Submission 206
Date received: 16/03/2011

Submission By

The Alannah and Madeline Foundation

For

House of Representative Standing Committee

Inquiry into the Role and Potential of the National Broadband Network

March 2011

Prepared By:
Dr Judith Slocombe
CEO
The Alannah and Madeline Foundation
PO Box 5192
South Melbourne Vic 3205
Phone:
Email:

Contents

1. Introduction

The following submission from The Alannah and Madeline Foundation (AMF) acknowledges the need to minimise risk and prevent social and personal harms associated with modern technologies and inadvertently with the rollout and take up of the National Broadband Network (NBN). The submission also expresses the need to create an environment that enables and supports the Australian community across homes, schools, workplaces, sport and recreation settings, libraries, health care facilities and other community institutions to engage in smart, safe and responsible use of technology.

Whereas it is in the national interest that Australians embrace the digital space and all that technology has to offer, there are considerable well-documented risks associated. These risks may be exacerbated by the introduction of the NBN. The last-published ABS data shows around 72 per cent of Australian households have internet access, and 78 percent have access to a computer. This is sure to increase significantly with fast, reliable broadband, and unless preventive action is taken so will the associated harms.

The challenge is to promote the benefits whilst managing the risks associated with a cyber-enabled society so that children, their families and the broader community can engage smartly, safely and responsibly with technology to enhance their lives.

Given its charter and the nature of its work, the focus of this submission by AMF is on children and young people within a broader community context.

Our submission proposes the adoption of eSmart as part of the NBN rollout to help ensure this major investment to increase Australian's access to modern information and communications technology is able to reap all the benefits while mitigating the risks. eSmart is a world leading, and evidence-based cultural change system designed and developed here in Australia to raise community awareness and provide a systematic and coordinated approach to cybersafety and security though schools and other settings.

Recommendations

The Alannah and Madeline Foundation recommends to this Inquiry that:

- The NBN rollout incorporates a comprehensive and well resourced cultural change approach to ensure that any associated personal risks and social harms are reduced.

- The Alannah and Madeline Foundation's eSmart system (a public education campaign and eSmart approaches in a range of professional and community settings) be adopted and funded as a health promotion, risk reduction and harm prevention measure, starting with eSmart Schools and eSmart Libraries.

- Research including a longitudinal study tracking the individual and social impacts of the NBN over time is included in the rollout plans.

When asked, "What's the best thing about being a young person today?" most children and teenagers would probably say "technology". They can't imagine a time when young people didn't have access to the tools of communication that enable constant contact with their peers and instant access to a world of information.

We can learn a lot from young people about using and enjoying the benefits of these technologies.

Unfortunately, it seems that almost every day there seems to be another media story of online sexual predators, gaming addiction, internet scams, identity fraud or cyberbullying. The dangers of cyberspace can make us increasingly worried for our children's safety, but also our own.

The introduction of the National Broadband Network will support communities to harness the productive and creative benefits of new communications technologies, while hopefully learning safe and responsible practices and minimising the risks.

2. The Organisation

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 Alannah and Madeline Foundation play an advocacy role and is a voice against childhood violence.

The Foundation's National Centre Against Bullying (NCAB) is a peak body made up of experts 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.

Our Cybersafety and Wellbeing Initiative – eSmart - 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. Following the evaluated success of this pilot phase, eSmart is currently being offered to schools nationwide.

3. The Environment

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.

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.

According to Australian Bureau of 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.

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).

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) support 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 The Australian Communications and Media Authority (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.

3.1 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 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 2009, as part of the Cybersafety and Wellbeing Initiative (*eSmart*) The Alannah and Madeline Foundation formed a Reference Group, 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 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.

A second Consultative Group brings together key stakeholders from the various educational jurisdictions from around Australian to ensure eSmart 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 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.

4. The Issues

The nature, prevalence, implications and level of risk associated with digital technologies are wide ranging and significant. They include:

- 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.

The section following explores these risks in more detail, providing evidence of the extent of the issues as we know them to-date. It is the Foundation's view that the online risks for young people will increase with the reach of the NBN, unless mitigating strategies are rolled out in parallel with the roll out of the technical infrastructure.

4.1 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.

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).

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.

4.2 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).

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.

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; and
- 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; and

- 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.

4.3 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.

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)

4.4 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.

4.5 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.

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.

