.[13] Once posted on the internet, such information may be beyond recall unless individual social networking sites have the technological capacity to control the spread of information and do this voluntarily or through legal compulsion.

- Privacy management tools provided by social networking sites may be deficient, or too complex for a child or young person to navigate successfully. Privacy advocates recently criticised Facebook's privacy settings on the basis that they were extremely complex and governed by a privacy policy that was over 5000 words long. Children are at greater risk than adults in terms of using and understanding complex privacy settings and policies.

- Where children do not effectively protect their privacy, there is some risk that their personal information will be used to contact them. Children may be contacted on the internet by people they do not know, including sexual predators.

- Even if children do take steps to protect their own privacy, the nature of social networking sites is such that their privacy may be breached by their peers, who may circulate their personal information without their consent. This may also be a risk with the use of mobile phones.

[11] The following federal legislation may have effect to regulate spyware in this regard: the *Criminal Code Act* (1995), the *Australian Securities and Investments Commission Act 2001*, the *Corporations Act 2001*, the *Privacy Act 1988*, the *Trade Practices Act 1974*, the *Telecommunications Act 1997* and the *Telecommunications (Interception) Act 1979*.

[12] Kelly, A, Schochet, T and Landry, C in their article 'Risk Taking and Novelty Seeking in Adolescence', (2004) 1021 *Annals of the New York Academy of Science* 27 found that:

> *"Risk taking and novelty seeking are hallmarks of typical adolescent behaviour. Adolescents seek new experience and higher levels of rewarding stimulation, and often engage in risky behaviour, without considering outcomes or consequences. These behaviours can … render the adolescent more vulnerable to harm."*

[13] Ireland, Judith, 'Peep Show Can Claim a Price', *Sydney Morning Herald* 29 May 2010.

As most of the major social networking sites are hosted overseas and store/hold personal data on overseas servers, they are unlikely to be covered by the *Privacy Act 1988* (Cth) in its current form, which applies to organisations based in Australia. Nor would they be covered by NSW's *Privacy and Personal Information Protection Act 1998,* which applies only to public sector agencies.

5. AUSTRALIAN RESPONSES TO CYBER SAFETY THREATS

Education Initiatives

It is necessary to understand how and why children make use of technology in order to assist them to become informed users. For example, a school in NSW surveyed Year 7 students about cyber safety as part of a general census. Questions asked included how regularly the internet was used, what sites were visited, and what other purposes the internet was used for (study, social networking, buying and selling items, playing games, looking at videos).

Upon confirming that about 80% of the students belonged to a social networking site, targeted discussions took place with students about never accepting unknown 'friends' or contacts, never disclosing identifying information such as a phone number and address, and never being publicly intimate. The school explains digital community building in a positive light but notes the need for a safe and secure community that students can trust.

The Department of Education and Training's *Online Communication Services: Acceptable Usage for School Students* policy deals with a range of issues relating to students' use of technology. These include access and security, privacy and confidentiality, intellectual property and copyright, and misuse and breaches of acceptable usage of the technology. The policy can be viewed on the Department's website at:
https://www.det.nsw.edu.au/policies/general_man/general/accep_use/PD20020046.shtml?level=Schools&categories=Schools%7CComputers+%26+Internet%7COnline+communication+services.

Students are asked to report any internet site accessed that is considered inappropriate and any suspected security breach involving users from other schools, TAFE or from outside the Department of Education and Training.

Students also receive instruction in relation to these issues as part of curriculum.

The Department of Education and Training is represented on the *Safe and Supportive School Communities* project, a collaborative initiative of the Commonwealth, States and Territories which oversees the *Bullying. No Way*! Website: www.bullyingnoway.com.au.

In support of this initiative schools are provided with a range of anti-bullying materials.

The Ministerial Council for Education, Early Childhood Development and Youth Affairs provides a forum for discussion of education matters across Australia. It could be an appropriate forum for:

- identifying quality practice in delivering solutions for creating safe, quality ICT learning environments and policy development involving education providers Australia wide;

- developing and exchanging resources for students, parents and teachers;

- identifying how the National Curriculum could be best utilised in this area;

- establishing a link with overseas stakeholders such as:

    - the Office of Standards Children's Services and Skills in the UK which has recently issued a report on the safe use of new technologies based on a small scale survey carried out between April and July 2009 in 35 English schools

    - The Secretary of State for Children, Schools and Families in the UK which commissioned a report 'Do We have Safer Children in a Digital World – A review of progress since the 2008 Byron Review'.

