The Alannah and Madeline Foundation
Keeping children safe from violence

Submission to

JOINT SELECT COMMITTEE ON CYBERSAFETY

25 June 2010

The Alannah and Madeline Foundation
Level 1, 6 Charles Street
PO Box 5192
South Melbourne 3205

www.amf.org.au

The Alannah and Madeline Foundation: *keeping children safe from violence*

Contributors

Ms Sandra Craig, Manager, *The National Centre Against Bullying*
Ms Jackie Van Vugt, General Manager, Cybersafety, The Alannah and Madeline Foundation
Dr Judith Slocombe, CEO The Alannah and Madeline Foundation
Ms Mandy Ross, School Services Manager, The Alannah and Madeline Foundation

For correspondence, contact: info@amf.org.au or 03 9697 0666

SUBMISSION FROM THE ALANNAH AND MADELINE FOUNDATION TO THE JOINT SELECT COMMITTEE ON CYBERSAFETY

Introduction to The Alannah and Madeline Foundation

The Alannah and Madeline Foundation welcomes the opportunity to submit a response to the Joint Select Committee on Cybersafety.

The Alannah and Madeline Foundation is a national charity protecting children from violence and its devastating impact. The Foundation was established in memory of Alannah and Madeline Mikac, aged 6 and 3, who, with their mother and 32 others were killed at Port Arthur, Tasmania on 28 April 1996.

The Foundation cares for children who experience or witness serious violence. We have a number of programs that help children and young people.

The Foundation's Intensive Support Program helps children by focusing on what they need to recover from traumatic events or violent circumstances. We work collaboratively with relevant agencies to make sure children who are suffering the effects of violence, and their families, have the community connections needed for immediate and long term support.

In Australia, tens of thousands of children are placed in emergency foster care or domestic violence refuges each year, often with nothing but the clothes they are wearing. The Buddy Bags Program provides these children with a back pack full of essential items including toiletries, pyjamas, socks, underwear, a teddy bear, photo frame and pillow slip. Buddy Bags provide personal belongings and help restore a sense of security in these children's lives.

A Refuge Therapeutic Support Program funds group therapy including art, pet and music therapy to help children who are residing in refuges and are distressed or traumatised by their experience of serious violence.
The Alannah and Madeline Foundation plays an advocacy role and is a voice against childhood violence.

Children365: celebrate them everyday is another way in which the Foundation advocates for the wellbeing of children. This initiative encourages adults to take the time to think about why the children in their lives are important and how they can spend time together. Through an annual calendar and a range of activities, Children365 gives people practical suggestions for ways they can engage positively with children. Children365 begins each year on the last day of children's week and was developed in memory of 4-year-old Darcey, who was killed on 29 January 2009.

The Foundation's National Centre Against Bullying (NCAB) is a peak body made up of experts (See Appendix 2) in the fields of childhood wellbeing and bullying, chaired by Alastair Nicholson AO RFD QC, former Chief Justice of the Family Court of Australia. NCAB works with school communities, government, media and industry to reduce bullying and minimise its harm to young people.

In addition, the Foundation develops programs designed to help prevent violence in the lives of children. The Better Buddies Framework is a peer support initiative designed to create friendly and caring primary school communities where bullying is reduced. In Better Buddies, older children buddy up with younger children and learn the values of caring for others, friendliness, respect, valuing difference, including others and responsibility. This occurs through formal and informal activities in the classroom and beyond. Better Buddies enables younger students to feel safe and cared for while older students feel valued and respected in their role of mentor and befriender.

Our Cybersafety and Wellbeing Initiative helps children and young people embrace the benefits of technology and reduce their exposure to cyberspace risks, such as cyberbullying, online sexual predation, sexting, identity theft and fraud. The initiative introduces a national framework in schools, which guides them through the implementation of policies and practices to ensure their teachers, students, and families are equipped to be smart and responsible users of the technology. The Framework has recently been piloted in more than 150 schools across Australia, with the support of the Department of Education, Employment and Workplace Relations. A report has been submitted to DEEWR.

Recommendations

The recent 4th Biennial *National Centre Against Bullying (NCAB)* conference in Melbourne (April 2010) focused on cybersafety and wellbeing ('Navigating the Maze: cybersafety and wellbeing solutions for schools'), attracting international delegates and presenters, with 400 delegates from across the world.

We support and endorse the recommendations for action (below) from that conference.

1. Early intervention

- Need to identify early (at pre-school and early primary school) those who may have peer relationship issues, and implement appropriate programs.
- Additional focus is needed on pre-school education to prevent bullying and promote wellbeing
- Need to raise awareness among schools and parents of the emerging evidence that children are using social networking sites at a young age.

2. Training teachers

- Need for pre-service teacher education programs to include a mandatory component, which addresses awareness and skills for preventing and managing bullying situations.
- Teachers must have ongoing access to training to develop the skills needed to respond effectively to bullying situations.
- Need for general education programs for teachers, students and parents as to the possible effects of the criminal and civil law on the use of communications technologies.

3. An appropriate legal framework

- Need to legally define the rights and responsibilities of schools in responding to bullying and cyberbullying situations, and cyber-defamation.
- Legal remedies in themselves are not a solution to bullying, but are a necessary part of the solution. Need to clarify the role of the criminal and civil law in relation to cyberbullying and bullying.

4. Increased focus on school transition

- Bullying peaks at times of transition between pre-school and primary school, and primary school and high school, therefore, education institutions need to increase their focus on bullying, including cyberbullying at these times.

5. A whole-school approach

- Schools need to use evidence-informed strategies and include teachers, parents, students and the wider community to enhance cybersafety and wellbeing, and reduce bullying.
- ·Funding is required to ensure every school has the required welfare personnel to support students.

6. A whole-community approach

- Solutions need to go beyond the school gate, given that bullying in schools is often a reflection on community behaviours and attitudes to violence.
- There is also a need to address all forms of bullying as a health problem. Health professionals need to undergo appropriate training and be involved in developing solutions.

7. Young people to be part of the solution

- Young people are essential to the solution and must be involved in policy development, parent education and development of multi-media education materials.

8. Technology to be part of the solution

- Adults, including parents and teachers, need to break down the digital divide by becoming savvy about technology.
- We all must recognise the creative use of technology as a powerful teaching and socialising tool.
- The focus needs to be on behaviours and positive relationships; and it is counterproductive to ban access to technology.

9. Support for ongoing research in Australia

- Research into cybersafety and wellbeing, including effective strategies for engaging parents, keeping up-to-date with changes in technology, appropriate interventions in schools etc.

10. Federal funding

- Sufficient Federal funding for an Australia-wide system to implement these cybersafety and wellbeing solutions for schools.

i. the online environment in which Australian children currently engage, including key physical points of access (schools, libraries, internet cafes, homes, mobiles) and stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers)

The online environment for Australian children and young people is a world which they perceive to be seamlessly connected with their own physical world. A number of commentators have adopted the term 'digital natives' when they reflect about the way young people engage with technologies as a vital part of their social life and the building of their identity. This contrasts with the ways older people ('digital immigrants'), use and perceive technologies as functional tools primarily used for practical or business purposes.

This environment offers young people unprecedented access to resources that continue to evolve ever more rapidly. This wonderful range of new technologies offers enormous educational potential but also poses some serious challenges and risks.

'In the 12 months prior to April 2009, an estimated 2.2 million (79%) children accessed the Internet either during school hours or outside of school hours. The proportion of males (80%) accessing the Internet was not significantly different from females (79%). The proportion of children accessing the Internet increased by age, with 60% of 5 to 8 year olds accessing the Internet compared with 96% of 12 to 14 year olds' (Australian Bureau of Statistics, April 2009).

The overall challenge for society and schools in particular is to embrace these new technologies as positive tools for building relationships, learning and teaching, whilst at the same time identifying and addressing the safety risks attached to their use. Young people are starting to develop a moral compass with which to navigate their way through cyberspace (Bauman, 2007) but have limited experience in assessing risk and predicting and weighing up the potential consequences of their behavioural choices.

Australian children enter the online environment through a number of key access points. These points of access have changed considerably over the last five years and are continuing to change rapidly.

Increasingly, the preferred way for young people to access the online environment is by mobile phone and other wireless devices. Using a 3G network, young people can make calls, create and send multi-media messages and emails and participate in online games. Users can also search for information, find or track locations via a Ground Positioning Satellite (GPS). If the phone has a Bluetooth connection, photos and other information can be transmitted phone-to-phone. There are now more mobile phones than people in Australia and even young people may have more than one.

According to ABS statistics, in 2009, 72% of Australian households had home internet access and 78% of households had access to a computer. Between 1998 to 2008-09, household access to the internet at home has more than quadrupled from 16% to 72%, while access to computers has increased from 44% to 78%. In addition, the Australian government has undertaken to provide individual

computer access for every high school student in years 9 to 12 by the provision of wireless netbooks, thus providing young people with unprecedented access to a range of applications, creating borderless classrooms and blurring the boundaries between school and home. The rollout of computers under this initiative is ongoing.

Young people also have access through schools and libraries, through other computer facilities in their homes, friends' homes and other venues such as cyber cafes.

Most schools have policies in place as well as filters provided by their educational authority. Those schools with effective behaviour management systems and vigilant supervision of student use of computers provide another layer of support and protection. Unfortunately, in many schools, policies are not backed up with clear procedures that are consistently followed by teachers, or widely known and understood by teachers, students and their parents/carers. Australian schools also have much ground to make up in producing robust acceptable use policies that reach beyond the school gate to include parents and the wider community.

Computer access by young people from libraries is also frequent, and libraries have internet use policies to guide users. The Australian Library and Information Association (ALIA) supports the basic right of library and information services users to unhindered access to information regardless of format and hold the position that "freedom can be protected in a democratic society only if its citizens have unrestricted access to information and ideas". Students may therefore be able to access information otherwise unavailable to them via home or school computers.

Libraries are also supported by ACMA and other bodies to provide users with information to keep themselves safe from offensive or illegal material. Young people can also expect to be provided with lists of safe websites to visit and useful links to help with schoolwork, hobbies or interests. Libraries also often provide training sessions on internet use and links to information to help with negative online experiences including cyberbullying.

The Foundation commissioned Sweeney's Research to undertake qualitative research with parents, teachers and teenagers to ascertain attitudes to and usage of technologies.

All participants identified themselves as high users of technologies. Parents used technologies in very functional ways, to search for information or to communicate while teachers used technologies for this and a wider range of purposes, including as a teaching tool and to build cognitive skills in students. Young people used technologies much more holistically; to communicate, learn, socialise, play, research, do homework, and in fact, their on-line life blended seamlessly with their offline life. Parents felt a lack of control because they did not fully understand how their children used technologies and cited threat from predators as their greatest fear. Teachers also felt a lack of control due to limited understanding of how children use technologies and they identified cyberbullying as the primary risk, with internet addiction and lack of sleep being other significant issues. Children and young people on the other hand were dismissive of their parents' and teachers' fears and cited their biggest issues as slow internet and viruses. However, further probing revealed that nearly all young people interviewed had experienced or witnessed cyberbullying and considered it common and extremely unpleasant.

Parents and teachers lacked knowledge about technologies and were fearful even paranoid about the risks, while young people were fearless but naïve about the risks. The goal is to bridge this digital divide by increasing both adults' and young peoples' knowledge about the smart use of technologies, about the potential risks and how to reduce and manage these risks, in other word create a culture of smart/savvy use within the community.