5. The Response – Leading to an eSmart Australia

The Alannah and Madeline Foundation recognises that the promotion of positive behaviours, prevention of harm and reduction of cyber related risk are neither simple nor straightforward. The response to existing and emerging issues is necessarily complex and comprehensive and must draw on the experience and expertise gained in dealing with other serious health and social issues whilst acknowledging what is unique and different about cyber related behaviour and broader social impacts.

Taking this into consideration AMF has developed a comprehensive and integrated response within the context of existing and emerging evidence, broader social change and the crucial role of schools. It has also considered the supportive and active environment into which the resulting eSmart initiative has been introduced.

5.1 Education

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.

5.2 A Comprehensive Change Model

Australia does not currently have in place a strategic cybersafety / cyberbullying behaviour change model that intersects with the education sector. The Alannah and Madeline Foundation recognised the need for an approach that builds 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 and the wider community need to make the links between cybersafety and wellbeing, and understand the importance of creating a caring and respectful culture where bullying and cyberbullying are not tolerated.

Currently most attention is given to cyber-related risk and harm. Less focus is placed on the interplay between the social, educational and economic benefits of the cyberworld and its less desirable attributes. Until now, applied social research has been another gap in the research landscape - particularly testing the efficacy of comprehensive and holistic systems such as eSmart that aim to develop safe, smart and responsible use of technology.

5.3 A Behaviour and Social Change Approach

The comprehensive integrated behaviour and social change approach of the eSmart initiative was chosen as both appropriate and effective because the opportunity to build on the evidence base and learnings of successful change approaches such as SunSmart, Worksafe, TAC and the tobacco control movement.

Australia has led the way internationally in these areas. The effectiveness of multidimensional, mass reach strategies underpinned by research, policy and practice frameworks is clearly established.

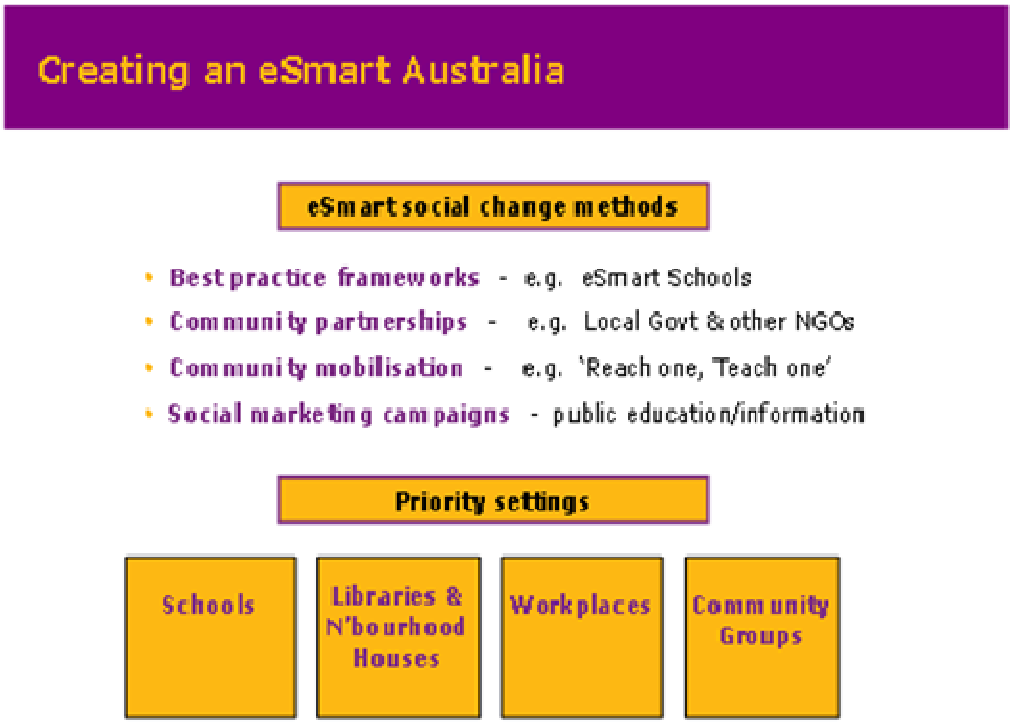
Social change approaches adopt strategies that shift societal norms and other environmental factors to bring about large-scale behaviour change. They consider communities, organisations, policies, laws, and popular culture, as well as individuals in a variety of settings including schools.