The Peer Mediation Program

Community Justice Centres (CJCs) developed, in partnership with the NSW Department of Education and Training (DET) and local schools, a Peer Mediation Program as one of a broad range of conflict resolution strategies available to schools. Peer Mediation involves students trained in mediation leading other students through a structured process to resolve a dispute.

The Peer Mediation Program was first initiated in 1994 as an early intervention strategy that offered an effective method to deal with and resolve some student disputes. It was designed to deal with a range of conflicts between students, including bullying and harassment. Cyber bullying was not an issue at the time of the Program's development. However, the issues and principles are similar to those encountered with bullying generally.

In 2004 Warilla High school sought the assistance of CJCs to introduce a Peer Mediation Program to address issues of school bullying, harassment, and conflict. Two training programs were conducted involving years eight, nine, and ten resulting in 40 peer mediators being accredited within the school. Warilla High School described its experience with the Program as follows:

> In partnership with CJC since 2004, CJC have provided a highly successful Peer Mediation training for over 70 Year 8/9/10 students. Not all students meet the rigorous standards to become a School Based Peer Mediator. The Peer Mediation Program is very much a preventative arm that the school wishes to build on to deal with

> issues of school bullying, harassment, aggression and conflict. The Program includes highly sought after employable skills of conflict resolution, mediation, stress/anger management, leadership, initiative, teamwork, negotiation, communication and goal setting. Peer Mediation involves bringing two parties in a dispute together for the central issue to be discussed and hopefully, an agreement between both parties can be reached *(John Berry/Sue Connell Program Coordinators).*

The Peer Mediation Program was initially introduced into target regions only. Following its success, other school communities across NSW subsequently took it up. The Peer Mediation Program is not a 'quick fix', but rather a long-term Program that is intended to incorporate and become part of the whole school philosophy to create a safe, happy and healthy school environment.

Internet Safety Package - ThinkUKnow

The online education package at www.thinkuknow.org.au contains several tools designed to promote cyber safety.

ThinkUKnow is an Internet safety program delivering interactive training to parents, carers and teachers through primary and secondary schools across Australia using a network of accredited trainers.

Created by the UK Child Exploitation and Online Protection Centre, ThinkUKnow Australia has been developed by the Australian Federal Police (AFP) and Microsoft Australia.

Law enforcement related responses

Cyber-stalking and sexual grooming

The NSW offence of stalking or intimidation with intent to cause fear of physical or mental harm explicitly captures conduct involving the use of telecommunication devices such as "telephone, telephone text messaging, e-mailing and other technologically assisted means" (section 7 of the *Crimes (Domestic and Personal Violence) Act 2007*).

The NSW offence of grooming a child under 16 for unlawful sexual activity also makes provision to capture online conduct and similar means of communication (section 66EB of the *Crimes Act 1900).*

Seeking information from networking sites to assist in law enforcement

The NSW Police Force experiences difficulty in obtaining information from social networking sites, many of which are hosted in the USA.

Current US legislation imposes certain privacy rules against government access, with exceptions for emergency circumstances. Most US social networking sites provide information to law enforcement agencies where illegal behaviour is involved, but some sites have shown an unwillingness to provide information, even when they are legally capable of doing so. Even where incriminating information is provided, it can only be admitted as evidence in Court in accordance with existing Mutual Assistance arrangements.

Self regulation by social networking sites could reduce risks, by:

- Clear and effective abuse reporting protocols;
- Decisive action to remove cyber bullies from the network;
- Cooperation to retain information and make it available to law enforcement agencies on request;
- Including as a condition of use that the host site report user abuse to the relevant ISP.

Identity Theft Sanctions

The recently enacted *Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009*, which commenced on 22 February 2010 modernised fraud and forgery provisions and introduced new identity crimes offences.

The new identity crime offences are based on the national model criminal code, but carry increased penalties. The reforms also allow victims of identity crime to obtain a victim's certificate from a NSW Local Court to help them restore their finances.