Stakeholders controlling or able to influence that engagement (governments, parents, teachers, traders, internet service providers, content service providers)

A variety of stakeholders is involved in the control and influence of these environments. These include governments and a variety of governmental agencies, internet service providers (ISPs), content providers, non-government organisations (including commercial and not-for-profit), teachers and school administrations, parents, and libraries.

In 2007, The Alannah and Madeline Foundation held a Cybersafety Symposium in Melbourne, which made a number of recommendations, (See table 1).

In 2009, as part of the Cybersafety and Wellbeing Initiative (*eSmart*) The Alannah and Madeline Foundation formed a Reference Group (see table 2), bringing together many key stakeholders involved in technologies, wellbeing and cybersafety. The aim of convening this group at regular intervals to is to ensure the Foundation and its *eSmart Schools* initiative incorporates the latest research and educational practices into the *eSmart Schools Framework*. The inclusion of the Australian Federal Police (AFP) and the Australian Communications and Media Authority (ACMA) and technology companies ensures the latest technologies and the way young people use them, and the latest risks that young people might face are understood and dealt with appropriately by *eSmart Schools*.

A second Consultative Group (see table 3) brings together key stakeholders from the various educational jurisdictions from around Australian to ensure the *eSmart Schools Framework* aligns with current educational policies and practices.

In 2010 the Alannah and Madeline Foundation's *National Centre Against Bullying (NCAB)* held the 4th Biennial NCAB conference where stakeholders from industry, the education sector, research as well as the legal and psychology professions came together to discuss the latest trends and information on cybersafety. International and Australian experts presented the latest research and programs focusing on wellbeing and cybersafety in schools.

The Alannah and Madeline Foundation, through the development of its Cybersafety and Wellbeing Initiative (*eSmart*) has done much to address some of the concerns identified by the 2007 symposium. Nevertheless, the intervening time has revealed even more clearly the need for ongoing action.

The Alannah and Madeline Foundation continues to work with a broad range of stakeholders to be able to provide advice about current best practice for cybersafety and wellbeing for schools.

Table 1 Cybersafety Symposium Recommendations

GOVERNMENTS

Governments have a key role to play in ensuring that internet services are safe, fast and accessible to Australian consumers:

1. **Continue to support Australia-wide consistency and accountability in safe and responsible use of ICT**

☐ Federal and State Governments have already developed a range of responses. Further responses are called for, involving a coordinated, collaborative and strategic national approach inclusive of all levels of government and beyond individual interest groups and party politics.

2. **Provide funding to support schools to implement policies, strategies, counselling and professional development for principals and teachers (both pre-and in-service)**

☐ Provide further support to schools to undertake the above tasks as a matter of urgency. Despite significant input from State and Federal governments, many teachers still lack skills and understandings. Course material for pre-service teachers, current teachers and principals needs to be reviewed and/or redeveloped.
☐ Encourage and reward the development of anti-bullying and wellbeing initiatives by schools.
☐ Develop a safe school accreditation scheme on the lines of the SunSmart initiative, incorporating school bullying and cybersafety issues.

3. **Continue to provide resources and education for young people, families, communities and businesses about safe internet usage**

☐ Education for parents and young people about safe ICT usage needs to be developed together with an action plan for their delivery.
☐ Key messages for parents can readily be developed and implemented in Australia.

4. **Federal, State and Territory governments develop integrated formal cybersafety approaches in schools that also, encourage student led participation**

☐ An integrated cybersafety curriculum to be taught across the key learning areas in every state and territory and involve the development of values, critical thinking as well as resilience skills and competencies. Student leadership and participation is also an important key to the success of such initiatives.

PARENTS

There is general agreement that involving parents is critical to ensuring children's safety and their respectful and responsible use of technologies. There is much work to be done to give parents a realistic view of benefits and risks pertaining to their uses. Young people are less apt to share or disclose with parents who don't appear to understand or care what their children are doing online. Young people can, however, have a key role in educating parents about their lived online experience – one that, it appears, they are keen to assume.

Parents have a key role in the education, supervision and protection of their children from the variety of risks they face in cyberspace:

1. **Take responsibility for their children's cybersafety when using these technologies and treat cybersafety issues in the same way they would about other safety matters – e.g. drug use or safe sex**

☐ *Need to be made aware of the potentially harmful effect on their children of extensive and/or unsupervised use of internet and mobile phone technology, and the range of risks their children potentially face*

☐ *Need to know that on line parenting uses similar strategies to off line parenting in which communication is the key and a variety of key messages can readily be developed to assist parents' understanding. Parents also need to support schools in their endeavours to manage these technologies.*

2. **Are aware of and monitor their children's activities and usage**

☐ *Provide instructions and information to help parents to access, monitor and manage their children's activities and usage of internet and mobile phone technologies easily and effectively.*

3. **Have clear understandings and agreements within the family about acceptable internet and mobile phone use**

☐ *Agreements established within the family are most effective in the context of respectful communication and behaviour modelling by adults. Some families may wish to formalise such agreements in writing. A number of such contracts/agreements are already available on such sites as microsoft.com*

4. **Are aware of the wide range of available resources available to help them manage their children's internet use such as:**

☐ *Publicity about and provision of net-filtering resources is already in the Federal Government's response to Cybersafety. However, as emphasised at the Symposium, these are more effective with younger children. We suggest that children and young people be encouraged and educated to take responsibility for their own use of ICT and online behaviour.*

Filtering software can also be applied in age-appropriate ways:

- Under 7yrs: high settings combined with education about good practice and resilient and responsible behaviours while using technology
- Over 7yrs: mid-adolescence: medium settings, combined with values- based education building personal responsibility for online behaviour
- Mid-adolescence – 18: low settings, together with an expectation that these young adults will increasingly adopt a guardianship role toward younger students/siblings, reinforced by cybersafety curriculum and community education

5. **Maintain open communication with their children about issues pertaining to ICT use**

☐ *Many children and young people are reluctant to tell their parents about cyberbullying and other forms of online abuse fearing that access to their social networks will be removed. Parents need to be supported to communicate effectively with their children on mobile phone and internet use (gaming, chat rooms, messages, keeping personal details private, voice masking, responding to unwelcome attention, combating addiction).*

Through community education initiatives, parents can be given a range of strategies and activities to help them teach their children the prosocial skills that underpin values.

TEACHERS / SCHOOLS

1. **Schools have a 'duty of care' to create a safe environment for their students and staff. Cybersafety is a part of this expectation**

☐ *The National Safe Schools Framework provides a template for action; however, ongoing support is needed for schools to develop action plans and a range of strategies for the creation of Cyber-safe environments.*

2. **As part of a whole-school wellbeing focus, support schools in the development of acceptable internet use policies and implementation guidelines that are understood and agreed to by the whole school community**

☐ *Policies are most effective when they are developed collaboratively, with the involvement of all school and community members. The development of such policies by all schools could be mandated by Federal and State Governments and perhaps be tied to school funding.*

☐ *Young people are very expert at manipulating these technologies but may not have the emotional or intellectual readiness for experiences they may encounter online. However, successful development of responses to the range of identified concerns must incorporate young people's input.*

3. **Schools continue to promote the Nine Values for Australian Schooling (Government of Australia) or work consultatively with their communities to develop their own agreed set of values**

☐ *Most members of the Symposium were unaware of the Federal Government's work in the area of values. The work currently being done by schools to teach children – particularly in the Values Framework Best Practice Grants Project should receive a higher profile. (However, research shows that young people – Generation –Y – refer less to core societal values than to the agreed values of their peer group and it would be prudent to recognise this when developing programs.) (McCrindle, M, 2002)*

4. **Measure and monitor the effectiveness of cybersafety policies and work as a whole community to address any issues**

☐ *A user-friendly evaluative toolkit in text and online versions to be developed and made available to all schools.*

INDUSTRY INVOLVEMENT

- Traders
- Internet service providers
- Content service providers

1. **Contribute to developing and implementing solutions where the safety of children and young people is the primary goal**

☐ *With key stakeholders, organise a national symposium along the lines of the recent Melbourne Symposium, in partnership with young people, to encourage further discussion and cooperation and the development of further strategic responses.*

2. **Take charge of key messages and initiatives at point of sale and online e.g. Microsoft Security**

☐ *While parts of the corporate and industrial sectors have already made a range of proactive responses, a more unified, coordinated response and perhaps development of a regulatory framework is necessary.*

YOUNG PEOPLE

While technologies offer attractive opportunities for young people, they also place them at risk of experiencing unsafe, abusive or aggressive behaviour online and through mobile phones such as cyberbullying, sexual predation, stalking, accessing inappropriate content, sexually suggestive images and identity fraud. They should gain sufficient knowledge to:

1. **Understand the consequences of cyberbullying and other harmful behaviours and the severe personal and societal consequences this can have**

☐ *The consequences of cyberbullying and other online abuse can be severe in the short and longer term for perpetrators of abuse and their targets, whole-school wellbeing and communities. There is good evidence suggesting that those who engage in antisocial behaviour unchecked at school often continue this behaviour in their adult lives.*

2. **Understand that they may be breaking the law and that there are legal penalties for cyberbullying and other harmful online or mobile phone activities**

☐ *A campaign publicising consequences for breaking the laws relating to cyber use would be part of any government cybersafety strategy, with messages reinforced by the family and through school curricula.*

3. **Be aware that the cyber-environment is not private and their online activities can be traced**

☐ *The cyber world is a public domain and online activities leave 'digital footprints' which can reveal the identity of those who engage in behaviour that is abusive to others or harmful to themselves. Students need a clear understanding of this, through school curricula and public advertising.*

4. **Be involved in seeking solutions and in developing cybersafety strategies**

☐ *Young people are very expert at manipulating these technologies but may not have the emotional or intellectual readiness for experiences they may encounter online. However, they must be involved in the development of responses to the range of identified concerns.*

LEGAL RESPONSES

1. **Draft legislation to ensure a legal framework to manage cyber-abuse that crosses state and political boundaries**

☐ *Federal, State, and Territory government convene a working group involving other stakeholders to consider an appropriate legislative response to cyberbullying and bullying in general in our schools.*

☐ *Because of the lack of boundaries for the abuse that occur online and with mobile phones, all Australians need to be confident that consistent rules and consequences will apply in all states and territories.*

2. **Create a nationally coordinated cyber-policy plan involving all jurisdictions**

☐ *People who have been the victims of cyber abuse need a dedicated body to which they can address concerns and complaints, and which has the expertise to remove offending material and prosecute offenders rapidly.*

FEDERAL and STATE GOVERNMENT

1. **Continue to support Australia-wide consistency and accountability in safe and responsible use of ICT**

☐ *Federal and State Governments have already developed a range of responses. Development and coordination of further responses are called for, involving a coordinated, collaborative and strategic national approach inclusive of all levels of government and beyond individual interest groups and party politics.*