In short, 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.

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 change attitudes.

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

The diagram below illustrates the scope of the approach undertaken.



5.4 Focus on Schools as a Starting Point

The Alannah and Madeline Foundation was confident that the initial phase of the eSmart approach should have schools at its centre, employing community awareness raising and education strategies in support.

Theory and evidence around a 'Health Promoting Schools' approach support the role of schools in affecting individual behaviour and influencing broader social change. 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.

Successful social change requires a catalyst to get the issue on the personal, community and political agenda, stimulate social dialogue and drive consideration, uptake and implementation of options for action.

Schools are in an optimal position to take on the challenge of being drivers for positive cyber-related change.

5.5 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.

5.6 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. Advocating in this area is already on the eSmart agenda similar to the way in which Cancer Councils through SunSmart advocated successfully for sunscreen product re-design.

5.7 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.

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.

5.8 Cooperation of Stakeholders

As would be expected in an area of such rapid growth and development, and one which has such potential to impact on the life of all Australians, there are many stakeholders. They represent a vast array of vested interests in ICT and associated issues.

The extent and type of this active collaboration and cooperation is outlined below. However, until the development of eSmart there has been no single system to assess and bring together the combined knowledge, understanding and resources, and solutions in a way that can provide accessible, evidence-based guidance and support to the schools and the broader community.

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* and *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.

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

Input to the development of the necessary components of a whole-school approach to cybersafety and wellbeing was sought from senior education administrators in various state government departments, the Catholic Education Office, and independent schools' representatives through Consultative and Reference Groups held in March and April 2009.

Other stakeholders provided information on current technologies and applications, usage patterns, current research, and the policy landscape. Consultation was undertaken with the Department of Broadband, Communications and the Digital Economy (DBCDE), Australian Communications and Media Authority (ACMA), Australian Mobile Telecommunications Authority (AMTA), the Australian Federal Police (AFP), Microsoft, Telstra, MySpace, Google and a range of experts in the fields of bullying, sexual predation, cybersafety, and communications technology.

5.9 Why 'Smart' Makes Sense

The Alannah and Madeline Foundation commissioned social marketing agency Shannon's Way to develop a positioning strategy and branding for its cybersafety and wellbeing initiative.

The agency began work in February 2009 with Sweeney Market Research to build the brand for the Initiative, ensure language used would be motivating and appropriate, and make sure the brand would engage and meet the expectations of parents, teachers and young people.

The market research identified a number of useful insights, which are summarised below:

1. Young people do not themselves use the terms 'cyberspace' or 'cyberbullying'— while they understand them, it's not their language.

2. Young people are generally not concerned with cybersafety, and believe that adults are somewhat hysterical in their fears of the Internet.

3. Despite their lack of concern, young people are putting themselves at risk and are quite naïve about the dangers.

4. 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.

5. Adults believe their ignorance has led to an unhealthy power shift, so that young people are too easily able to operate under the radar, and without the normal boundaries around their behaviour.

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

7. Teachers believe parents should take a lot more responsibility for their children's behaviour (both online and offline).

8. Parents (and teachers) would like to know more about the virtual spaces young people inhabit, but don't know where to start.

These insights helped to identify that the primary positioning for the initiative should be 'smart'. Young people would be more amenable to activities that were dealing in the realm of 'smart' rather than 'safe', and adults understood that they had to get more 'smart' in order to keep their children 'safe'.

The market research also identified that parents and teachers were supportive of the Initiative being delivered by a not-for-profit, and a non-government organisation. They believed the Foundation would be a strong fit because of its focus on children's safety; that it is credible because it is a not-for-profit organisation (not in it for the money); and that the Foundation has a reputation for 'getting things done'.

6. Supporting Culture Change in Schools

It is essential to support schools to change their culture as a means of increasing positive and smart use of technology and reducing the incidence and harmful effects of cyberbullying and other cyber-risks. This support includes:

- 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;

Cyberbullying 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.

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; and

- 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 modeled 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.

6.1 The Alannah and Madeline Foundation's eSmart System

eSmart 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.

- eSmart supports exploration of:

    - protective behaviours;

    - supportive and relationship building behaviours; and

    - reporting of incidents.

eSmart embraces:

- whole-of-school wellbeing issues including values/relationships/self-esteem;

- e-security;

- ethics including downloading and plagiarism; and

- criminal activity including sexual harassment and predation.