Cross jurisdictional coordination

Significant cross jurisdictional issues arise in addressing cyber crime. For example, an offender may be physically located in jurisdiction #1, the ISP the offender uses may be in jurisdiction #2, the satellite used may be governed by jurisdiction #3, the victim may be located in jurisdiction #4, and the investigating Police may be located in jurisdiction #5. For this reason, it is essential that there is national and international coordination to address cyber crime.

At the last meeting of the Standing Committee of Attorneys-General (SCAG) on 7 May 2010, the issue of technology and the law and, in particular, cyber crime was discussed. Ministers discussed the work being done by a number of different bodies throughout Australia to combat the growth of cyber crime. This problem is complex and affects a broad range of public and private sector stakeholders across all jurisdictions. Ministers agreed to create a National Cyber Crime Working Group to facilitate a co-ordinated response to this important issue.

Possible initiatives that could further mitigate the e-security risks to Australian internet users

NSW's laws include computer offences and fraud, forgery and identity crime offences.

The Department of Justice and Attorney General is currently considering a recommendation of the NSW Sentencing Council regarding the use of the internet by sex offenders on parole and serious sex offenders on extended supervision orders. The imposition of internet use restrictions and inspection powers for parole officers and/or other supervising officers from Corrective Services NSW are being examined as part of this process.

The NSW Government also draws the Committee's attention to the Government's submission to the Inquiry into Cybercrime by the House of Representatives Standing Committee on Communications. As previously stated in the NSW Government submission to the Inquiry into Cybercrime:

- There are gaps in current model national legislation on computer and identity crime offences which may need to be addressed. For example, existing computer offences focus on hardware rather than cyber space more broadly. The model identity crime offences were established to capture the members of the syndicates misusing information to commit a crime rather than those at the head of the syndicates or those that develop the means to obtain the information.

- Identity crime is growing and merging with cyber crime as technologies develop. It crosses national and international borders, with the more serious cases of identity crime coordinated by international syndicates. Identity crime occurs in many forms. At the low end it may be through the photocopying of a document. High volume, high impact identity fraud is, however, most often perpetrated by exploiting the opportunities the internet provides. Whilst the states have passed legislation tackling identity crime, the extreme and aggravated form of the offending should be separately reflected by a specific offence in the Commonwealth Criminal Code - committing identity crime using the internet.

- A broader issue relating to cyber crime is police powers, such as 'remote access powers'. By allowing a warrant to be obtained for remote access, law enforcement would be more likely to be able to decipher encrypted data by conducting surveillance at a point between the user and the encryption interface. This would involve remotely accessing (or "hacking into") a computer via the internet to obtain transmissions of product passing over that computer at a point at which it is unencrypted. Such powers would require legislative amendments both at a State and Commonwealth level.

6. WAYS TO SUPPORT SCHOOLS TO CHANGE THEIR CULTURE TO REDUCE THE INCIDENCE AND HARMFUL EFFECTS OF CYBER-BULLYING

Any attempts to change school culture must be supported by parents and the broader community, and reflected by the culture in the homes in which students reside and the community in which they live.

School climate is an important factor in reducing the incidence and harmful effects of bullying. Those schools with high conflict and poor student/teacher morale report higher levels of bullying. Conversely, research shows that bullying is minimised in schools where:

- there are high expectations of students;
- students feel supported;
- there is consensus and cohesion among staff;
- there is a sense of community;
- staff model appropriate behaviour.[14]

Consistent implementation of whole school comprehensive policies is the single most effective action a school can take to reduce bullying. [15]

Research has identified the need for education settings to implement prevention and intervention strategies and methods to address bullying that include:

- ensuring that the concept of bullying is explained clearly;
- delivering programs to teach pro-social behaviours;
- being aware of what is happening and how stakeholders feel about it;
- developing a well supported anti-bullying policy in consultation with students, their parents and the broader school community;
- ensuring that learning how to identify and respond to bullying behaviour, including the development of appropriate bystander behaviour, is part of children's social education and is part of the school curriculum;
- collecting relevant data.[16]

Peer helper programs, buddy programs and transition programs all support the ethos of a school to help one another. Curriculum programs incorporating the direct teaching of values education, empathy training and the use of stories and

[14] James, D.J., Lawlor, M., Courtney, P., Flynn, A., Henry, B., Murphy, N. (2008). Bullying behaviour in secondary schools: What roles do teachers play? Child Abuse Review, 17, 160-173.
[15] Smith, P.K., & Sharp, S. (Eds.) (1994). School bullying: Insights and perspectives. London: Routledge.