2.	**Provide funding to support schools to implement policies, strategies, counselling and professional development for principals and teachers (both pre-and in-service)**
☐	*Provide further support to schools to undertake the above tasks as a matter of urgency. Despite significant input from State and Federal governments, many teachers still lack skills and understandings. Course material for pre-service teachers, current teachers and principals needs to be reviewed and/or redeveloped.*
☐	*Encourage and reward the development of anti-bullying and safe school initiatives by schools.*
☐	*Develop a safe school accreditation scheme on the lines of the Sun-Smart initiative, incorporating school bullying and cybersafety issues.*
3.	**Continue to provide resources and education for young people, families, communities and businesses about safe internet usage**
☐	*Education for parents and young people about safe ICT usage needs to be developed together with an action plan for their delivery.*
☐	*Key messages for parents can readily be developed and implemented in Australia.*
4.	**Federal, State and Territory governments develop integrated formal cybersafety curriculum taught across key learning areas, encouraging student led participation**
☐	*An integrated cybersafety curriculum to be taught across the key learning areas in every state and territory and involve the development of values, critical thinking as well as resilience skills and competencies. Student leadership and participation is also an important key to the success of such initiatives.*

Table 2 Reference Group membership

***The Cybersafety and Wellbeing Initiative* Reference Group**	
Chris Althaus	CEO, Australian Mobile Telecommunications Association
Terry Aulich	Executive Director, Australian Primary Principals Assoc.
Andrew Blair	President, Australian Secondary Principals Assoc. and Member NCAB.
Dr Michael Carr-Gregg	Adolescent Psychologist, Media Commentator, Member NCAB
Ian Claridge	GM Student Wellbeing and Support, Vic Dept of Education & Early Childhood Development
Sandra Craig	Manager NCAB and RMIT eSmart Schools, The Alannah and Madeline Foundation
Prof. Donna Cross	Professor, Edith Cowan University, Member NCAB
Maree Davidson	Health Promotion/Social Change Consultant, Davidson Consulting
Jo Degney	Program Manager, Inspire Foundation
Karen Flanagan	Child Protection Program Manager, Childwise
Neil Gaughan	National Manager High Tech Crime Operations, Australian Federal Police
Julie Inman-Grant	Regional Director, Internet Safety and Security, Microsoft
Darren Kane	Corp Security & Investigations; Exec. Dir. Mobility Products & Device Management, Telstra
Nerida O'Loughlin	General Manager Industry Outputs, and Manager Cybersafety Programs, ACMA
Marco Pantano	Industry Manager - Government, Education & Medical, Intel Australia
Carol Ronken	Research & Policy Development Manager, Bravehearts
Greg Sutherland	Executive GM Strategy & Marketing, NAB (and AMF Board)
Mary Tobin	Manager Student Wellbeing, Catholic Education Office
Irene Verins	Senior Program Advisor- Mental Health & Wellbeing, VicHealth
Andree Wright	Executive Manager of Codes, Content & Education Branch, ACMA

Table 3 Consultative Group membership

***The Cybersafety and Wellbeing Initiative* Consultative Group**	
Ms Kris Arcaro	Department of Education and Early Childhood Development, Victoria
Ms Larissa Brenner	Department of Education, Tasmania
Mr Greg Cox	Department Education and Children's Services, South Australia
Ms Anita Davidson	Department of Education and Training, Northern Territory
Ms Denise Deverill	Department Education and Training, New South Wales
Ms Bronwyn Egan	Catholic Education Office, Victoria
Ms Jeanette Hasleby	Department of Education, Western Australia
Ms Christine Lucas	Department of Education, Employment and Workplace Relations (DEEWR)
Adjunct Professor Helen McGrath	Royal Melbourne Institute of Technology School of Education
Ms Sandy Phillips	Department of Education and Early Childhood Development, Victoria
Ms Katrina Reynen	Department of Education and Early Childhood Development, Victoria
Ms Robyn Treyvaud	Centre for Strategic Education/CyberSafeWorld
Ms Lisa Wait	Australian Communications and Media Authority (ACMA)
Dr Paul Weldon	Association of Independent Schools Victoria

ii. the nature, prevalence, implications of and level of risk associated with cybersafety threats, such as:

- **abuse of children online (cyberbullying, cyber-stalking and sexual grooming);**
- **exposure to illegal and inappropriate content;**
- **inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking);**
- **identity theft; and breaches of privacy;**

Cyberbullying

Recent research reveals that approximately 10% of Australian students in upper primary and secondary schools have experienced cyberbullying (Cross et al, 2009). Evidence from the USA and UK suggests this trend will increase, with about 30-40 per cent of students in these countries experiencing cyberbullying. It can happen at any hour, anywhere and reach a vast audience. Cyberbullying has been and remains the most pervasive form of serious risk faced by young people when they use technology.

Cyberbullying is a subset of bullying and considered a form of aggression, involving the abuse of power in relationships. Bullying per se is recognised globally as a complex and serious problem. While bullying has been recognised as a phenomenon for many years, more recently it has been defined as a specific type of aggressive behaviour intended to 'cause harm, through repeated actions carried out over time, targeted at an individual who is not in a position to defend him/herself' (Olweus, 1980). This definition of bullying, as a form of unprovoked, intentional behaviour characterised by a power imbalance, is widely accepted in Australia and internationally.

Bullying has many faces, including the use of emerging technologies, and varies by age, gender and culture (Kandersteg Declaration Switzerland, June 10, 2007). The development of 3rd generation mobile phones and Web 2.0 technologies is changing this landscape almost daily, with an increase in risk for young people.

We are now conscious of distinct differences between cyberbullying and face-to-face bullying: a form of covert bullying, it can happen at any time, anywhere; and there is no escape behind doors. Audiences can be huge and reached quickly. Power is allocated differently, and bullying can be inter-generational. Perpetrators can have at least an illusion of anonymity and their behaviour can be disinhibited because of this; empathy is also reduced because the victim's reaction is not seen.

However, there is little common agreement in the way the term 'cyberbullying' is used. Many websites refer to any negative online behaviour in this way, without stressing its repeated nature. Students describe and appear to understand 'cyberbullying' as a set of discrete behaviours such as ignoring or excluding, threatening, rumours, and bullying' (Cross, et al, 2009), carried out through mobile phone (text or SMS messages) pictures sent, phone calls, email, chat

rooms (MSN) social networking, games like Runescape or World of Warcraft, blogs or through websites (Cross, et al, 2009).

Sweeney Research commissioned by the Foundation identified a number of useful insights about the ways in which young people think and talk about these behaviours. They do not themselves use the terms 'cyberspace' or 'cyberbullying' although they understand them. They are generally not concerned with cybersafety, and believe that adults are somewhat hysterical in their fears of the Internet. Nevertheless, they put themselves at risk and are quite naïve about the dangers.

Parents, and to a lesser extent teachers, feel overwhelmed and ignorant about what's going on in social networking sites, chat rooms, online gaming and other areas in cyberspace. Teachers believe parents should take a lot more responsibility for their children's behaviour (both online and offline). Parents (and teachers) would like to know more about the virtual spaces young people inhabit, but don't know where to start. Both groups believe their ignorance has led to an unhealthy power shift, so that young people are too easily able to operate 'under the radar', or outside the usual boundaries governing their behaviour.

Most understood that ultimately it is not the technology itself but behaviour that is the issue.

All forms of bullying can lead to poor outcomes for many of the young people involved both those who are victimised and those who take part in bullying others. In some cases, these negative effects have been shown to persist in later life. Cyberbullying, now seen as an aspect of the larger picture of covert bullying has the potential to result in more severe psychological, social, and mental health problems than overt bullying (Cross, et al, 2009), problems that are not only more difficult for schools and parents to detect, but which have the capacity to impose social isolation much more broadly.

Young people who are victimised have a higher likelihood than do other young people of experiencing adverse health outcomes (Rigby, 2005, McGrath, 2006) and social adjustment health problems. Young people who engage in repeated bullying are more likely to engage in ongoing anti-social behaviour and criminality, have issues with substance abuse, demonstrate low academic achievement and be involved in future child and spouse abuse. Both victimised young people and those who take part in bullying across time may demonstrate lower levels of academic achievement than expected (McGrath et al, 2005).

Lesbian, gay and bisexual young people tend to be disproportionately victimised relative to their heterosexual peers, as a direct result of the ignorance, fear and prejudice that surrounds them. Homophobic bullying tends to be systematically carried out by large groups of young people rather than individuals. Lesbian or bisexual adults who were bullied at school have identified very negative mental health outcomes from those experiences; in the short term, alcohol abuse and drug use self-harm, and in the longer term, high rates of suicide and suicidal thinking, (McGrath et al, 2005).

The aspects of cyberbullying that most affect young people are the viciousness of much of the bullying: they often do not know the identity of the person or persons who are bullying them, the public humiliation of having images of them posted on the internet and their seeming inability to escape it. No one seems to be available to help them, and they are worried that their parents and teachers will find out, adding to the public humiliation. They are also concerned that in the effort to protect them, adults will remove their access to technology.

The relationship of bullying to cyberbullying is integral – we see cyberbullying as bullying through technology – and is to do with behaviour rather than applications. It 'mirrors and magnifies' traditional bullying often with severe effects to the mental, social and academic wellbeing of the young people concerned.

It is our view that responses to cyberbullying are best focused on behavioural change in the school and beyond. They are most effective when developed collaboratively and involve school personnel, parents, young people, the internet industry and the wider community.

Each of these groups needs guidance, knowledge and support about their roles and responsibilities in this area. Schools need guidance about their duty of care in addressing bullying and cyberbullying, both on and off school property. To date, little professional training in understanding or dealing with cyberbullying has been delivered, and while this is changing (ACMA has an excellent outreach learning program) this remains an area to be remedied. Many parents still have little understanding of their children's approaches to and uses of communications applications, although this too is changing. The internet industry has a strong role to play in addressing cyberbullying, and strengthening user protections through agreements with Internet Service Providers is a key way this group can help protect children and young people in the online environment. Easily accessed and clear information for children, young people and adults, about safety, privacy settings and how to seek help should be provided by technology providers involved in providing access, and content, including search engines, social networking sites, chat room or blog facilitators, and game sites. Up-to-date plain language information needs to be developed for parents and other community members about the protection of young people and distributed widely in translation.

There needs to be greater coordination of anti-bullying and anti-cyberbullying initiatives.

Online sexual exploitation of young people – cyber-stalking and sexual grooming

The sexual abuse and exploitation of children is an abhorrent and heinous crime. Children, because of their incomplete social and emotional development, have always been at risk of being the prey of older people with a pathological interest in them, and in some cases because young people inherently engage in inherently risky behaviour. Children with 'low self-esteem, lack of confidence and naivety are more at risk and more likely to be targeted by offenders. Sexually curious adolescents … are also more willing to take risks than less-curious children, thus making them a target for predators' (Choo, Kim-Kwang, 2009).

Offenders no longer have to move into a suburban street or assume a position of authority in the community to gain access to a child. Offenders also no longer work from a blank canvas because personal information is easily found in online spaces, thus often don't have to look for long to find a target.

Child grooming is a calculated behaviour, which aims to set up a relationship with a selected child through demonstration of particular interest in them and development of trust over time. Once trust is gained, the sexual agenda is introduced. This is made easier by young people's extensive participation in the online environment: in a 2009 ACMA study, at ages three to four 40% of children

were shown to be computer users, a figure that rose to 88% in the 15-17 age groups (AMCA 2009).

Online predation of children and young people is now recognised as a Serious Organised Crime. With the advancement of network capabilities, wireless and mobile technology, Global law enforcement (Virtual Global Taskforce) understands that crime syndicates operate across borders to groom children and offend against them both for financial gain (creation, production and distribution of images) and for sexual gratification. These two prime reasons for offending are often blurred and not widely seen in isolation.