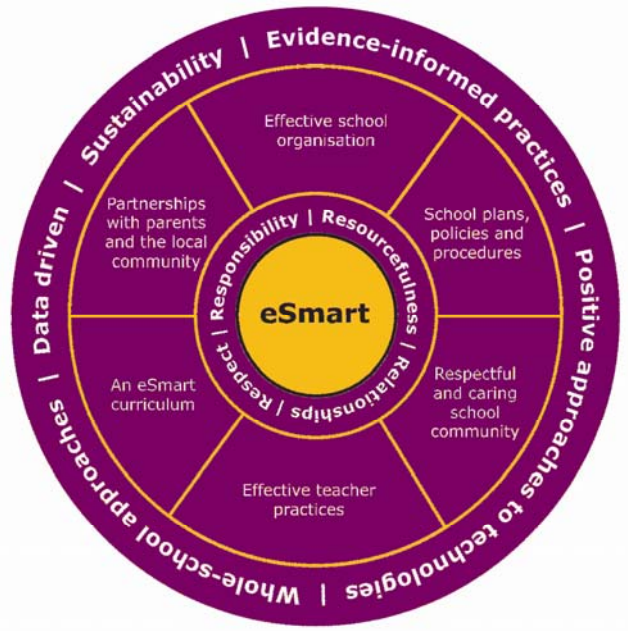
eSmart is underpinned by the positive embrace of ICT and the promotion of smart use of technology.

eSmart 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 eSmart 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.

6.2 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 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 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 will be regularly updated to reflect new knowledge and will point to new, high-quality programs and resources for schools.

eSmart 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 (eSmart), involving over 150 schools across Australia. This Pilot concluded in mid 2010, and was independently evaluated by Prof Donna Cross' team at the Child Health Promotion Research Centre at Edith Cowan University with very positive results.

Through the national pilot, schools identified eSmart as an effective road map to guide schools on how to deal with bullying and cybersafety; the missing piece to navigate through the plethora of available resources, and to implement and sustain relevant policies and practices.

- 98% of schools reported that eSmart is a **very effective** approach to cybersafety and wellbeing in schools and nearly 100% **recommended eSmart be rolled out to all schools.**
- 96% of school staff interviewed reported they would recommend eSmart to other schools.
- Schools reported eSmart prompted action in cybersafety that they would otherwise not have undertaken.
- 100% of schools reported eSmart was consistent or very consistent with their current school policy and practices and eSmart was compatible with their school's priorities, culture and student needs.

- Schools were very satisfied with eSmart and the way it was presented on the internet. Schools were happy with the support provided by the Foundation's Schools Liaison Team, particularly the Help Desk.

- Education and industry stakeholders alike said eSmart addressed all essential elements for cybersafety and wellbeing in schools.

7. Conclusion

This submission has outlined the already existing risks to children and young people through their use of ICTs and in particular, the internet, and argues that with the introduction of the NBN the prevalence of these issues will only increase.

In order to reap the full, positive potential of the NBN it is vital that a comprehensive risk mitigation strategy be rolled out in parallel with the technical infrastructure.

eSmart is submitted to this Inquiry as the most fully developed strategy to address the issues related to the smart, safe and responsible use of ICTs and the internet (increasingly to be facilitated by the NBN). With its 'smart' positioning, and emphasis on positive use of ICTs, the brand is complementary to the positive benefits promised with the rollout of the NBN.

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.

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, Laurel Downey, Manager, Practice Development and Training, Take Two, Berry Street Victoria.

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.

Yahoo web forum:

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

Review of Existing Australian and International Cyber-Safety Research (Dr Julian Dooley, Professor Donna Cross, Dr Lydia Hearn) Child Health Promotion Research Centre, Edith Cowan University, April 2009.

Sweeney Market Research, Commissioned by The Alannah and Madeline Foundation, February 2009.

Evaluation of the National Pilot of the Cybersafety and Wellbeing Schools Initiative - the eSmart Schools Framework. Prepared by: Child Health Promotion Research Centre, Edith Cowan University, April 2010, Investigators Stacey Waters, Professor Donna Cross and Dr Julian Dooley.

A Report on the National Pilot of the *Cybersafety and Wellbeing Initiative – An approach to cybersafety for schools,* Australian Council for Educational Research June 2010.

Appendix 1:

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.

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 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.