[16] Rigby. Bullying in schools and what to do about it. http://www.kenrigby.net/

drama embedded in the curriculum, as well as direct teaching of 'netiquette', could all help to reduce cyber-bullying.[17]

A range of resources to support learning from Kindergarten to Year 12 about cyber citizenship is available to NSW Department of Education and Training teachers via the Teaching and Learning Exchange.

Specific curriculum related support in cyber citizenship includes:

- An exemplar Stage 5 teaching unit, *Think before you click*, which provides a six to ten week teaching program for the mandatory Key Learning Area Personal Development, Health and Physical Education. In this unit students examine issues relating to online behaviour and develop strategies to keep themselves and others safe. A student resource package accompanies this unit;

- Targeted resources, including the *Laptop wrap: Cyberbullying*, designed to equip students to protect themselves against cyber-bullying and *Sites2See: Cybersecurity and safety*, which builds e-security awareness and cybersafety practices.

Professional learning resources that incorporate cybersafety include:

- *Leading my faculty*, an online program for head teachers to support the Digital Education Revolution – NSW, includes a segment on cyber citizenry;

- Laptops for Learning, a face-to-face workshop program for teachers, and related support materials (e.g. frequently asked questions) include material about cybersafety relevant to the Key Learning Area, such as online communication and appropriate images.

Whole School Approaches

NSW government schools implement *MindMatters*, a whole school approach to mental health promotion for secondary schools. *MindMatters* includes modules to foster the development of social and emotional skills, and encourage effective home, school and community partnerships.

Parents play a key role in teaching their children about cybersafety and how to use the computer safely. The NSW Department of Education and Training has developed a technology guide for parents on cybersafety which is available on the Department's website at:
http://www.schools.nsw.edu.au/news/technology/cybersafety/index.php

[17] Campbell, Marilyn A. (2005). Cyber bullying: An old problem in a new guise?, Australian Journal of Guidance and Counselling 15(1):68-76.

Although no parent can 'bully-proof' a child, research suggests parents can assist by:

- helping their children to acquire good interpersonal skills, including making friends and acting assertively when necessary;
- supporting their children if they do become involved in bullying/being bullied at school and being prepared to work collaboratively with the school to solve it;
- assisting schools as much as possible with the development of policies and practices to address the problem.[18]

Given cyber-bullying largely occurs outside the school environment, it is likely that parents have a greater role to play in supervision to prevent bullying by technology than other forms of bullying. This may present challenges for parents who are ill at ease with technology and rely on their children to explain how to use it.[19] At home, the location of the computer is an issue that parents need to consider carefully.[20]

Schools can assist in parent education and encourage parents to talk to young people about the technology. In this way, young people are made aware that adults do know something about the technology and they can seek help from adults when they need to.[21]

CommunityMatters was developed to strengthen the Aboriginal focus of *MindMatters*. *CommunityMatters* includes material that addresses the intersection between bullying and racism directed towards Aboriginal children and young people. For more information, see: http://www.mindmatters.edu.au/resources_and_downloads/community_matters/communitymatters_landing.html

KidsMatter is the first national mental health promotion, prevention and early intervention initiative specifically developed for primary schools. The *KidsMatter* initiative aims to improve the mental health and wellbeing of primary school students, reduce mental health problems amongst students and achieve greater support for students at risk of experiencing mental health problems. *KidsMatter* commenced in 2006 with a national two year trial involving 100 schools from all sectors.

Strategies embedded within whole school approaches include strategies for primary schools such as 'NO GO TELL', which promotes a culture of creating a "telling" school. Strategies for high school students such as 'TRUST, TALK,

[18] Rigby. Bullying in schools and what to do about it. http://www.kenrigby.net/

[19] Ribak, R. (2001). Like immigrants: Negotiating power in the face of the home computer. New Media and Society, 3, 220–238.