Children who are groomed through social networking sites, chat rooms, blogs or other means using technology are at particular risk because inappropriate contact can be made by older teenagers or a predatory adult pretending to be a person of the same age. Online users can assume any identity, wearing any mask they like. The virtual world is perhaps the largest and most dynamic playground that exists. Unfortunately, the online spaces in which children and young people naturally engage are also ones to which offenders will gravitate.

Some websites, designed to attract young people ask for their personal details and a photo before they can begin using the application. Often this information is defaulted to being 'public' and privacy settings are hard to find and complicated to manipulate for many users. Predators use this publicly available information to engage in personal contact as they begin the grooming process. Technology has not substantially increased the number of paedophiles but it has certainly sped up the grooming process and the geographical reach and intensity of sexual exploitation. In a recent case in Victoria, a man was arrested and questioned over sexual assaults of five teenage girls, some as young as thirteen, whom he befriended on social networking sites. His method, it was alleged, was to befriend them, film them via webcam in compromising poses before blackmailing them into a range of activities including rape, indecent assault, stalking, making child pornography and making threats (News.com.au April 1, 2010). This particular case typifies the grooming process identified by sexual exploitation units in both Australia and internationally.

The degree to which children are targeted for online sexual purposes is difficult to determine because of its illegal nature and the secretive behaviours of both perpetrators and victims. Child victims are unlikely to report for the same reasons they do not report bullying: shame, fear that adult intervention will make the problem worse or that their access to favourite applications will be removed.

Choo (2009) cites a study in which it was shown that people who post photos of themselves and have profiles on social networking sites are more likely to be contacted by people they do not know offline and, if factors are constant, girls more than boys. The figures for young people (10-17) who have been exposed to unwanted sexual material are drawn from studies from overseas (Wolak, Mitchell and Finkelhor, 2006, US Internet Safety Survey 2006 and others).

Choo cites a study by Ybarra, Espelage and Mitchell (2006, pp 22, 23) in which, a survey of 1588 youths aged between 10 and 15 found the following:

Internet harassment or unwanted sexual solicitation

- 35 percent reported being the victim of either internet harassment or unwanted sexual solicitation
- 21 percent reported perpetrating either internet harassment or unwanted sexual solicitation internet harassment only

- 34 percent of all youth reported being the victim of internet harassment at least once in the previous year while eight percent reported being targeted monthly or more often
- 21 percent reported perpetrating internet harassment of others at least once in the past year and four percent reported doing so monthly or more often

Unwanted sexual solicitation only

- 15 percent reported being victims of unwanted sexual solicitation at least once in the past year and three percent reported at least once a month or more often
- 3 percent reported perpetrating unwanted sexual solicitation of others in the past year and one percent reported doing so monthly or more often.

This group also displayed many physical, behavioural and psychological problems.

Choo cites clear evidence from the academic literature that sexual abuse during childhood 'creates long-term problems for those who have been victimised. Many exhibit serious mental health problems as well as behaviour disorders and addictions. This occurs not only with children who experience offline sexual abuse, but also online exploitation' (Choo, 2009, xiv). These problems include alcohol and drug misuse, particularly in adult males as well as post-traumatic stress disorder, anxiety and substance abuse.

The Office of the Child Safety Commissioner (Victoria) cites effects including cognitive disorders, emotional pain, avoidance behaviours, low self-esteem, guilt, self-blame, self-harming behaviours, delinquency, substance abuse, vulnerability to repeated victimisation, interpersonal difficulties, dissociation and disbelief about the abuse, functional amnesia and effects on relationships with others (Calmer Classrooms, 2007). These can affect a young person's ability to experience success at school, either by the effects the abuse has had on the cognitive capacity of the child, or, exclusion from school due to extremely challenging behaviours. As can be seen the effects are long lasting and for many, the damage is permanent.

Young people are often unaware of the offline consequences of their online actions. Adolescents who are vulnerable for a variety of reasons and who may be having trouble at school or at home tend to engage in the most serious risk-taking online. They are the group that is the least likely to self-protect online by guarding passwords, or showing caution in posting pictures and so forth.

Exposure to illegal and inappropriate content

Online or mobile content is unrestricted by age. It is a real concern that children and young people may be exposed to a range of age-inappropriate or illegal content or sites, including sexual, violent, racist, and hate content, as well as misinformation or other problematic content.

Sexual content may include legal adult pornography, illegal child abuse or self produced 'sexting' images and other inappropriate images, video or audio files. While the likelihood of stumbling across child abuse images is relatively low, these images are deliberately sent as part of the 'grooming processes' to normalise sexual behaviour. On the other hand, very graphic adult pornography is easily accessed and often free. While young adults have viewed pornography in 'magazine format' for decades, at no other time have we experienced such heightened access to pornographic material.

'Sexting' is the sending of nude or partially nude or inappropriate images and is very prevalent amongst both children and young people. Often a young person will take an image of themselves in the hope of impressing a boyfriend or girlfriend. When that relationship deteriorates, this image may be posted online, used to cyberbully or end up in the offenders' abuse collection.

Sexting legislation needs to be addressed. Currently, most states in Australia can use child abuse legislation to prosecute regardless of age, on the grounds of production and distribution of images. This can mean young people may have a criminal record and in a worst-case scenario, although unlikely, find themselves on the sex offenders register.

Illegal material is also often accessed accidently via the downloading of illegal music or video content via bit-torrent/ file sharing websites like Limewire and Torrent Man. Children and young people with limited funds use these websites to download their favourite band's music, movies and television shows rather than paying for them on legal sites like iTunes. Often these files have attached viruses or are simply labelled wrongly and are in fact pornographic or inappropriate images or videos.

Cyber-racism is a term used for racism on the internet. Racist acts are those that are 'reasonably likely, in all circumstances, to offend, insult, humiliate or intimidate people on the basis of their race, colour or national or ethnic origin'. Cyber-racism includes racist websites, images, blogs, videos and comments on web forums. (http://www.hreoc.gov.au/racial_discrimination/publications/cyberracism_factsheet.html).

Hate sites like that of holocaust denier Fredrick Töben can be charged under the Racial Discrimination Act, using the argument that such sites are a form of publishing and subject to the same rules (Norris, et al, 2005). Hate crimes are not subject to separate legislation in Australia. However, whether use of the internet by extremists translates into actual (offline) behaviour is not known. 'Attempting to completely eradicate all hate material would be seemingly an impossible task and neither is it a panacea for eradicating hate crimes and racism' (Norris, et al, 2005). Definitions of what constitutes a hate site can also be subjective.

The use of values-based material, which stresses inclusivity, and acceptance of difference will probably be an effective way of addressing many of these sorts of websites. Internet providers also have an important responsibility to respond rapidly by removing offensive material or that which is intended to incite hatred. A unified legislative response across the states and territories will prevent perpetrators seeking the least restrictive environments in which to operate.

Inappropriate social and health behaviours in an online environment (e.g. technology addiction, online promotion of anorexia, drug usage, underage drinking and smoking); Identity theft; and breaches of privacy;

Another content risk for children and young people are sites advocating for a range of unhealthy life choices, including pro-anorexia (pro-Ana) sites. A quick search brings up dozens of such sites, many of which offer 'thinspirational' tips such as 'creeds', motivation, tips and tricks and advice on how to stay thin. Pro-suicide websites contain more than detailed information on how to commit the

act: many incite the reader to 'end the pain' to 'achieve the bliss of death'. Others hector and harass the reader by telling him or her how worthless is their life, and how worthwhile it is to end it.

Open-question forums provide a range of advice from bloggers on subjects such as whether to take drugs while still at school and elicit responses such as this: 'started doing weed when i was 14.. started missing school by.. well a few weeks later.. and i left at 15, but i got a good job straight away and im 16 soon enough so i'd say do it haha', posted on a Yahoo 7 forum on 10/5/2010. (http://au.answers.yahoo.com/question/index?qid=20100509231241AAC1cU3).

How many children and young people access such sites? We don't know. A study published in the 'British Medical Journal' found that people searching the web for information on suicide are more likely to find sites encouraging the act than offering support. Researchers used four search engines to look for suicide-related sites. The three most frequently occurring sites were all pro-suicide while sites focusing on suicide prevention accounted for 13 percent, and those discouraging suicide accounted for 12 percent (http://news.bbc.co.uk/2/hi/health/7341024.stm).

The report shows the ease of obtaining detailed technical information about methods of suicide. The risk for vulnerable young people is their lack of an analytical lens through which to examine the information presented. A well-publicised Melbourne case of two young girls who hanged themselves after having accessed a pro-suicide website drew attention to the problem of vulnerable young people who lack social support accessing material of this kind. "The internet is a powerful new medium where marginalised young people at the risk of suicide who might not otherwise meet are able to come into contact. It's providing content such as graphic self-harm sites, which are potentially very dangerous to a lot of these young people. I think we have a real problem," (Professor of adolescent health at the Royal Children's Hospital, Melbourne) (http://www.theage.com.au/news/national/lost-in-cyberspace-fears-over-teen-sites/2007/04/23/1177180567880.html?page=fullpage)

Increasingly concerns have been raised about the normalisation of unhealthy attitudes and behaviours through the online medium.

Many children have unrestricted access to violence on the internet, through a variety of media, including videos, and violent games. Recent studies show that increased access to violence normalises this behaviour within young people's social groups and can in a minority of cases lead to increased levels of violent behaviour.

A statistical analysis of studies on more than 130,000 young gamers in the US, Europe and Japan 'strongly suggests' playing violent video games increases aggressive thoughts and behaviour and decreases empathy particularly when accompanied by other risk factors. Centre for the Study of Violence at Iowa State University in Ames (Carnagey, et al, 2005).

Young people are also exposed to highly sexualised images of peers on social networking sites, which can, in some cases, provide an example influencing them to post inappropriate and sexualised images of themselves. Recently, more than 30 of Australia's leading child experts called for an ban on the sale of adult magazines and other 'soft porn' material from newsagents, milk bars, convenience stores, supermarkets and petrol stations. The group has also asked Australia's censorship ministers to review the rules by which so-called 'lad mags'

are reviewed, arguing that they are becoming increasingly explicit and contributing to the sexualisation of children.

A number of companies now routinely review a potential employee's online history, particularly on facebook and other social networking sites, and use this information as part of their decision making in the recruitment process. Because of permanent records or the 'digital footprint' that young people leave on the internet, naïve and inappropriate postings may have a long term and detrimental effect on a young person's life.

Internet addiction - is there such a thing?

While there is a large commentary on internet addiction in the media, it is nevertheless valid to ask the question; does internet addiction exist? The following discussion is drawn from The Alannah and Madeline Foundation's Literature Review for the Cybersafety and Wellbeing Initiative (2009).

Young (1998) originally proposed the term 'Internet Addiction Disorder' and developed the Diagnostic Questionnaire for Internet Addiction (YDQ) which she adapted from the criteria outlined in the DSM IV (APA, 1994) for 'pathological gambling', which is cited in the DSM IVTR as an example of an Impulse Control Disorder. Although a small number of writers and researchers (the commentary particularly from writers in China, Taiwan and Korea) claim that this is an identifiable behavioural syndrome, there is neither sound research evidence nor convincing theoretical support for such a syndrome at this time. It has been suggested that 'internet addiction' is a term that has been promoted and sensationalised by the media but so far has little clinical validity

There is no official psychological or psychiatric diagnostic syndrome called 'Internet Addiction Disorder'. The most recent edition of the Diagnostic and Statistical Manual of Mental Disorders, DSM-IV-TR (APA, 2000), does not include such a diagnostic category. The DSM IV is published by the American Psychiatric Association (APA) and provides diagnostic criteria for mental disorders/ syndromes. It is used extensively around the world as the diagnostic 'bible' by clinicians, researchers, agencies that regulate psychiatric drugs, legal systems and health insurance companies. The research and theory for all of both proposed and established disorders are continually monitored by the APA and each new version contains some deletions, revisions and additional disorders. The next version (DSM-V) is due for release in 2012. 'Internet Addiction Disorder' could only be accepted as a disorder if research was able to demonstrate that such a syndrome can be reliably measured and established as significantly different from existing disorders, and that the diagnosis has external validity in that it reliably correlates with treatment outcomes, case histories and prognosis.

The following are some of the difficulties with the concept of 'Internet Addiction Disorder':

- Sound published studies on internet addiction from Western countries are scarce. The majority has been conducted by Chinese and Korean researchers, perhaps reflecting the publicised concerns in those countries about what has been described as excessive use of the internet (mainly for online gaming purposes) in the millions of very large internet cafes that have been established. For example in August 2005, the BBC reported the death of a young Korean man who had continuously played online games in an internet café for 50 hours, neglecting to eat, drink and sleep. Most studies are based only on surveys, using self-selecting samples but no control groups. Some of the other published papers on internet addiction

are theoretical papers that speculate on the philosophical aspects of internet addiction but provide no data (De Angelis, 2000).

- There certainly have been speculations that some of the unique aspects of the internet may lure people into difficulties they might otherwise avoid such as online gambling, accessing of pornographic sites and the development of inappropriate sexual relationships ('cyber-affairs'), online auctions and online shopping. However it isn't enough simply to describe an activity that people can spend too much time on, or engage in to excess on occasions as an 'addiction'. Different researchers in each country have developed their own scales and there are at least five different scales available.

- There is no research evidence that a passion for the internet is long lasting or that excessive internet usage is not simply a reflection of a problem such as social phobia or loneliness.

- Many of the strongest proponents for establishing that the category of internet addiction does exist separate from other disorders have some commercial interest in doing so. For example Kimberley Young (1998), who first proposed the disorder and developed the first questionnaire, runs a private centre to treat excessive internet usage and train others to do so (http://www.netaddiction.com).

- Dr Jerald Block, an American psychiatrist who is one of the strongest advocates for the inclusion of Internet Addiction Disorder in the next version of the DSM also disclaims that he "…owns a patent on technology that can be used to restrict computer access" (Block, 2008). Greenfield (1999) surveyed 18,000 internet users who logged onto the ABC News Web site and found that 5.7% of the self-selected respondents met the supposed criteria for compulsive internet use but he has also for some time, run a private centre, which provides treatment and training (www.virtual-addiction.com).

- Several Chinese, Taiwanese and Korean researchers who have surveyed young people (mostly aged 12-18) using one of the many questionnaires that purport to measure internet addiction have found some interesting co-occurring behaviour patterns. Their results suggest that those young people whose scores on these various tests suggest they are 'addicted' to the internet have a range of other symptoms as well. In particular a pattern emerges in which those with supposed internet addiction also have scores on other measures which suggest they also have symptoms of ADHD, show high levels of impulsiveness, social phobia, hostility, depression, hyperactivity and emotional problems, and lack pro-social behaviour (e.g., Cao et al., 2007; Yen et al., 2007; Yoo et al., 2004). Yen et al. (2007) conclude that many of these characteristics (e.g., depression) are the result of internet addiction. Yoo et al. (2004) have suggested that some of these characteristics may be risk factors for internet addiction while Cao et al. (2007) argue that such characteristics may indicate the presence of psychiatric disorders which are co-morbid with internet addiction (i.e. they occur simultaneously but are not necessarily related to each other). However, it makes more sense to assume that excessive internet usage may be a symptom of disorders that are already included in the DSM IV –TR such as ADHD, Social Phobia or Depression.

At a later point, 'excessive internet usage' may be given as an additional example of an Impulse Control Disorder. This disorder already exists in the DSM IV-TR and currently includes examples such as compulsive gambling, pyromania, trichotillomania (hair pulling), gambling, kleptomania & intermittent explosive disorder (in which the person has outbursts of uncontrollable rage). Impulse control disorders sometimes have characteristics that are also common in other disorders and often occur in conjunction with other conditions, such as ADHD or conduct disorder (Sisk, 2006).

Identity theft and breaches of privacy

We increasingly live in a society where online users are forced to enter their personal data to access services, purchase goods or interact with one another. Nothing online is private and in fact every keystroke leaves a digital footprint. Law enforcement agencies find this digital footprint useful and increasingly use it to track arrest and bring offenders of many persuasions to account.

However, in 2009, Australians lost more than 70 million dollars to identity theft. Previously, for someone to steal an identity they would have to break into your home, steal your wallet, medical records and access your bank account information from statements thrown out with your rubbish. Now we are facing unprecedented virtual attacks on our identity. These virtual attacks to access personal information are predominantly coming from off shore professional hackers, where Australian law enforcement finds it harder to prosecute, and can be from as remote locations as North Korea and Russia.

Organised crime networks exist that employ rooms full of hackers to seek personal information to sell, or manipulate, for financial gain. This funds other crime, such as conventional terrorism. Virtual thieves obtain personally identifiable information through a number of different avenues and identity theft is a primary risk for all Australians, young and old, when they use connected technologies. Both businesses and individuals are targeted in the pursuit of these data. Australian adults are largely at risk of identity theft, and research indicates they are often unaware of where the dangers exist and do not protect themselves adequately. Australian businesses are often vulnerable to attack through the inadvertent actions of staff members. Small businesses, without dedicated ICT resources or adequate expertise are often targeted and unaware their data has even been obtained by a hacker.

When young people create personal profiles online, they often include identifiable information like their full names, date of birth, hometown, school, relationship status, sexual preference, mobile numbers and email addresses. PEW research on American teens showed that 82% of teens with online profiles post their first name, 79% a photo of themselves, 61% their city/town name, 49% include the name of their school and 29% their last name (Wallbridge, 2009). Wallbridge suggests that posting of personal data has become normal in order to gain access to online services.

Information stolen from young people is typically facilitated by their imprudent posting of personal data such as names, email addresses, photographs, school attended and so forth on social networking sites. Sharing of passwords with friends is a very common way young people compromise their security, but the use of weak passwords, predictable password re-set questions as well as computer hacking and different forms of spy and malware are also common means by which identities are stolen and privacy breached.

Bluesnarfing (the unauthorised access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops and PDAs) allows access to a calendar, contact list, emails and text messages.

Prevalence of identity theft among young people is difficult to establish, as most does not involve criminal activity as such. Indeed a recent ACMA study suggests that young people have 'a high level of awareness of the risks of Internet use particularly when involved in social networking on the Internet'.

Privacy is a notion that does not technically exist in the online environment. If a technical system can be built by developers, it may be broken by hackers. However, privacy or the lack of privacy affects the average online user when information is shared and an embarrassing or unflattering incident occurs.

A common complaint in relation to social networking sites is the difficulty of controlling personal information and adjusting the privacy settings. With the growing awareness of the importance of protecting personal information comes an increased expectation of user control over how much other people can view of their digital footprint.

iii. Australian and international responses to current cybersafety threats; their effectiveness and costs to stakeholders, including business

- **Education**

If we look towards the United Kingdom, which has perhaps the most robust cybersafety and cyberbullying education campaign, we can see the British Home Office have achieved good results in tackling the issue. They have raised awareness of the issue through multifaceted media campaigns that harness the power of industry. They have also mandated school policies and procedures through the Federal Department of Education (DCSF), embedded targeted resources in the school curriculum, and run professional development through local education networks. The UK is also currently looking to reform legislation in relation to cyberbullying.

The Northern Hemisphere (European Parliament, Canada and the United States and Interpol) looks towards the UK as the leaders in cybersafety and cyberbullying education reform, and partner closely with UK law enforcement to bring offenders to account. Media scrutiny and an established Home Office committee also hold industry more accountable, asking them to play an active role in promoting cybersafety messages.

New Zealand's leading cybersafety agency Netsafe has also moved away from offering 'one off' school programs and is embedding these resources in the curriculum, as well as providing professional development, partnering with parents and the wider community, and ensuring a minimum standard of policies and reporting procedures exist in all NZ schools.

Both NZ and the UK are fortunate to exist under one federal government, enabling a cohesive response, rather than state-based agendas. Australia also requires a consistent federal response to both cybersafety and cyberbullying issues.

Australia's cybersafety education arena has many good stand-alone education resources and programmes targeting Australian schoolchildren. Interestingly more than 1.6 million young Australian's have received cybersafety lessons in the classroom, but the incident rates of cyberbullying, sexting, identity theft, privacy breeches and sexual exploitation continue to rise. What is needed is more than 'one-off' programs. Theory and evidence from Health Promoting Schools literature, and experience from successful behaviour change programs such as SunSmart, shows the most effective approaches to behaviour change involve a multi-layered strategy that goes beyond the provision of information or curriculum.

Australia does not currently have in place a strategic cybersafety / cyberbullying behaviour change model that intersects with the education sector. What is needed is an approach that recognises the importance of building young people's skills for protecting themselves and for being responsible online citizens, but also looks to systemic change in school environments to support cybersafety. Existing evidence-informed information resources and programs should be embedded within the school curriculum, teaching staff require compulsory professional development, parents and the wider school community need to be informed and brought into policy decisions around ICT use and all schools need robust reporting procedures. Moreover, schools need to make the links between cybersafety and

wellbeing, and understand the importance of creating a caring and respectful school culture where bullying and cyberbullying are not tolerated.

eSmart is a world-first approach to cybersafety. The *eSmart Schools Framework* is a proactive and strategic response to these and other cybersafety concerns facing schools throughout Australia. The Initiative is a broad social change approach, acknowledging that cybersafety is the responsibility of the whole community. The Foundation is confident that the initial phase of the approach should have schools at its centre, employing community awareness-raising and education strategies. At the heart of this approach is the need to work systematically with young people, teachers and parents to increase awareness, knowledge and skill in a suitable environment.

The focus of the Initiative is to create a cultural norm of smart, safe and responsible use of communications technologies within the Australian community.

- **Filtering**

Home level filtering is not often applied, despite the widespread availability of filtering systems. When it is applied, there is a risk of parents/carers being given a false sense of security about their children's access to inappropriate content or risk of being contacted by online strangers, thereby encouraging them to think they can leave their children to go online unsupervised. This is concerning and should be addressed when considering the roll-out of both filtering at an ISP level, and when the Federal Government offers free filtering software to Australian families.

Software cannot replace the eyes and awareness of an engaged parent or carer.

- **Regulation**

'Safer by design' is the term used when industry is asked to create safer products and systems for the online user before the product or service is released. Age-authentication of a user and the release of content currently poses several 'safer by design' challenges and is a key area that requires the attention of both industry and government. To move forward responsibly in this virtual space governments and industry need to follow the example set by law enforcement and collaboratively tackle illegal sites, age-authentication, geography of the user and the release of inappropriate content within that geography.