[20] Pew (2001). The Internet and education. Retrieved July 19, 2004, from http://www.pewinternet.org

[21] Campbell, Marilyn A. (2005). Cyber bullying: An old problem in a new guise?, Australian Journal of Guidance and Counselling 15(1): 68-76.

TAKE CONTROL' emphasise that older students are more likely to talk to their friends.

The 'Friendly Schools and Families' program comprises whole school (including family) learning and teaching strategies, resources and case studies from Australian schools. It is based on six years of research involving over 6,000 school students, their parents and teachers. This evidence-based program has been rigorously evaluated and found to improve young people's social skills and reduce bullying behaviour.

In 2009, 39 primary and secondary schools worked in local community clusters on strategies promoting student safety and wellbeing in Years 5 – 8.

Restorative practices are essentially about relationships and interactions, and aim to promote a sense of connectedness within schools and their communities. A great deal of variability between schools in the application of the principles and processes is expected. This makes it difficult to evaluate across settings. However, if implemented correctly, it may improve the school environment and enhance the learning and development of young people.[22]

Restorative practices may be an effective mechanism to counter bullying. This approach concentrates on promoting values likely to lead to responsible citizenship, such as pride in one's school and an obligation to help others. Addressing the problems of bullying is seen as requiring confrontations with the person bullying, the deliberate inducement in them of appropriate shame, and action undertaken by them to restore positive relations with the person being bullied.

Restorative practices are used in a number of NSW government schools in ways that meet the particular needs of that school community. The results in those schools are a marked, positive culture change.

There is Australian data that indicates that there is a decrease in suspension rates through the application of restorative conferencing in schools, along with high rates of participant satisfaction (e.g. person harmed, parents and wrongdoer) and high rates of compliance with agreement (above 90%).

Positive Behaviour for Learning

Positive Behaviour for Learning is a school-wide systems approach to prevent problem behaviour and improve academic outcomes. Research suggests that improved academic outcomes require an explicit focus on social behaviour combined with effective curriculum and effective instruction. An important component of Positive Behaviour for Learning is the adoption of a continuum of behaviour supports that acknowledges the fact that, like academic

[22] Youth Justice Board for England & Wales, Restorative Justice in Schools Report. 2004, p.65

instruction, students will need differing levels of behavioural intervention and supports to be successful in school.

Interventions for children and young people who bully

In many cases, children who bully others are asserting their social power and have learned to use that power aggressively. The challenge is to redirect this leadership potential from the negative strategies of bullying to positive leadership skills and opportunities. These children require support to find positive ways of gaining power and status within their peer relationships. They need to be provided with formative rather than punitive consequences. Interventions should provide a clear message that bullying is unacceptable, but also build awareness, skills, empathy and insights and provide appealing alternatives to bullying.

Interventions for children and young people who are bullied

Children who are persistently bullied experience abuse from peers and are often not supported by children who witness the bullying, or by adults (who may be unaware of the problem). The task is to help these children find ways to develop positive connections with peers and a trusted adult.

There is some evidence that teachers can help promote positive relationships through:

- establishing buddies;
- circles of support;
- peer mentors;
- finding ways to highlight the child's talents for others to see.

Support can be provided through programs that emphasise social skills, but especially through consistent moment-to-moment support from teachers, parents and peers.[23]

Interventions for children and young people who witness bullying

Research is increasingly recognising the important role bystanders (those who witness bullying) play in instances of bullying, and the role the peer group plays in reinforcing bullying behaviour.

Research has documented the benefits of engaging bystanders to take a stand against bullying by safely intervening directly, telling a trusted adult, or at least by not encouraging the bullying child. Some research suggests that bystanders might be easier to influence than those who bully. This is because bystanders often think that bullying is wrong and they would like to do something to help.

[23] Boyle, D.J. (2005). Youth Bullying: Incidence, Impact, and Interventions. Journal of the New Jersey Psychological Association, 55(3), 22-24.

However, it is noted that converting bystanders' already existing attitudes into behaviour is a challenging task.[24]

Children need help understanding their social responsibility to intervene when bullying is taking place. For example:

- peers can be coached in taking a stand when bullying occurs;
- children and young people may need scripts for what to say and do to intervene in a positive way;
- adults need to establish conditions in which children feel responsible, and to encourage children to take the risk of speaking out against bullying;
- adults need to listen respectfully and respond with relationship solutions to empower children to act.