- **Enforcement**

Under proposed changes to the Sex Discrimination Act to be introduced by the Australian government, young people who have experienced cyberbullying and online sexual harassment will be given legal protection, and victims under the age of 16 allowed to use sexual harassment laws to pursue their persecutors.

While these new laws will doubtless be beneficial, particularly in the most aggressive and persecutory cyberbullying and abuse, criminal sanctions provide, at best, only part of the answer. Recent research has shown school bullying – at least face-to-face bullying - has declined over the last 10 years (Rigby, 2010) in Australia and overseas. While acknowledging that all sorts of bullying are a serious problem, we advocate seeking more collaborative solutions rather than increasingly punitive remedies.

To ensure a safe and secure environment for young people on and offline, schools must be equipped with the tools to create robust cybersafety, cyberbullying and acceptable use polices that effectively deal with and in fact prevent many incidents from occurring. It is essential that both students and parents are involved in the drafting of these policies and if legislative reform were to occur, perhaps mandating schools to create these policies and procedures would be a positive step that would not criminalise* young people but instead build a generation of smart, safe and responsible users of technology. We also advocate a system where schools can demonstrate policies are disseminated and implemented.

***See Appendix I**

iv. opportunities for cooperation across Australian stakeholders and with international stakeholders in dealing with cybersafety issues;

Many opportunities exist for Australian stakeholders to cooperate and share resources with others in the local community and with international stakeholders on cybersafety issues. Paradoxically, the technologies that have provided educators and parents with such challenges of understanding and management continue to facilitate and enhance cooperation and exchange among researchers, educationalist, developers, governments and many others.

Local and international researchers in the fields of bullying, wellbeing and cybersafety work collaboratively on a number of projects, such as the 'Insights into the Human Dimension of Covert Bullying Study', a qualitative study that used technology to explore covert bullying and cyberbullying through the voices of young people. Another collaborative project is also underway with researchers from across Australia, entitled 'Cyberbullying: An evidence-based approach to the application and reform of law, policy and practice in schools'. The *Australian Universities Cyberbullying Research Alliance* has recently been formed to highlight the collaborative work that conducted nationally and internationally and to provide the scientific evidence required to underpin policy development and the implementation of cybersafety initiatives in schools and the community.

State and National coalitions of academics and other experts such as *The National Centre Against Bullying* and the *Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools* also work in the field.

The Technology and Wellbeing Roundtable is convened by the Inspire Foundation to bring together thought leaders who work to promote evidence based and best practice approaches to young people's positive engagement with technology. There are thus extensive national and international networks and many countries working together to promote positive uses of technology and to enhance understanding of evidence based cybersafety.

The Cybersafety Consultative Working Group convened by the Australian Government with representation from community groups, internet service providers, industry associations, business and government considers aspects of cybersafety that Australian children face, such as cyberbullying, identity theft and exposure to illegal and inappropriate content. It provides advice to the Government on priorities and measures required by government and industry to ensure world's best practice safeguards for Australian children engaging in the digital economy.

The Australian Federal Police draws upon the expertise of its sister organisation the Child Exploitation and Online Protection Centre in the United Kingdom and has launched *ThinkUKnow* because of that collaboration.

The Principals' organisation represents all the education sectors—Government, Independent and Catholic, primary and secondary - and can therefore be said to represent the interests of teachers and wider school communities across Australia. National initiatives such as *KidsMatter*, *MindMatters* are managed and overseen by this body, as was the rollout of the first iteration of the *National Safe Schools Framework* in independent schools.

Industry associations such as the Internet Industry Association represent not only internet service providers but also major content platforms, search platforms and hosting platform and the new social media sites many of which support user generated content.

Safer Internet Group, which is a broad alliance of both community and industry organisations are looking to propose alternative measures to internet filtering to enhance cybersafety in the community.

On the international stage, the *European Cooperation in Science and Technology (known as COST)* has a project entitled 'Cyberbullying: Coping with Negative and Enhancing Positive Uses of New Technologies in Relationships in Educational Settings' which brings together 27 European countries and Australia to examine cyberbullying within and across national and cultural boundaries. In April this year, a related European-Australian research training school entitled 'From Research to Policy and Practice: Innovation and Sustainability in Cyberbullying Prevention' was held here in Melbourne, in order to link with the *NCAB* Conference, where some 30 European and 20 Australian researchers worked intensively over five days on issues around cyberbullying and how best to research them to promote sustainable positive outcomes for young people.

The Alannah and Madeline Foundation has integrated a collaborative process into the development of its *eSmart Schools Framework* through the formation of Reference and Consultative Groups, bringing together experts in the areas of technology, education and cybersafety.

While these are positive developments, there is still insufficient collaboration in research and development activities and much duplication of research, pointing to the need for increased effectiveness in international cooperation and dissemination of materials.

v. examining the need to ensure that the opportunities presented by, and economic benefits of, new technologies are maximised;

The Australian Government recognises the importance of technology in the classroom. Substantial resources through the *Digital Education Revolution* initiative have been provided to professionally develop and support teachers, and acknowledge and build Australia's participation in a globalised world.

The Digital Education Revolution

The aim of the *Digital Education Revolution (DER)* is to contribute sustainable and meaningful change to teaching and learning in Australian schools that will prepare students for further education, training and to live and work in a digital world. Through the DER, the Government is providing $2.2 billion over six years to:

- provide for new information and communication technology (ICT) equipment for all secondary schools with students in years 9 to12 through the *National Secondary School Computer Fund*
- support the deployment of high speed broadband connections to Australian schools
- collaborate with states and territories and Deans of Education to ensure new and continuing teachers have access to training in the use of ICT that enables them to enrich student learning
- provide for online curriculum tools and resources that support the national curriculum and specialist subjects such as languages
- enable parents to participate in their child's education through online learning and access
- support mechanisms to provide vital assistance for schools in the deployment of ICT.

In the future, schools will have a stronger role to play in preparing students for a digital world - both in and out of the classroom. It will be incumbent on them to implement policies and practices to ensure that the whole-school community is aware of leading cybersafety practices.

Increased access to digital technologies because of the Commonwealth Government's *Digital Educational Revolution* and roll-out of the *National Broad Band Network* brings enormous benefits to young people. However, it also brings with it increased risks and a national approach to cybersafety to mitigate these risks should be implemented.

vi. ways to support schools to change their culture to reduce the incidence and harmful effects of cyberbullying including by:

- **increasing awareness of cybersafety good practice;**
- **encouraging schools to work with the broader school community, especially parents, to develop consistent, whole school approaches; and**
- **analysing best practice approaches to training and professional development programs and resources that are available to enable school staff to effectively respond to cyberbullying;**

The recent *National Centre Against Bullying (NCAB)* conference in Melbourne (April 2010) focused on cybersafety and wellbeing (Navigating the Maze: cybersafety and wellbeing solutions for schools), attracting international delegates and presenters, with 400 delegates from across the world.

The conference developed 10 key action statements to which the participants pledged their ongoing commitment (see recommendations, P 3).

Cyberbullying (as discussed earlier in this submission) is generally considered a subset of bullying: often now, we speak of online and offline bullying. Bullying itself indicates a breakdown in relationships. Because it occurs in specific social contexts, it is often complex to manage in schools and other environments, including sporting clubs, workplaces and the home.

Schools are guided in their management of all kinds of bullying by the development and implementation of an anti-bullying, or by an overall wellbeing policy. To ensure shared understanding of terms and consistency of application, policies should be developed in collaboration with members of the wider school community (including parents, students, community members as well as leaders and teachers), revised regularly, supported by clear procedural guidelines and communicated regularly.

This policy should support other policies and approaches used within the school, including the explicit teaching of values, rights and responsibilities and citizenship, and consistent use of appropriate techniques for behaviour management (such as restorative justice, method of shared concern, and support group approach, with more limited application of punitive approaches).

There is quite wide insistence through State and Territory educational jurisdictions that schools have cyberbullying policies and acceptable use of technology agreements in place; however, implementation of these policies across states and territories is inconsistent.

The Alannah and Madeline Foundation believes that, to be effective over time, schools' initiatives to increase cybersafety and reduce cyberbullying must be aligned with evidence-informed efforts to increase the overall wellbeing of all members of the school community as a foundation for learning and citizenship. In addition, there needs to be a range of interventions in place to drive change in schools that will reduce cyberbullying and other types of bullying. These include

- support and professional development for teachers in behaviour management, bullying/cyberbullying, cybersafety, and in the use of technology to support the development of peer relationships within and beyond the classroom

- systemic processes of induction for all staff, students and their families in the expected behaviours, policies and procedures for complaint and resolution of incidents

- sustained teaching of cybersafety principles, with relevant content embedded in many parts of the curriculum

- opportunities for students to showcase and exchange their knowledge of Web 2.0 technologies, and also the management of risk in cyberspace

- involvement of parents/carers in the effort to minimise cyberbullying and other cybersafety risks

- a mechanism to support and monitor schools' implementation of the suite of interventions required to achieve cybersafety.

The school leadership team has a vital role in creating and maintaining a respectful and caring school culture that is modelled by teachers in their interactions with each other and students; students are quick to see when words and deeds are inconsistent, and when policies are in conflict with observed behaviour of leaders and teachers.

For schools to achieve these goals, it will be necessary to provide significant support, including, but not limited to, adequate professional development, both holistic and targeted. By this, we mean that whole school communities will need information in order for messages to be consistent across their stakeholder groups. Schools can become a significant conduit of cybersafety messages and principles to parents and their whole school communities. In addition, particular individuals in the teaching staff will need to be up-skilled in ways to use technology for instruction.

The Alannah and Madeline Foundation's *eSmart Schools Framework*

The Framework provides a consistent and practical whole-school approach for the implementation of evidence-informed cybersafety programs and practices. It is a culture and behaviour change model targeted at the whole school community - and as such, is not a one-off lesson, unit of work, program or policy that sits in isolation from the day-to-day business of schools.

More specifically, it aims to:

- Integrate cybersafety with schools' current knowledge and practices about wellbeing (including policies such as the National Safe Schools Framework)

- Assist schools to develop more effective curriculum around cybersafety and wellbeing and the smart use of technologies

- Help to up-skill teachers in smart, safe and responsible use of technologies

- Assist school communities in developing safe and supportive schools where bullying and violence are minimised and the values of responsibility, resourcefulness, relationships and respect are fostered in cyber-space

- Assist schools in becoming cyber-safe.

The *eSmart Schools Framework* supports exploration of:

- protective behaviours
- supportive and relationship building behaviours
- reporting of incidents.

The *eSmart Schools Framework* embraces:

- whole-of-school wellbeing issues including values/relationships/self-esteem
- e-security
- ethics including downloading and plagiarism
- criminal activity including sexual harassment and predation.

The Framework is underpinned by the positive embrace of ICT and the promotion of smart use of technology.

The *eSmart Schools Framework* is designed to:

- Help schools develop policies and practices (that are developed with input from students and parents) encouraging students to use technology responsibly and respectfully

- Point schools to high quality teaching resources on cybersafety and those which help create a safe, respectful and caring environment

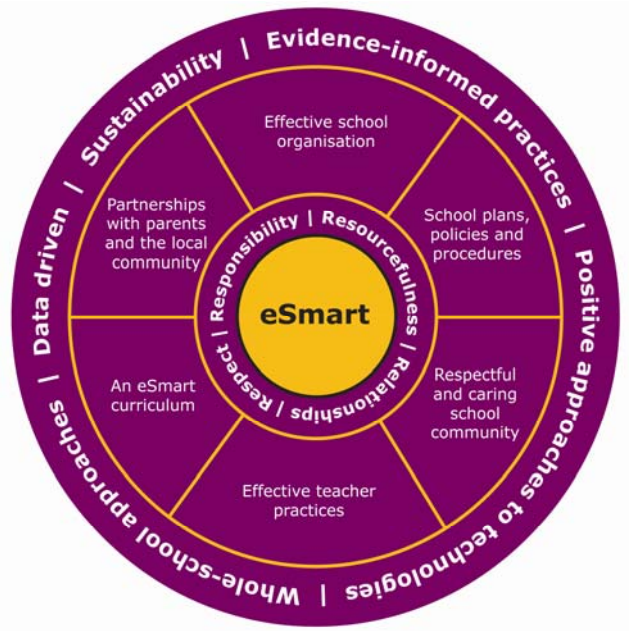
- Encourage schools to embrace the positives of internet and communications technology within their teaching practice to enhance learning

- Establish a system for schools to provide evidence that they are actively implementing these policies and practices

- Help reduce the digital divide between adults and young people, so adults can become a credible source of advice on avoiding the risks of cyber-space.

The major mechanism for delivery of the *eSmart Schools Framework* into schools is an interactive website. Schools are further supported by other resources such as a welcome kit, newsletters, a Help Desk as well as training in using the *eSmart* system.

The eSmart Schools Framework



Schools complete activities in six Domains to demonstrate that they have achieved *eSmart* status. These are:

- Effective school organisation
- School plans, policies and procedures
- Respectful and caring school community
- Effective teacher practices
- An *eSmart* curriculum
- Partnerships with parents and the local community.

When all six Domains are taken together, they represent a whole-school approach that is capable of transforming the way that schools work with, offer, teach and think about internet and communication technology. Most importantly, the six Domains create a consistent and common language that can be used by the whole school community to reinforce positive cultural change.

eSmart Schools effectively assists schools to find the best and most appropriate programs from a vast quantity and quality of implementations, books, websites, e-technologies software and more, competing for schools' money and time. Schools are able to access quality resources through the *eSmart Schools* website that relate specifically to activity in the different Domains. These are updated constantly, and presently, the excellent resources developed by the Federal Government and State and Territory jurisdictions are being mapped to activities schools are expected to complete.

The Alannah and Madeline Foundation has put in place staff and processes for keeping up-to-date with current best practice and new evidence in the area of cybersafety and especially cyberbullying. *eSmart Schools* will be regularly updated to reflect new knowledge and will point to new, high-quality programs and resources for schools.

eSmart Schools is more than a one-stop source of information and resources for schools - it is designed to drive implementation of cybersafety. Schools provide proof of their achievement of set milestones to attain recognition of their cybersafety and wellbeing practice, and must regularly re-apply for retention of their *eSmart* status. Importantly, the Framework ensures that schools take a holistic approach to embedding cybersafety and positive school culture.

The Department of Education, Employment and Workplace Relations provided $3mil to the Foundation in June 2009 for a National Pilot of The Cybersafety and Wellbeing Initiative and its *eSmart Schools Framework*, involving over 150 schools across Australia. This Pilot has just concluded, and was independently evaluated by Prof Donna Cross' team at the Child Health Promotion Research Centre at Edith Cowan University with very positive results

The need for mass communication campaigns to promote school-level action on cybersafety.

Effective social change requires many interventions across the whole spectrum of the community. The best social change campaigns have been intricately tied to a range of actions that change the way things are done within organisations and community settings through policy and practice changes, as well as regulation, enforcement, and communication. Well-known examples include the long-running tobacco control and the SunSmart campaigns, as well as WorkSafe and the TAC campaigns.

Before we can achieve behaviour change we have to address the systemic changes needed on the ground, but it is also important to communicate widely to raise awareness, increase knowledge and to shift attitudes.

The Foundation believes that *eSmart* can drive the systemic changes needed within schools but that its effect will be greatly enhanced by a supporting communications campaign.

Designing the Framework

The design of the *eSmart Schools Framework* was informed by:

- an international literature review on technology and young people by Adj. Prof. Helen McGrath of RMIT University's School of Education
- a needs analysis in relation to cybersafety and wellbeing knowledge, resources and practice in 400 schools Australia-wide, conducted by the RMIT School of Education, Consultancy and Development Unit
- the body of existing knowledge about how to generate long-lasting behaviour/cultural change
- the body of research available on cybersafety, bullying and cyberbullying.

Australia has led the way internationally in many behaviour/cultural change initiatives. The effectiveness of multidimensional, mass reach strategies underpinned by research, policy and practice frameworks is clearly established.

Social change approaches adopt strategies that shift societal norms and other environmental factors to bring about large-scale behaviour change. They consider

communities, organisations, policies, laws, and popular culture, as well as individuals in a variety of settings including schools. There is an excellent body of evidence to indicate that the Foundation's approach to cybersafety and wellbeing will be successful in safeguarding Australia's young people against real and potential risks faced in cyber-space.

In addition to drawing on the evidence as described above, broad consultation with education and industry stakeholders was also undertaken.

This wide engagement with schools and the other stakeholders ensured the content made available through the *eSmart Schools* website met schools' requirements. It also ensured the Framework complemented and even enhanced current school policies and practices, was user-friendly, likely to be accepted by schools, was an appropriate approach to cybersafety within schools and guided schools to resources that would keep them at the forefront of current knowledge in cybersafety and wellbeing for their school community.

The Foundation is supported in this by the *National Centre Against Bullying (NCAB)*, a peak body made up of experts and chaired by Alastair Nicholson AO RFD, QC, former Chief Justice of the Family Court of Australia. The Foundation also convenes Consultative and Reference Groups made up of education sector representatives from wellbeing and ICT areas from all jurisdictions, principals associations, school council association, experts in the fields of bullying, cybersafety and behaviour change, as well as from internet and technology industry.

Key findings from schools' needs analysis

An overwhelming number of respondents **(97 per cent) saw benefits for their school in becoming an acknowledged *eSmart* school**.

The strongest theme that emerged from the research was that very positive perceptions were held by the respondents about the model, criteria and verification processes. Terms used included *excellent, user-friendly, logical, appropriate, reasonable, great, specific, clear, supportive and thorough.*

The second strongest theme related to the **comprehensiveness** of the criteria, that is, all of the important areas were covered and **nothing had been left out.** Respondents were very positive about the potential benefits to their school. Many commented that they had already started to address cybersafety and that the Framework would help them to keep the momentum going and improve it. Other common responses were that the Framework would:

- enable access to additional resources and expert information that is up-to-date and reflects evidence-based practice
- enable the school to put together a coherent and consistent framework which was co-ordinated and not just ad hoc – and that this would enable the school to give a consistent message about cybersafety
- reassure parents and send a message to them that the school was serious and proactive about cybersafety.

Most schools thought it essential to include smart use of technologies as a positive tool for learning.

Questions about current practices revealed:

- Independent schools (65 per cent) and Government schools (52 per cent) were more likely to explicitly teach about cyber-risk and cybersafety than Catholic schools (40 per cent)

- Thirty-eight per cent of primary schools, 71 per cent P–12 and 50 per cent of secondary schools explicitly taught about cyber-risk and cybersafety

- About 50 per cent of respondents in each state said that they taught explicitly about cyber-risk and cybersafety

- Almost all schools had a formal published policy about bullying (three secondary schools and one primary did not)

- Having a reasonably detailed policy on cyberbullying was more common in Independent schools than Government or Catholic schools and in secondary or P–12 schools than in primary schools

- All but one primary had a published Acceptable Usage Policy

- Mobile phone policies were less prevalent in primary schools when compared to secondary or P–12 schools

- A smaller percentage of Catholic schools had mobile phone policies than other schools

- Eighty-two per cent of responding schools said that none or only a few of their teachers had attended professional development dealing specifically with cyber-risk and cybersafety

- Teachers from secondary schools were slightly more likely to have attended relevant PD than primary or P–12 teachers.

vii. analysing information on achieving and continuing world's best practice safeguards

Keeping abreast of the ever-changing world of technology, the ways children and young people access and use technology, and the current most prevalent and most serious cyber-risks is an ongoing challenge. Importantly, effective strategies to manage cyber-risks need to be developed and constantly reviewed to ensure they continue to be effective and reflect best practice. The development of these strategies must be underpinned by a strong evidence base.

Australia leads the world in research into many areas of cybersafety and wellbeing, and ongoing support of research in these areas is vital. Constant review of overseas research and practices is also important as is an understanding of how this information applies to the Australian context. The need for support of ongoing research into cybersafety and wellbeing in Australia was one of the key outcomes of the 4th Biennial *NCAB* Conference, 'Navigating the Maze - cybersafety and wellbeing for schools'.

Because of the borderless nature of the internet and other technologies, Australia needs to support ongoing links and knowledge transfer with other countries. This will maximise alignment and cooperation in efforts to implement policing practices and help overcome barriers that varying legal jurisdictions bring to the management of cyber-risks. Ongoing analysis and research into these areas is also important to ensure Australia is informed about and can benefit from cutting edge practices in place overseas.

Both formal and informal networks exist to enhance dissemination of knowledge and to help ensure best practice safeguards are in place. A number of these are discussed in part iv of this submission. For its own part, The Alannah and Madeline Foundation has developed links with key stakeholders, nationally and internationally, including the technology industry, education sector, research and community organisations in order to remain informed of the current best practice safeguards for cyber-risks and to ensure that these are encompassed in its own work.

viii. the merit of establishing an Online Ombudsman to investigate, advocate and act on cybersafety issues

The Alannah and Madeline Foundation advocates a broad community change approach to cybersafety. Fundamental to the model is empowerment of children, young people and adults alike to keep themselves safe and to deal with the inevitable risks the online world brings. This includes the ability to report and seek support when risks and potential harm are identified.

When in immediate danger, the advice always given is to call 000. Children and young people are always encouraged to seek help from a trusted adult. Help Line and Kids Helpline receive calls regarding cyberbullying and cybersafety issues. Social networking sites also have mechanisms on their sites for reporting cybersafety issues.

There are currently a number of other, more specialised, mechanisms for reporting cybersafety issues, including reporting to the Australian Communications and Media Authority (ACMA) issues around cybersafety and inappropriate content, reporting to the Privacy Commission concerns around breaches of privacy, reporting to the Australian Human Rights Commission complaints of discrimination and human rights breaches, and reporting potential criminal activity and illegal content to the Australian Federal Police.

Any new mechanism being considered for investigating, advocating and acting on cybersafety issues should take into consideration the significant resources, support and expertise already available and should include how these current mechanisms can be better harnessed, coordinated and communicated.

An appropriate legal framework for bullying, cyberbullying and other cyber-risks is fundamental for an effective response to cybersafety issues, and would strengthen the existing avenues of complaint, reporting and redress.

It is important that it is clear to the community how and where to seek help, that it is easy to do so, and that the response is timely and effective.

References

ACMA (2009) click and connect: young Australians' use of online social media 02 Quantitative research report.