[24] Salmvalli, C. Bullying is a group phenomenon – What does it mean and why does it matter? See http://www.education.com/reference/article/peer-social-group-role-in-bullying/?page=2

7. THE ROLE OF PARENTS, FAMILY AND THE COMMUNITY

The role of adults, including teachers and parents

Bullying and cyber-bullying are whole of community issues and they require whole of community responses. Parents, families, carers, the community, all levels of government, school systems, schools, and researchers have a role to play in efforts to address bullying and cyber-bullying.

The NSW Government response to the report of the Legislative Council General Purpose Standing Committee No 2 *Inquiry into Bullying of Children and Young People* outlines the actions the Government has planned to address bullying including cyber-bullying. The report recognises that bullying is a whole of community issue and commits the Government to work hard to ensure greater coordination and cooperation across all levels of government, school systems, schools, the community and researchers in efforts to address bullying.

The Department of Education and Training hosted a Cyber-bullying Forum in November 2009 which resulted in new links between educators, researchers, industry experts, students, parents and community members who will all continue to work together to develop strategies for the whole community to address cyber-bullying.

Research has established that adults need to take responsibility for constructing environments that promote positive peer interactions. This includes:

- adults discouraging grouping together children who are similarly aggressive and engaged in bullying, because of the potential for this to reinforce bullying behaviour;
- school staff modelling appropriate behaviour management in the classroom and other learning environments;
- teachers ensuring that working groups in the classroom are balanced with a mix of abilities. By proactively reorganising children's social groupings, teachers can avoid embarrassment for students who have not been chosen by any group;
- providing children with consistent lessons to develop the complex skills required for healthy relationships. Solutions need to focus on promoting relationship skills for all children involved in bullying: those who bully, those who are bullied, as well as those who are bystanders.[25]

Researchers identify that lower rates of bullying are associated with the following teacher behaviours:

- caring for students;

[25] Pepler, D., Craig, W http://www.education.com/reference/article/role-of-adults-in-preventing-bullying/

- using effective teaching practices;
- monitoring student behaviour;
- appropriately intervening in cases of student misbehaviour;[26]
- remaining conscious of cyber-bullying and intervening in suspected incidents.[27]

Child Protection Education provides a framework for learning about respectful relationships and personal safety. Child Protection Education is mandatory at every stage of education from Kindergarten to Year 10 in NSW government schools.

An important message of Child Protection Education is that children and young people should seek help when they feel unsafe. Students learn to assess their personal safety in various situations and learn to identify feelings and other signs that indicate when they may be unsafe. These may include feeling uncomfortable or being asked for too much personal information when using the internet. Students learn a range of protective strategies and ways to seek help.

There is an extensive network of staff who provide support to students in NSW government schools. This network includes class teachers, executive staff, the school's learning support team, home school liaison officers, support teachers learning assistance, out of home care teachers and a range of other regional positions including student welfare consultants, who work with schools to develop whole school programs and to provide support to individual students. School counsellors are also a component of this network.

As well as having a specific role in providing psychological services, school counsellors contribute to student emotional and social wellbeing through collaboration with and membership of student welfare teams.

They are available to support students experiencing issues with cybersafety through exploration of the issues, and through assisting the student to access helpful websites such as the *Bullying No Way* website located at: www.bullyingnoway.com.au. School counsellors also assist students to identify legal support, for example by liaison with police.

Children in Out-Of-Home Care (OOHC)

When a child or young person in OOHC has been identified as either a victim or a person responsible for perpetrating cyber bullying, an interagency response may be warranted, with consideration given to the particular

[26] Ryan, R.M. (2008). *Too Good To Last* in Pajares, F. & Urdan, T. (Eds) (2008) The Ones We Remember. *Scholars Reflect on teachers Who Make a Difference.* USA. Age Publishing Inc.
[27] Campbell, Marilyn A. (2005). Cyber bullying: An old problem in a new guise?, Australian Journal of Guidance and Counselling 15(1):68-76.

vulnerabilities of children and young people in OOHC, as a result of past experiences of abuse and neglect.