Australian Communications and Media Authority, (2009) Click and Connect: Young Australians' Use of Social Media, Qualitative Report Volume 1. Pp 10-11.

ACMA (2009) use of electronic media and communications: early childhood to teenage years.

ACMA Cybersmart Guide for Library Staff Commonwealth of Australia 2009

Australian Bureau of Statistics 8146.0 - Household Use of Information Technology, Australia, 2008-09 (accessed online, May 16, 2010)

Australian Covert Bullying Prevalence Study, Child Health Promotion Research Centre, Edith Cowan University, May 2009, published by the Department of Education, Employment and Workplace Relations.

BBC Online News 'Fears over pro-suicide web pages '(http://news.bbc.co.uk/2/hi/health/7341024.stm) Accessed, May 2010.

Bauman, S. (2007), Cyberbullying: a Virtual Menace, Paper presented at the National Coalition Against Bullying National Conference, November 2 – 4, 2007, Melbourne, Australia. Retrieved May 2010 from: http://www.ncab.org.au/pdfs/NCAB%20papers/Workshops/Bauman,%20Dr%20Sheri%20-%20Cyber%20Bullying%20The%20Virtual%20Menance.pdf

Cao, F. & Su, L. (2007), Internet addiction among Chinese adolescents: prevalence and psychological features, Child: Care, Health and Development, Volume 33, Number 3, May 2007 , pp. 275-281(7)

Carnagey, Nicholas L., Anderson, Craig A., and Bushman b, Brad J., (2007) The effect of video game violence on physiological desensitization to real-life violence, Journal of Experimental Social Psychology 43 489–496 (accessed online June 2010).

Child Safety Commissioner, Melbourne, Victoria, Australia, (2007) Calmer Classrooms.

Choo, Kim-Kwang Raymond (2009) Responding to online child sexual grooming: an industry perspective, Trends & issues in crime and criminal justice no. 379, Australian Institute of Criminology

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

DSM IV, (Diagnostic and Statistical Manual of Mental Disorders-4th Edition), 1994, APA (American Psychiatric Association),

DSM IV-TR (Diagnostic and Statistical Manual of Mental Disorders-Text Revision), 2000, APA (American Psychiatric Association)

DeAngelis, T., 2000, Is Internet Addiction Real? Monitor on Psychology, Volume 31, No. 4, April 2000

Greenfield, D.N. (1999), Psychological characteristics of compulsive Internet use: a preliminary analysis. Cyber Psychology and behavior, 2, 5, 403-412.

Kandersteg Declaration Switzerland, June 10, 2007 (http://www.kanderstegdeclaration.com/storage/English%20KD.pdf) website accessed 22 June 2010.

McGrath, H., (2009) Young People And Technology: A review of the current literature (unpublished document, The Alannah and Madeline Foundation.

McGrath, H., Craig, S and Stanley, M, Final Report and Antibullying Policy and Practice in the State of Victoria (unpublished document, 2005)

News.com.au April 1, 2010 (Accessed May 2010).

Norris Gareth, Lincoln Robyn and Wilson, (2005) Paul Contemporary comment: An examination of Australian internet hate site Humanities & Social Sciences papers, Bond University.

Olweus, D. (1980). Familial and temperamental determinants of aggressive behavior in adolescent boys: a causal analysis.
Developmental Psychology, 16, 644-660.

Rigby, K., (2010) Evidence does not support the view that bullying is on the rise The Australian Teacher Magazine, April (accessed online, 18 May 2010)

Sisk, Cheryl L. (2006) New Insights Into The Neurobiology
Of Sexual Maturation, Sexual and Relationship Therapy, Vol 21, No. 1, February

The age newspaper online: Lost in cyberspace: fears over teen sites April 24, 2007, accessed May 2010.

Wallbridge, R., (2009) How safe is Your Facebook Profile? Privacy issues of online social networks, ANU College of Law, The Australian National University, Acton ACT 0200, Canberra, Australia

Yoo H.J, Cho S.C, Ha J, Yuen, S.K, Kim S.J, Hwang J, Chung A, Sung Y.H & Lyoo I.K, 2004, Attention deficit hyperactivity symptoms and internet addiction, Psychiatry and Clinical Neurosciences ,58(5):487-94

Yahoo web forum
((http://au.answers.yahoo.com/question/index?qid=20100509231241AAC1cU3) accessed 18 May 2010.

Young, K. n.d., Centre for Internet Addiction. http://www.netaddiction.com/

Appendix 1

The Sydney Morning Herald: national, world, business, entertainment, sport and technology news from Australia's leading newspaper.

Is cyberbullying a crime?

Nick Abrahams with Victoria Dunn
May 21, 2009 - 1:52PM

Cyberbullying is back in the spotlight. Earlier this month the federal government announced it had established a Youth Advisory Group, consisting of young Australians, to advise it on cyberbullying and other online issues.

Within a week came the report that two year 9 students had been forced to leave a Sydney girls' school for cyberbullying. As a result, I have been asked a number of times - shouldn't there be laws to stop this?

The answer is that there are some laws which cover the most aggressive forms of cyberbullying but, unless you want to start filling jails with 15-year-olds, criminal sanctions are not the answer.

Bullying has been around for a long time. Recently, many schools have really focused on the issue and there has been some success in reducing the incidence of traditional school yard bullying. However, the internet is the bully's new school yard. Studies have shown that cyberbullying is widespread, with at least one in three teenagers the victim of cyberbullying.

Cyberbullying presents new challenges to young people, their parents and society. Cyberbullying is different to traditional bullying in a number of key respects:

1. Anonymity: The impression of anonymity in the online world leads young people to feel less accountable for their actions and provides a false bravado to would-be bullies. In fact, a recent study has shown that, of bullies surveyed, 70 per cent had engaged only in cyberbullying.

2. Geography: Rather than being limited to the school-yard, cyberbullying operates wherever a young person uses the internet or a mobile phone. There are few areas of a young person's life which cyberbullying cannot penetrate.

3. Impact: The internet provides a means to make bullying comments available to a wider audience than ever before. Through social networking sites, comments can be viewed by potentially thousands of people. The impact of and embarrassment caused by these statements is therefore magnified.

4. Permanence: Verbal comments are fleeting. Online they stay around, potentially forever.

Where cyberbullying is serious, it may be appropriate for the law to step in to impose penalties on bullies.

In cases where bullying involves a threat to kill or seriously injure a person, state-based criminal legislation could be used to lay criminal charges against bullies. However, where bullying does not include such threats, but is more in the realm of emotional cruelty, legal protection offered to victims is piecemeal.

Under the NSW Crimes Act it is a criminal offence to harass or intimidate a school student while the student is at school. This offence can be applied to traditional off-line bullying, but has its limits as it applies only to activities done at school.

As cyberbullying can occur exclusively outside the school yard, it is quite possible that cyberbullying would not be caught by this provision.

The Commonwealth Criminal Code sets out an offence of using a carriage service (such as a mobile phone service or the internet) in a way that is menacing, harassing or offensive. The maximum penalty for committing the offence is 3 years imprisonment.

While it has the potential to be used in cases of cyberbullying, to date charges under this section of the Code have been brought only in relation to harassing phone calls.

Some state governments have specifically expanded the scope of the off-line harassment laws to cover online activities.

In Victoria, for example, the stalking provisions of the Crimes Act could extend to catch cyber-bullies who post information about a victim on the internet, intending the post to cause mental harm to the victim, or to cause the victim to fear for his or her safety.

However, even where specific legislation designed to apply to such online activities exists it has been of little effect, with no cases of successful prosecution for cyberbullying in Australia.

In the absence of specific and effective laws dealing with cyberbullying, victims must rely on laws largely designed to apply in the off-line world and, in many cases, developed before the advent of the internet.

Such laws include defamation law (which may offer some redress to victims about whom false statements have been published online) and laws preventing harassment of individuals on the basis of race, region and sexual orientation.

This piecemeal legal regime does not offer a comprehensive response to the increasing problem of cyberbullying - nor should it.

Given the subjectivity of bullying, and the young age of many cyber-bullies, the traditional legal approach of deterring potential offenders by threatening criminal sanctions is not appropriate, except in the most serious cases.

There are those that propose that there should be laws requiring Internet Service Providers to remove bullying-related material from websites. While I am sympathetic to why people would want this, it is very difficult to create a workable solution.

How is the ISP to judge what is bullying content and what is not?

It is so subjective and places a heavy burden on ISPs. This issue of take down will become more acute in the future as more people seek to change their digital footprint - not just because of bullying material but perhaps because the content might be defamatory, or just something they wish a friend didn't put up on the internet when everyone was 18 or even something they themselves wish they did not put up on the internet when they were 18.

Currently, the most effective weapons for combating cyberbullying are education programs and a commitment by schools to implement and enforce policies. Such education programs should include:

:: continuing education of teachers and schools about changes in technology and the potential for technology to be used by cyber-bullies;

:: educating kids about cyberbullying - why not to do it and how to deal with it; and

:: educating parents about technology so they can understand what their kids are doing online and talk to them about it.

Bullying happens, but it should not be accepted as inevitable. Much has been done by schools and parents in recent years to raise awareness of and to reduce off-line bullying. This has been achieved without resorting to specific off-line bullying laws. Similarly, cyberbullying needs to be targeted and stopped at the grass roots level.

The law should be there to backstop schools and parents in the most serious of cases. But new laws may become necessary depending on how cyberbullying develops. Technology magnifies the potential for harm to be inflicted in ways we had not before imagined.

Remember the recent Lori Drew case. Who would have thought that a mother would make up a fictitious boy on MySpace, use the "boy" to court one of her teenage daughter's friends, then drop her coldly, causing the girl to commit suicide. Only in America - or maybe not.

Nick Abrahams is a Partner and Sydney Chairman of the law firm Deacons. Victoria Dunn is a lawyer with Deacons.

APPENDIX 2 National Centre Against Bullying

***The National Centre Against Bullying* membership**	
Chair The Hon Alastair Nicholson AO RFD QC	
Members	
Dr Pamela Bartholomaeus	Lecturer, Flinders University
Andrew Blair	President, Association of State Schools Principals
Dr Marilyn Campbell	Lecturer, School of Learning and Professional Studies, Queensland University of Technology
Dr Michael Carr-Gregg	Adolescent Psychologist, Author and Speaker
Sandra Craig	Manager, National Centre Against Bullying
Prof Donna Cross	Child and Adolescent Health, Edith Cowan University
Maree Davidson	Principal, Davidson Consulting
Evelyn Field	Psychologist, Author and Speaker
Stephen Franzi-Ford	CEO, Association of School Councils of Victoria
Andrew Fuller	Clinical Psychologist and Family Therapist
Coosje Griffiths	Area Manager, Student Services, Department of Education and Training, Western Australia
Adj. Prof Helen McGrath	RMIT University, School of Education
Rob Masters	Principal, Robert Masters and Associates
Dr Toni Noble	Senior Lecturer, Australian Catholic University
Prof Ken Rigby	Adjunct Professor, University of South Australia
Prof Phillip Slee	School of Education, Flinders University
Barbara Spears	Senior Lecturer, School of Education, University of South

	Australia
Maree Stanley	General Manager, Prevention The Alannah and Madeline Foundation
Dr Judith Slocombe	CEO, The Alannah and Madeline Foundation